THE SECURITY LEADERSHIP SERIES

CLOUD MIGRATION: THE SKY IS THE LIMIT

TrustedImpact
PROTECTING DIGITAL

PRODUCED IN PARTNERSHIP WITH

AISA

"The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user, not the Cloud Provider, who fails to manage the controls used to protect an organisation's data...

Through 2025, 90% of the organisations that fail to control public cloud use will inappropriately share sensitive data...
Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks...
Through 2025, 99% of cloud security failures will be the customer's fault....

Exaggerated fears can result in lost opportunity and inappropriate spending. [...] There is no such thing as perfect security protection. Accepting some risk is necessary for leveraging public cloud services but ignoring these risks can be dangerous."

– Gartner[1]

1. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Foreword from AISA's Chairman, Damien Manuel

For the last 10 years, cloud computing has been an increasingly attractive subject of conversation, and it's easy to understand why. The cloud allows organisations of all sizes to access their data from anywhere; at any time. It's also scalable which makes it very practical in the logic of 'pay for what you use'. Cloud computing has therefore become a 'must have' for many organisations who are embracing these service as quickly as possible – particularly in a COVID-19 'work from home' world. However, cloud adoption can sometimes come at the cost of security and business resilience, especially if the appropriate risk and security implications are not considered along the journey.

Trusted Impact's 'Cloud Computing: Sky Is The Limit' Leadership Series paper provides valuable insight into how a number of leading Australian organisations are embracing the cloud. It also presents practical approaches for organisations and security practitioners to consider as they migrate to, and truly leverage, the vast benefits of the cloud.

The Australian Information Security Association's (AISA) partnership with Trusted Impact is part of a collaborative industry approach, with the aim of sharing industry insight and expertise to strengthen the security posture of all Australian organisations. We look forward to continued collaboration in the future as our industry continues to grow and expand to support a strong and resilient digital Australia.

As a nationally recognised not-for-profit organisation and charity, AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia.

Established in 1999, AISA has become the recognised authority on information security in Australia with a membership of over 7500 individuals and corporate organisations across the country. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA

Cyber | smart · safe · secure

aisa.org.au

The Study

To identify the key trends, issues and considerations regarding cloud adoption and to leverage local insight into the cloud adoption we chose to conduct a comprehensive study that gathered data and insight from approximately 30 influential Australian leaders in technology and security.

Survey participants were chosen from a diverse range of large to small; Commercial and Government organisations, and from various industry sectors including, for example, financial services, education and healthcare.

While these Leaders were given an overall structure from which to respond to key questions, an important aspect of the survey involved having an interactive conversation to capture views from their individual and organisation's perspectives.

We chose to base the questions broadly around the NIST Cyber Security Framework[3] and more particularly its 5 main 'functions' of Identify, Protect, Detect, Respond and Recover. The NIST Cybersecurity Framework is a comprehensive set of 'best practices' in relation to helping organisations improve their cybersecurity maturity.

The aim was to capture practical insight from various perspectives; to identify significant maturity gaps, and formulate constructive recommendations regarding what could be done to help Australian organisations to 'shift to the cloud' in the safest way possible.

3. https://www.nist.gov/cyberframework

Contents

Preface

THE DIGITAL TIPPING POINT

A tipping point, or inflection point, is a phenomenon in both the physical sciences and in human interaction. It is a point in time when everything changes— the moment of critical mass, the threshold, and the boiling point[2]. This is when a biological system, cultural change, technology or a new idea moves from fad to trend; from interesting sidenote to landscape-altering tsunami. We fundamentally believe we've reached the tipping point in relation to "digital transformation".

Today we live in an 'always on' world where our smart watches are connected to our smart phones; which connect to our smart, nearly autonomous cars, that we park at our smart homes, where we ask our digital assistants, Siri, Alexa or Cortana to play a song, check the weather or turn on the lights – all simply by communicating on the internet. Now over half of the world's population – nearly 5 Billion global consumers can transact; wherever they are and whenever they want.

To meet this opportunity, organisations of all types are transforming the way they engage with their customers or stakeholders by digitally intertwining customers, citizens, employees, partners, suppliers, shareholders and stakeholders into a tightly woven global digital supply chain with the battle cries of new markets, accelerated innovation, increased speed to market, lowered costs and improved service.

And just when we thought digital transformation couldn't accelerate much faster, the global COVID-19 pandemic has been that 'landscape-altering tsunami' where there is both urgency and overwhelming need to engage digitally for nearly every aspect of our daily lives.

ENTER THE CLOUD

One of the cornerstones of digital transformation has been Cloud Computing. In 1996, George Favaloro and Sean O'Sullivan predicted that most software services would move to the web and introduced what they called 'cloud computing-enabled applications', and in 2006, Google CEO Eric Schmidt first introduced the term to an industry conference.

The use of cloud-based services and the multiplication in the diversity of services has since been increasing at a dramatic speed. Cloud computing is indeed very attractive, explaining why so many organisations are so eager to transfer everything they've got to the Web. According to David Mitchell Smith: "Cloud computing is increasingly becoming a vehicle for next-generation digital business as well as for agile, scalable and elastic solutions [...] CIOs and other IT leaders need to constantly adapt their strategies to leverage cloud capabilities."

Providing data access from anywhere – and at any time – is one of the top reasons for cloud adoption. Disaster recovery, flexibility, and relieving IT staff's job are amongst the top answers as well. This is linked to the fact that many organisations think that Data Security and everything regarding Incident Management and Disaster Recovery is the responsibility of the Cloud Provider.

Cloud computing also eliminates the historical challenge of buying and maintaining hardware and enables both users and enterprises to run software without needing to install it. Cost optimisation and 'pay for what you use' is the primary reason why nearly half of enterprises undertake cloud migration.

