MIND THE SECURITY GAP

Microsoft Partner | Gold Cloud Platform

Microsoft

**Rackspace study**

Closing the communication gap around security & digital transformation

*rackspace.*

# Why the board and it decision-makers must work together to 'mind the security strategy gap'

*Many companies are investing in implementing a cloud strategy as part of their digital transformation plans in order to realise increased scalability, efficiencies and drive innovation. IDC predicts that by 2021, enterprise spending on cloud services and cloud-enabling hardware, software, and services will reach more than A$9.8 billion, with more than 65% being multi-cloud.*

**95% OF CIOs** EXPECT CYBER-THREATS TO **INCREASE** OVER THE NEXT **THREE YEARS**

Boards and IT decision-makers (ITDMs) are aware not only of the immediate benefits of the cloud but of the long term commitment to network maintenance and security that needs to be considered as part of any cloud strategy. According to a Gartner 2018 Cybersecurity report, 95% of CIOs expect cyber-threats to increase over the next three years. In fact, while businesses are feeling the pressure to move fast to implement cloud, they know that proactively tackling the security risk associated with common breaches is not only a nice to have, but an imperative. A severe breach could result in hefty government fines, especially since the introduction of the Notifiable Data Breach Regulations and GDPR, and long term reputational damage.

In October, 2017, media widely reported the data breach of an Australian Defense government contractor, which allowed hackers to get their hands on commercially sensitive data including details about new vessels being built for military use. The long term impact of a breach has yet to be determined and it serves as a reminder of the IP, customer data and reputation at stake for many businesses.

Despite cybersecurity being front of mind for board members, many admit they do not have a strategy to tackle the 'how, what, where and why' questions related to data protection. Through various sources, it is clear that the vast majority of board members acknowledge cybersecurity as a key priority, however the presence of a supporting strategy remains less evident. Also, whilst phishing attacks still account for a high percentage of successful exploits, staff training and awareness across businesses appears haphazard. Arguably, against the backdrop of such atmospherics, there is still a gap between widespread boardroom acknowledgement and meaningful action.

In this eBook we will discuss why this is the case. We will explore the challenges of communicating with the board, present and future organisational priorities and the skills disconnect – the looming gap – that exists, and is widening by the day. This not only exists in the form of a communication gap that prevents CEOs, CIOs and ITDMs from agreeing on realistic timelines and expectations, but also around priorities: today's legacy and modernisation needs vs tomorrow's digital transformation requirements. Lastly, the burgeoning skills gap is, in itself, a threat to cybersecurity strategies. Combined, these are making it increasingly difficult for businesses to proactively monitor and put in place a strategy to tackle cybersecurity risk.

*It's a gap that businesses need to mind. Pride they say, goes before a fall, **cloud security before a gap.***

A PROACTIVE RISK MITIGATION STRATEGY WILL HELP ITDMS TO SLEEP BETTER AT NIGHT

# A multi-layered and proactive cloud strategy is the key

*In the three parts of this eBook we will outline why the board and ITDMs need to work together to strategically plan, review and implement the process, technology and skills needed to ensure their business is cloud-centric. This should be a business, not simply cloud strategy, directed by the board and based on aligned expectations. That means speaking the same language and truly understanding the challenge.*

The IT department will need to immerse themselves in the language of business, to be able to accurately tackle the myths and misaligned expectations that remain around data and security at the board level.

And, they will need to demonstrate proactive leadership – both in putting in place the right risk mitigation strategies, assessment tools and technologies and in choosing the right managed cloud services partner to help them do so. In the event that an attack happens, you want a partner than can ensure that the breach is detected, isolated and shut down within hours – not days - to ensure damage limitation.

A proactive risk mitigation strategy will help ITDMs to sleep better at night and ease the IT team's admin and work burden. They will thereby be better empowered to focus their energy on strategies that go beyond simply 'keeping the lights on.'

# Tackling the expectation and communication gap

*Board members understand that they are fully accountable to shareholders should a security breach occur. They know that hefty fines from breaches could not only eat into the bottom line but also threaten their position at the company. It has not been unknown for board directors to step down due to such an occurrence. As explained by Steve Durbin, managing director of the Information Security Forum (ISF) in an interview with CIO magazine this year, "The board, as a rule, does get it. It understands it is operating in cyberspace. What it doesn't understand, in many cases, is the full implications of that."*

The first time the board considers the full implications of a breach, shouldn't be right before the press conference. In fact, findings from a 2018 ISF research report reveal that misalignment between the board's expectations and reality of the IT function's ability to deliver results against them, constitute one of the most prevalent cyber-security dangers. To overcome this challenge, analyst reports from Gartner confirm that the board is apportioning larger budgets to support security detection and response capabilities. However, growing budgets and heightened board-level concerns will not always lead to the prevention of an attack. Simply hiring more people to address security risk is not always the solution.