"There was a time when every household, town, farm or village had its own water well. Today, shared public utilities give us access to clean water by simply turning on the tap; cloud computing works in a similar fashion. Just like water from the tap in your kitchen, cloud computing services can be turned on or off as quickly as needed.

Like at the water company, there is a team of dedicated professionals making sure the service provided is safe, secure and available on a 24/7 basis. When the tap isn't on, not only are you saving water, but you aren't paying for resources you don't currently need." –Vivek Kundra, Federal CIO, United States Government, 2010.

While the shift to the Cloud represents an exciting opportunity for scalability, availability and cost-optimisation, it also opens the door to new kinds of threats if not consciously and conscientiously considered.

FOR EVERY POSITIVE, A NEGATIVE

Pablo Picasso said, "Every positive value has its price in negative terms... the genius of Einstein leads to Hiroshima".

Indeed, as the digital web becomes more intertwined and complex every day, the threats to security also grow both in number and sophistication. This complexity is mainly due to the growing interconnection of both people and devices; the increase in number of malicious cyber actors, and eventually the attractiveness of cyber-related attacks. The new oil of the digital machine

2. https://en.wikipedia.org/wiki/The_Tipping_Point

is data – it's confidentiality, integrity and availability.

As noted in the Australian Cyber Security Strategy 2020 "The world has never been more interconnected; our reliance on the internet for our prosperity and way of life never greater [...] However, as the opportunities have increased, so too have cyber threats. Well-equipped and persistent state-sponsored actors are targeting critical infrastructure and stealing our intellectual property. Cyber criminals are also doing great harm, infiltrating systems from anywhere in the world, stealing money, identities and data from unsuspecting Australians."

Cloud computing and cloud-based assets are attractive targets and miscreants of society are finding new and different ways to exploit the cloud because it's:

- easy to get to (with no traditional geographic or physical distance limitations),
- easy to access (due to weak access control)
- easy to exploit (due to technical and configuration exposures and vulnerabilities),
- easy to avoid apprehension (due to cross country jurisdictional constraints)
- easy to monetise (thus increasing motivation), and
- easy to learn (limited barriers to entry – with free tools and training)

FINDING YIN-YANG

The aim of this Leadership Series paper was to have meaningful conversations with a number of Australian 'leaders' involved with technology, cybersecurity and/or cloud computing in order to better understand what is being done in Australia to achieve the 'yin-yang' counterbalance of these interconnected and opposite forces.

Our initial data gathering and industry research uncovered a number of potential hypotheses worthy of assessing with our local Leaders. According to various industry papers such as the Thales 2020 Data Threat Report, some of the main concerns appeared to be privacy, security and lack of staff training – "95% of cloud security failures will be the customer's fault". In addition, leakage of sensitive customer/personal data, unauthorised access and data corruption were often raised as impediments to cloud adoption. However, we noticed that those concerns didn't necessarily prevent organisations from jumping to the cloud... Indeed, the desire and need to embrace digital transformation and cost advantages are too appealing.

Hence, as organisations 'jump to the cloud' without even blinking, it seemed crucial to address security concerns for Australian organisations, and more precisely regarding the protection of sensitive data. The first concern that we would like to address regards the lack of executive level involvement in the development of cloud policies and overall cloud migration strategies: Cyber Security is not an 'IT problem' but definitely a business challenge!

Our second concern is the lack of cloud-specific awareness training: awareness training is on the rise, but it doesn't seem to include cloud risks. Yet, cloud use is growing and so are the threats that users might face. Therefore, we believe that cloud risks should be included in every Cyber Security Awareness Program. The third concern we would like to address is the 'high trust, low proof' approach that tends to characterise the relationship between Cloud Providers and their customers: our research work showed us that even though most organisations perform risk assessments before engaging with Cloud Providers, they still tend to trust their Cloud Providers (especially top tier ones) and are not actually checking if their security measures are effective. Our fourth and final concern is 3rd party/customer dissociation: during our research work we noticed that even when thorough assessments are performed by organisations – and that they know the Cloud Providers actually implement the measures (and that they are effective), a lot of organisations tend to dissociate themselves from their 3rd party, relying solely on Cloud Providers' security measures. Yet, it's their data and reputation that is at risk.

Thus, we believe that a shift to the cloud needs to be accompanied by a 'shift of mindset' through the implementation of strong, smart security behaviours. Adopting this mindset is the only way to optimise the use of cloud services and to allow organisations to benefit from their shifts without having to face potentially disastrous consequences.

As a result, we will use this question as the 'live wire' of our paper: "Why does cloud adoption require the development of a new security mindset ?"

01
Executive Summary

The top 4 conclusions from the synthesis of the survey inputs and results are:

① Information security is a 'leadership challenge.' Boards and Executive Suites need to 'lift their game' by adjusting and realigning the organisation's investments, priorities, policies and processes to be more reflective of the use of cloud technology and its unique risks.

② Organisations must accelerate their security and cloud-specific risk awareness programs to improve ineffective policy compliance so the organisation can more sensibly adopt cloud technology.

③ It is essential that organisations go beyond the simple responses of 'yes' to critical questions on essential security processes or controls, and begin to seek evidence that controls not only exist but are effective.

④ Even when organisations know that the measures implemented by their Cloud Providers are effective, they shouldn't rely on Cloud Providers' measures ONLY, especially for Disaster Recovery.

Each conclusion is described further on the following pages.

01

100 percent of the leaders interviewed are embracing the cloud, and 40% of their data in the cloud would be considered to be sensitive. They also indicated that they were planning on storing more sensitive data in the cloud moving forward.

While the use of the cloud is critically important and increasing, there was an overwhelming 'lack' of response to multiple questions asked on the use of 'innovative or unique' tools, techniques, or approaches regarding the 5 NIST functions: Identify, Protect, Detect, Respond and Recover.

Furthermore, 43% did not discuss cloud related risks at the board level. On average, participant organisations are using fourteen different Cloud Providers. While a significant portion (80%), have policies regarding the use of cloud resources, 32% believe the processes for compliance are not effective.

One might conclude that the organisation's adoption of cloud technology is too aggressive or too fast. However, given the business imperatives in today's COVID environment, we would suggest it is the organisation's alignment to the idiosyncrasies and unique challenges of the cloud which is too slow.

We often see that information security is a 'leadership challenge' and not an 'IT problem' – the purpose and priorities of an organisation get set at the top. As such, we suggest that **Boards and Executive Suites need to 'lift their game' to adjust and realign the organisation's investments, priorities, policies and processes to be more reflective of the use of cloud technology and its unique risks.**

The cost of inaction will be more data breaches, potential loss of sensitive data or intellectual property and greater risk of business interruption resulting in reputational damage to their brand.

02

As the concept of 'shadow IT'[4] has been around for some time, we were surprised to learn that cyber security training programs did not include cloud-specific modules; in fact, 64% of participants do NOT train their staff with respect to the use of the cloud or cloud-specific risks.

Organisations need to include cloud use/risks in their Cyber Security Awareness Programs. It is all about going beyond the "don't do it" mindset in order to create long-lasting behavioural change and to minimise the use of 'rogue' or potentially risky cloud services. Building '**Unconscious Awareness'** is the goal.

Organisations will continue to rapidly adopt cloud technologies; therefore, it is also clear that **organisations must accelerate their security and cloud-specific risk awareness programs to improve ineffective policy compliance so the organisation can more sensibly adopt cloud technology.**

Not doing so will result in an increased risk for organisations' business critical systems and sensitive data. Furthermore, in a COVID-19 Work From Home (WFH) environment, building understanding and awareness to remote distributed organisational structure becomes even more essential.

4. Shadow IT (also known as embedded IT, fake IT, stealth IT, rogue IT, feral IT, or client IT) refers to information technology (IT) systems deployed by departments other than the central IT department, to work around[1] the shortcomings of the central information systems (https://en.wikipedia.org/wiki/Shadow_IT)

03

We were impressed when we calculated the average response to find that organisations assessed a third-party Cloud Provider's security prior to engaging them as "most of the time" (1-5 scale. Most of the Time = 4. Average 3.94), and encouraged to learn that 85% would not engage with a Cloud Provider if they could not demonstrate they were undertaking secure approaches (some very clear implications for Cloud Providers!).

Yet, we quickly realised that there is a **'high trust - low proof'** situation where many organisations seem to be asking the questions, but to not seek proof or evidence that the answer is actually true. For example, 79% of respondents believe Cloud Providers have Incident Response Plans, yet 38% didn't know if the plans had ever been tested. Only 23% had ever been involved in a cloud Incident Response exercise. It was similar with Disaster Recovery – nearly all (89%) said their Cloud Providers have Disaster Recovery plans; yet only 30% knew if they had ever been tested. As Dwight Eisenhower said, "plans are worthless, but planning is everything."[5]

In a related finding, a majority of organisations encrypted data 'in transit' (84%), and well over half agreed that their Cloud Providers encrypt 'at rest' (60%). Yet, over half (54%) did not understand how encryption keys were managed, and 66% did not know whether their 'data in transit' technologies are using secure versions or ciphers.

Another saying is "What can be asserted without evidence can also be dismissed without evidence"[6]. As mentioned previously, 100 percent of leaders are embracing the cloud; 40% of their data in the cloud is sensitive, and they plan on storing more sensitive data in the cloud moving forward. **With this trend, it is essential that organisations go beyond the simple responses of 'yes' to critical questions on essential security processes or controls, and to seek evidence that they not only exist but that they are effective.**

History has proven that (particularly with technology) incidents occur, disasters happen, and the best intentions are a poor surrogate for independent validation of effectiveness. As the cloud becomes one of the most essential tools of the digital age, we must mature our approaches to assessments or accept the likelihood that an issue – some with significant consequences – will occur.

04

Although most organisations conduct assessments before engaging with Cloud Providers and can certify that their data is well protected, a lot of them tend to rely on Cloud Providers' security measures only for Disaster Recovery. Almost half of respondents do NOT have a Disaster Recovery Plan in place if they lost the availability to the organisation's cloud resources (45%). Even then, only 32% of those actually test the Disaster Recovery Plan. Participants also explained that they do log activity within their use of the cloud but don't perform active monitoring, relying on Cloud Providers' detection tools as well. Regarding authorised external access, some participants also rely on their Cloud Providers for access management and monitoring.

A large number of organisations are therefore putting their fate in their Cloud Providers' hands… but who's data and reputation is at risk?

Even though one of the advantages of the cloud seems to lie in the 'shift of responsibility', it is crucial to remember that no Cloud Provider is too big to fail – if something happens to your Cloud Provider and subsequently to your data, it's your data that is lost, and your reputation that's impacted. Therefore, it is important to remember that even though your data sits 'somewhere else', your organisation is better safe than sorry, and developing a Disaster Recovery Plan in the event of a cloud disaster could prevent you from becoming a headline.

5. https://quoteinvestigator.com/2017/11/18/planning/ 6. Hitchens's razor: https://en.wikipedia.org/wiki/Hitchens%27s_razor

02

Survey Results

by NIST function

IDENTIFY

One main behaviour was made obvious regarding the 'Identify' function. Not all questions were used to build this report. A few 'main answers' allowed us to identify behaviours regarding each function. We will display the questions that drew us to those findings.

① Cloud risks and policies are not always reviewed and understood at the executive or board level

Are cloud-related risks/policies defined at the executive board level?

Out of all the organisations that we interviewed for this survey, we realised that half of them were not defining cloud risks and policies at the executive level. This echoes to the old misconception that Cyber Security is an 'IT problem'. Yet, a cyberattack impacts an organisation as a whole. We are therefore convinced that cyber security and the challenges that it embodies – such as the shift to the cloud – needs to be seen as a leadership challenge. Boards need to be involved in the development of cloud-related policies, risks, compliance processes and overall strategy.

Another main finding was that most participants assess their Cloud Providers before engaging with them and wouldn't engage with a Cloud Provider if they couldn't demonstrate secure practices.

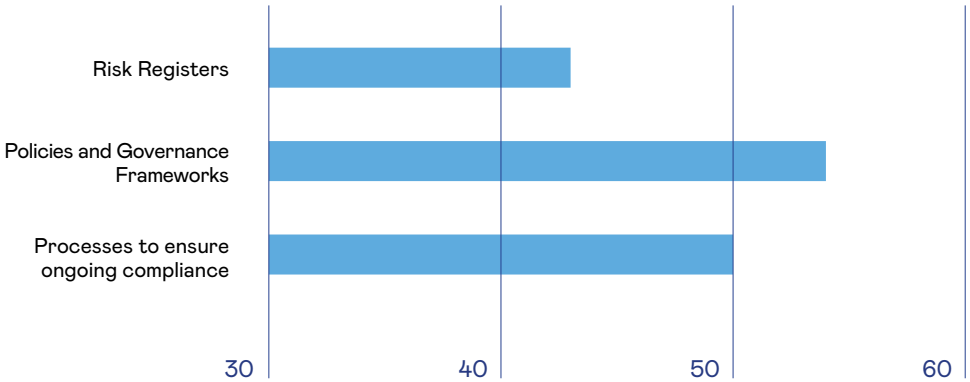
Are your Cloud Providers assessed for their security practices before you engage them?

This is very positive as 79% of participants said they assess their Cloud Providers before engaging them. When assessed, on average, 67% of Cloud Providers are using advanced security practices according to the participants.

However, as will be shown with other functions' results, risk assessments might need to be more detailed if organisations want to keep their sensitive data safe, especially because the amount of data stored in the cloud is ever increasing, according to participants and various studies on the use of the cloud.

IDENTIFY —— STATISTICAL ANALYSIS

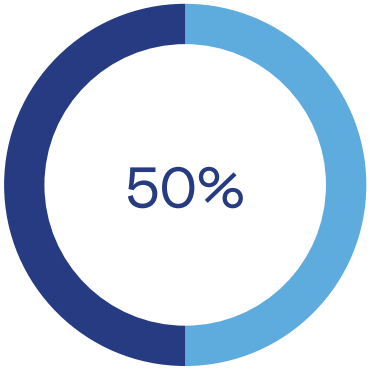
% OF ORGANISATIONS THAT HAVE CLOUD SPECIFIC...



Most participants are including cloud in their holistic risk registers, general policies and governance frameworks. This is very positive.

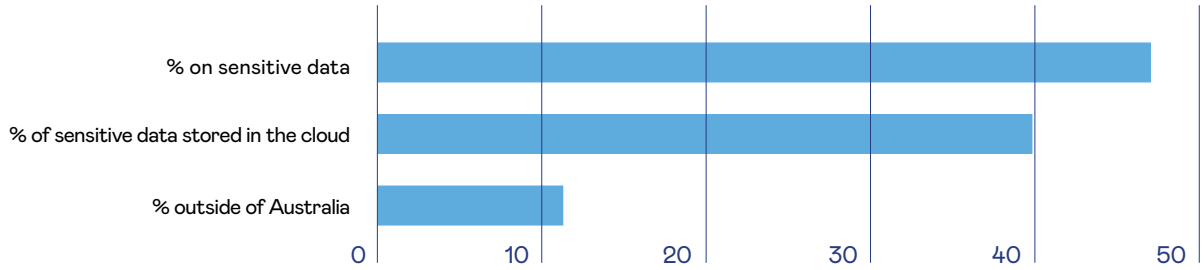
The average of 50% or less is due to the high number of participants saying they include cloud in their existing risk registers, policies, governance frameworks, as well as apply their requirements to the use of the cloud (a rating of 5 out of 10 was given to participants that said they include cloud in their general risk registers, policies and governance frameworks).

% OF ORGANISATIONS THAT DEFINE CLOUD RISKS AT THE BOARD LEVEL



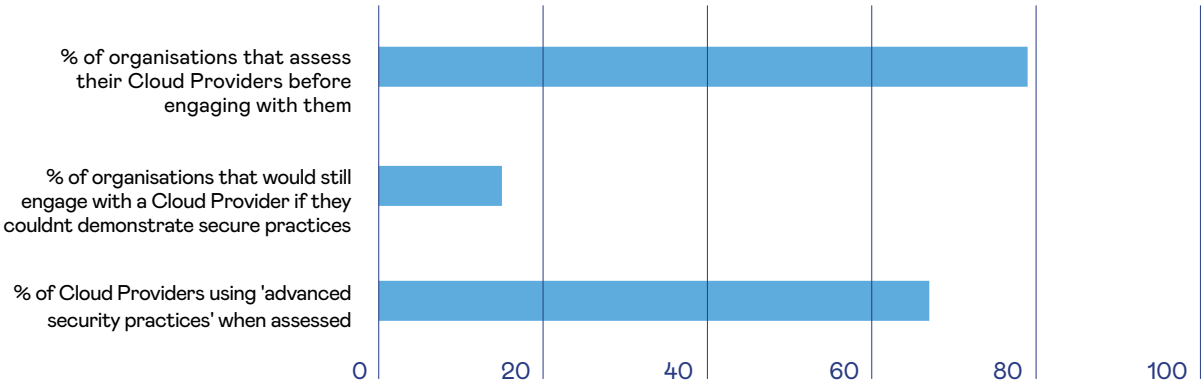
However, cloud risks and policies are not always defined at the board level. In fact, only half of participants agreed that the executive level was involved in the development of cloud-related policies, risks, compliance processes and overall strategy.

UNDERSTANDING OF SENSITIVE DATA



The results also showed that a significant percentage of organisations' data is sensitive (47% on average) and that a large part of that is stored in the cloud (40% on average). A relatively small amount of this data is stored outside of Australia (13% - most answers were around 0%, the results being amplified by some participants using 1 or 2 Cloud Providers only, all storing in the US for instance).

Most participants also agreed that they were highly aware of sovereignty regulations, explaining why they are not storing anything outside of Australia or trying not to.



Finally, 79% of participants said they assess their Cloud Providers before engaging with them. When assessed, on average, 67% Of Cloud Providers are believed to be using advanced security practices (rating: 'little to no' security practices / 'some' security practices / 'advanced' security practices).

On top of that, 85% of participants would not engage with a Cloud Provider if they couldn't demonstrate secure practices.

PROTECT

Two main findings were identified regarding the 'Protect' function.

② Staff are not adequately trained regarding cloud risk, but an organisation is only as safe as its weakest link.

Is all organisation staff trained with respect to the use of the cloud or cloud-related risks?

Most participants replied that their staff was not trained regarding cloud-related risks. At best, cloud was included in 'Cyber Security Awareness' training modules, at the very high level. However, users need to be trained with respect to shadow IT and cloud use best practices.

③ Because most organisations perform risk assessments (cf. identify function) most of them seem to be quite aware of the security measures implemented by their Cloud Providers. The ratings are also quite good regarding the percentage of Cloud Providers implementing those measures (according to the interviewees). However, we realised that most organisations don't seek evidence that the security measures implemented by their Cloud Providers are effective.

This finding comes from the relatively high number of 'Unknown' answers regarding the implementation of security measures by the Cloud Providers. Therefore, it is safe to say that a fair number or participants tend to put too much trust in top-tier Cloud Providers. Yet, no Cloud Provider is 'too big to fail'. On the other hand, when it comes to a smaller Cloud Provider, its failure can be extremely crippling depending on the type of data being stored. Hence, after gathering data from 30+ industry leaders, we realised that an important number of participants knew their Cloud Providers were protecting their data at rest but had a poor understanding of the key management processes.

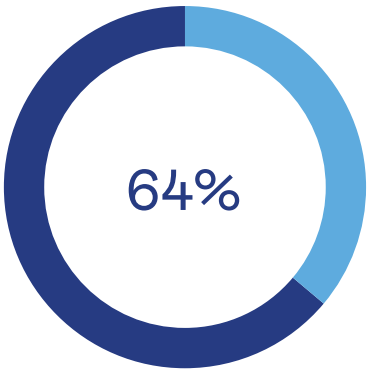
Furthermore, by looking at the survey as a whole (indistinctively of functions), we realised that a high number of participants agreed that their Cloud Providers had an Incident Response Plan and Disaster Recovery Plan but didn't know if the plans had ever been tested. In fact, most of the participants that didn't know if the plans were tested said they assumed Cloud Providers would do the right thing.

This led us to conclude that there is a 'high trust, low proof' mindset when it comes to Cloud Providers. Therefore, when performing a risk assessment, we recommend to seek evidence that the security measures implemented by the Cloud Providers are effective and that their plans are tested.

This reinforces the idea that organisations need to develop a more detailed risk assessment before engaging with a Cloud Provider.

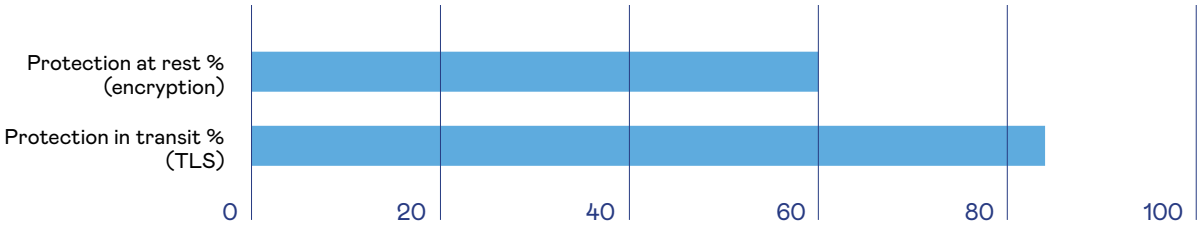
PROTECT —— STATISTICAL ANALYSIS

% OF ORGANISATIONS WHERE STAFF ARE NOT TRAINED WITH RESPECT TO CLOUD USE/RISK



More than half of the organisations that we interviewed (64%) indicated that their staff were not trained with respect to cloud use/risk. In addition, most of those that said their staff were trained agreed that cloud was addressed at the 'high level' only.

Aside from the lack of training, the ratings are quite good regarding the measures implemented by both organisations and Cloud Providers in order to protect sensitive data:



60% of participants said their sensitive data is protected at rest. 84% of participants said their sensitive data is protected in transit. However, if we go further in precision:

- Organisations tend to have a poor understanding of the encryption key management processes and/or assume it's done well: only 36% of participants went to the effort to understand the cloud providers processes.
- 66% don't know whether their 'data in transit' technologies are using secure versions or ciphers.
- 40% said that they don't know if their data is protected at rest, or know it isn't.

This echoes to the 'high trust, low proof' mindset: some organisations still assume that their Cloud Providers do the right thing, especially top tier Cloud Provders.

DETECT, RESPOND & RECOVER

Finally, one last behaviour was identified, encompassing the Detect, Respond and Recover functions but also echoing the 'Protect' function.

④ Even when a thorough cloud security assessment is done (cf. Identify function), and organisations know that their data is well protected (cf. protect - statistical analysis), they tend to rely on Cloud Providers' security measures for Disaster Recovery.

- This was made evident by the fact that an important number of organisations indicated that they are not implementing a Disaster Recovery Plan related to potential cloud disasters (*Does your organisation have a Disaster Recovery Plan in-place if you lose 'availability' of cloud services or data?*).
- Participants also explained that they do log activity within their use of the cloud but don't perform active monitoring, relying on the Cloud Providers' detection tools. Regarding authorised external access, some participants also rely on their Cloud Providers for access management and monitoring (Do you log/monitor access or activity with YOUR use of Cloud Providers? / Do you manage/monitor external authorised access to your cloud services?)
- On top of that and referring to finding ③, a large number of participants indicated that they didn't' know if their Cloud Providers were testing their Incident Response Plan/Disaster Recovery Plans.

As stated before, even though there are various ways to make sure that your Cloud Provider is doing the right things (performing a risk assessment, not engaging with a Cloud Provider that cannot demonstrate secure practices…), there is no guarantee that this Cloud Provider will not be attacked or will not fail at some point. Hence, it is crucial for organisations to maintain some kind of proactivity in the way they use the cloud and implement their own security measures, whether it relates to protection (managing and monitoring 3rd party access, understanding the key management processes or even using your own keys) or detection (monitoring suspicious behaviour within you use of the cloud trough the implementation of detection tools).

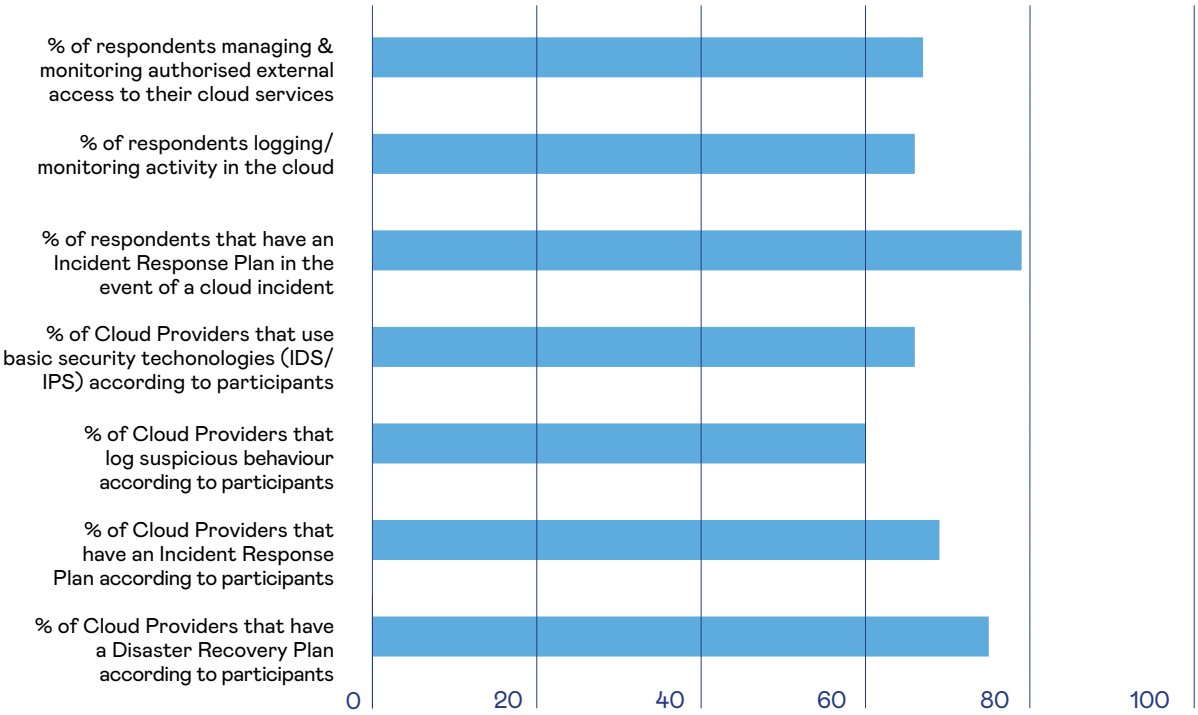
Organisations should also consider their cloud-based assets when developing a Disaster Recovery Plan / Business Continuity Plan, and exercise those plans (including your Incident Response Plan). The goal is to be able to make the most out of the cloud – the shift to the cloud can be an incredible adventure if it's done properly.

<u>Additional finding</u>

Most organisations would be able to recover within days/weeks if they lost all their cloud data. The main issue according to the participants wouldn't be the loss of data but the loss of availability of the service. One of the most crippling losses would be the failure of Office 365. This shows that even if we can prevent loss of data availability, some organisations would still struggle to find an alternative in order to 'replace' a service, if a major Cloud Provider like Microsoft was to go down for a long period of time. Furthermore, if Microsoft went down, which clients get priority in the recovery queue to restore services? Therefore, the loss of a service's availability, along with data confidentiality & availability, is also something that needs to be taken into consideration when developing a cloud-related Businesss Continuity Plan.

6. https://www.thenonprofittimes.com/npt_articles/blackbaud-faces-class-action-lawsuit-after-data-breach/

DETECT, RESPOND, RECOVER —— **STATISTICAL ANALYSIS**

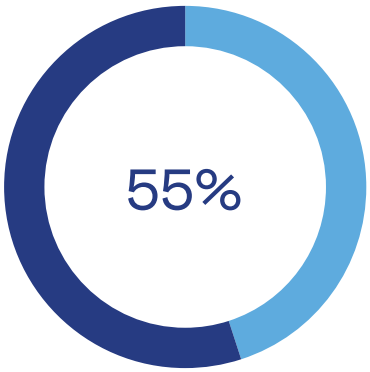


As mentioned earlier, the results for the 3 functions are quite good: most organisations have an Incident Response Plan in the event of a cloud incident (79%) as well as test their plans (80%). More than half (66%) also log and monitor activity in the cloud as well as manage and monitor authorised external access (67%). Cloud Providers also implement strong security practices according to participants: 69% are said to have an Incident Response Plan and 75% to have a Disaster Recovery Plan. Participants also said 60% of their Cloud Providers log suspicious behaviour and 66% use basic security technologies such as Intrusion Detection System (IDS) or Intrusion Protection System (IPS).

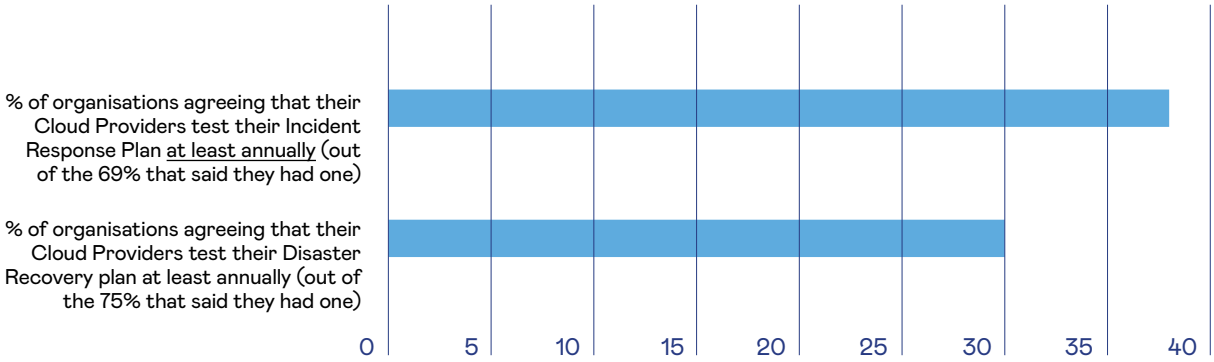
However, even though a high percentage of participants log activity within their use of the cloud, most of them indicated that they do not perform active monitoring and are still relying on the Cloud Providers' detection tools.

Finally, quite a few organisations still rely on their Cloud Providers only for Disaster Recovery. In fact, almost half of respondents (45%) do NOT have a Disaster Recovery Plan in place if they lost access to cloud resources. Furthermore, among those that DO have one, only 32% tested them regularly.

% OF ORGANISATIONS THAT INCLUDE CLOUD DATA IN THEIR DISASTER RECOVERY / BUSINESS CONTINUITY PLANS



Additionally, echoing finding #3, a high number of participants indicated that they don't know if their Cloud Providers are testing their Incident Response Plan/Disaster Recovery Plans: almost 3 quarters (69%) of respondents believe Cloud Providers have Incident Response Plans, but only 38% know (if) the plans are tested. Moreover, only 13% have been involved in a cloud Incident Response exercise. It's a similar scenario with Disaster Recovery – 75% believe Cloud Providers have Disaster Recovery Plans in place, but only 30% know if it has ever been tested – even then, less than 1/3rd have ever seen a copy or evaluated the effectiveness.



These results reflect once again the 'high trust, low proof' mindset around cloud use.

03

Interesting Inputs

There was an overwhelming 'lack of response' to the question of innovation or interesting things being done in the cloud – when asked, 50% were not able to identify anything they considered to be innovative. However, those that did, provided some insights into what can be done to 'jump to the cloud' in a safer way.

IDENTIFY

In order to better identify their sensitive assets, some participants are:

- Using centralised login in order to minimise the number of login pages / entry endpoints. On top of making application access smoother, it also minimises the risks of exposing credentials.
- Analysing proxy logs in order to see where staff upload/download data to/from.
- Using discovery scans and conducting periodic reviews of user access.

PROTECT

In order to better protect their sensitive assets, some participants are:

- Implementing their own key management processes: one of the interesting inputs we gathered during the interviewing process was the idea of a '"Bring Your Own Device"' key. Making sure that your encryption keys are separate from your Cloud Providers is a good way to maintain control of encrypted data. This way, you will have a full understanding of the key management processes and will be able to make sure that your data is well protected.
- Using a cloud access & security broker (CASB), with an agent on every endpoint in order to monitor user behaviour.

DETECT & RESPOND

In order to better detect suspicious behaviour in the cloud, some participants are:

- Using detection tools (threat hunting tools) to detect anomalies and Shadow IT.
- Developing in-house vulnerability management tracking systems.
- Using Artificial Intelligence tools to detect anomalies & bots for internal scanning (anomaly behaviour).

RECOVER

In order to better recover from a cloud disaster, some participants are:

- Implementing 'on-prem backups': A great insight regarding the Recover function came from a participant explaining they had on-prem backups synced to their cloud services to maintain availability of their data if a Cloud Provider was to fail.

> "Because it's not only about finding what's not being done right... But highlighting good or leading practices."

04

The Way Forward

What now?

As explained in the preface, the cloud is attractive for many reasons: you can access your data from anywhere (this is especially important in a 'working from home' perspective), scalability, reduced IT cost, collaboration efficiency and flexibility, high performance processing... the list goes on and on.

Furthermore, our study highlighted that most organisations are aware of the risks that migrating to the cloud can represent. One of the positive aspects of the study was that most participants are highly aware of sovereignty regulations and have an 'Australia only' storage policy for sensitive information. It was also positive to learn that most organisations conduct 3rd party assessments before engaging with a Cloud Provider and would not engage with them if they could not demonstrate secure practices.

However, as organisations shift to using a range of different Cloud Providers for their core systems and information, it's essential they maintain the same high standards for these Cloud Providers, as they would if they were providing this service themselves.

Why? At the end of the day, when your critical systems or business-essential information is not available; when sensitive customer data is lost, or confidential information and Intellectual Property is exposed or exploited, it is not the Cloud Provider's reputation that is impacted, but yours.

Hence, it is not necessarily a bad thing to 'hope for the best', but it seems necessary to also 'prepare for the worst'. The goal is not to scare people or to depict the cloud as an enemy of security, but rather to help organisations implement a safe cloud-migration strategy.

Make sure you don't outsource your reputation to the cloud and perhaps someone who is less concerned about it than you.

05

Recommendations

If you are wondering how to more safely migrate to the cloud, here is a quick checklist that can be used by any organisation that wishes to strengthen their cloud security posture. The following are nine important considerations to create your "CLOUD 9"!

1. Do you know where your information assets reside? If you don't have one, create an Asset Register and assess whether any of that information resides in Cloud environments. **Knowing what you have, and where**, is the first step towards being able to protect it. Don't forget to include any 'development or test' environments as well if they hold sensitive information (many do).

2. Consider creating a '**cloud protection matrix**'. First, rank your Cloud Providers in order of importance (prioritising along the lines such as; holding sensitive information, what it does is fundamental to the main operation of your organisation, and the impact if you couldn't get access to those resources). Then, for each 'column', enter the functions of 'Protect, Detect, Respond and Recover' – go through each cell in that matrix to make sure you've got them all covered.

3. Assess your high priority Cloud Providers (from above) and ensure that Multi-Factor Authentication (and similar logout/lockout functionality) is enabled for ALL users. No excuses; our experience shows the (severe) risk of credential stuffing is easily mitigated with these relatively simple measures.

4. Obtain evidence that key cloud security measures (in particular Disaster Recovery) are effective. A plan is just the start – 'planning' is the key – make sure they're tested and working effectively.

5. Review your Risk Registers to make sure you have **clearly articulated cloud-related risks** around confidentiality, integrity, and availability of your systems and the information that reside there. Make sure these risks are elevated and discussed at the right level in the organisation (e.g., the Board of Directors).

6. With the insight of an Information Asset Register, assess useful technology solutions (i.e., Cloud Access Security Broker (CASB)) that can **manage and monitor** access to these assets. Don't just have these systems generate 'logs', but define a number of 'abuse cases' across disparate pieces of the technology/cloud supply chain and set up monitoring **and alerting** for triggered events.

7. Develop clear employee policies and processes around the use of Cloud assets. Don't just define the policies and processes – actively engage your staff via an ongoing and iterative **education/awareness** program that highlights their role in protecting the organisation's assets and use of cloud resources. Remember not to simply 'preach' the rules, but educate and empower your staff to make the right decision(s). Don't forget, making lasting change requires reinforcement – once is not enough – **reiterate this training** on a regular, recurring frequency.

8. In our experience, one of the weakest areas of the use of sensitive information and cloud resources is at the **Board of Director's** Level – **make sure Policies, Processes and Awareness are tailored explicitly to this key audience** and ensure they aren't storing and/or emailing sensitive information using public email services such as Gmail, Hotmail, or Yahoo.

9. Make sure you have an **Incident Response 'capability'** that also reflects your cloud assets – relying on your Cloud Provider is not enough. The first step is to ensure your Incident Response Plan reflects your ability to Respond and Recover cloud-based assets if required. Then, ensure it reflects the assets that reside in the cloud in the event of confidentiality and integrity issues (not just availability). Finally, do the most important part; 'practice' an incident (with cloud-related assets) to ensure your plan is practical and reflects the reality of cloud assets.

About Trusted**Impact**

Trusted**Impact** is a boutique consulting firm with a singular focus in Information Security. We provide advice, guidance and insight to enable clients to achieve their business objectives, while protecting the flow of their important information from unauthorised access, use, disclosure, disruption, modification, theft, or destruction.

Information security is all we do – we're focused specialists with a unique combination of expertise spanning Cyber Risk & Strategy, Cyber Awareness/Culture Change, and in-depth technical skill. One size does not fit all in security, and thus, we tailor our advice to align with the unique risks and business environment of our clients.

We're also an independent consulting firm with no financial affiliation with 'downstream' technology products or managed services. Our business model is focused entirely on what our clients need to do to safely or securely succeed in the digital era across all aspects of 'people, process and technology'.

Finally, we recognise that security is a business challenge. We're seasoned security professionals with business nous to better position our clients for their growth and success. This 'business driven context' means our advice and recommendations are uniquely practical; they reflect your business situation and integrate well into your day-to-day operations. Simply stated: **Tailored. Independent. Outcomes.**

About The Author

Charline Quarrè studied History and has a Bachelor's Degree from the University of Toulouse, France and a Master's Degree in Strategic Studies, Security and Defence policies from HEIP Paris - School of Advanced international and Political Studies. After her first experience at the Department of Home Affairs in France, she relocated to Australia and joined the Trusted**Impact** team as a Research Analyst. With a strong desire to participate in the defence of Australian organisations as well as having an appetite for the analysis of the 'human factor' in cyber security, this naturally led Charline to drive the 'SecureThinking' area at TrustedImpact.

A number of other Trusted**Impact** professionals assisted in the creation of this whitepaper who should be noted; namely; Darren Arnott, Tom Crampton, Sairam Jetty, Jim Karvounaris, Ed Latter, Genio Maiolo, Geoff Rasmussen and Demetrios Stoupas.

TrustedImpact
PROTECTING DIGITAL

Level 9, 22 Albert Road,
South Melbourne VIC 3205
+61 (0)3 9023 9710

trustedimpact.com
Twitter: @trustedimpact
LinkedIn: linkedin.com/company/trusted-impact