While the board must take accountability where it should, it is for the ITDMs to anticipate and proactively communicate their plan around mitigating security risks. To do so, they must be able to speak the language of business so that the right objectives and key performance indicators (KPIs) are set in agreement with the board. If this means slowing the speed of the overall digital transformation strategy so that it is implemented with risk mitigation as a key priority at the outset, then this should be communicated in a way that 'sells' this advice. A focus on a multi-layered, gradual move to the cloud will often ensure that the right people, processes and technology are in place and aligned with the risk mitigation strategy –going beyond simply making sure that the firewall is up.

ITDMs must also clearly outline to the board that it is not a matter of 'if' a breach may occur, but in fact, when it will. Their risk management strategy should then not only tackle the prevention of breaches but also the incident response process in order to limit the scope of such an attack. Additionally, regular reporting on the status of implementation of any security strategy will ease communication on both sides, helping to proactively address any board concerns and limiting the amount of 'surprise' thoughts or opinions during the journey to the cloud. The reports should be concise, clear and data driven and measure performance against clear KPIs.

In reality, doing the above sounds straightforward but with many different board objectives and priorities, it can be a challenge. Working with partners to plan for a risk mitigation strategy will help ITDMs to step back and truly adopt the role of consultant and trusted advisor.

Ultimately, this will empower them to have the conversation before an attack has taken place.

> **The board, as a rule, does get it.** It understands it is operating in cyberspace. What it **doesn't understand,** in many cases, is the **full implications of that."**

**500 ITDMS**
ONLY A MINORITY **(43%)**
ARE TOTALLY **CONFIDENT** THAT
THEIR **SECURITY PROCESSES**
ARE UP TO DATE

# Minding the gap between today and tomorrow's business priorities

*The threat landscape is clearly evolving. Not only are hackers finding new ways to break security systems but they are doing so at an alarming and ever-increasing pace. The moment one new method is identified, another equally challenging way to hack into a system crops up. And, attacks can come from a range of sources, from a foreign entity trying to steal IP to someone working for another company or even a former employee.*

Keeping on top of these threats is not just an exercise in being organised, well-resourced and well-funded. It also requires creativity. ITDMs must find a way to stay, consistently, ahead of the attacker.

However, many ITDMs are unable to deliver a proactive risk mitigation strategy because they are still focusing on immediate challenges such as modernising legacy systems. A 2018 Vanson Borne survey found that out of 500 ITDMs only a minority (43%) are totally confident that their security processes are up to date.  This means that when a security breach does

happen, it takes – according to a Marsh and McLennan report - on average, 99 days for the team to detect it.

Regardless of the pressures ITDMs face from today's immediate demands, tomorrow's concerns should not be deprioritised or they will sneak up and catch the business unaware. To plan for a future looking risk mitigation strategy, they should involve different stakeholders from the outset (the board and different departments) and, where possible, devolve and empower others to act in a proactive fashion. This is because many IT teams simply don't have the resources or skills to proactively spot and track an intrusion and raise an alarm quickly, for instant response and mediation to be able to limit the scope of a breach.

# Provisioning for the skills gap

*The threat landscape is evolving quickly and businesses can barely keep up. As previously mentioned in this eBook a security breach is inevitable. However, it is how companies manage that breach that will dictate the impact on its reputation and the scope of the damage. Having the right resources to hand to manage an incident helps to implement a strategy. However, it is not the panacea to a business' security strategy issues.*

With a large and widening skills gap, it is difficult for ITDMs to adequately resource and scale up incident response teams without taking members off other important projects. Gartner's 2018 cybersecurity report reveals that "skills challenges continue to plague organisations that undergo digitalisation, with digital security staffing shortages considered a top inhibitor to innovation." The skills gap not only concerns the board but puts equal amounts of pressure on capacity strapped IT teams. Many businesses feel that they have two options: to either up-skill the workforce or out-task the work.

In trying to grow the skills in-house, many ITDMs are starting to feel like they are growing 'jack of all trade' talent within the business. Trying to be an expert at everything is exhausting, not only for those who are asked to perform such a task, but also by those who manage them – when, inevitably knowledge gaps do appear.

From a security strategy perspective, the key to success is to find the right expertise either within the business or externally that specialises in a proactive form of monitoring for attacks. Experience in identifying weaknesses in the network and reading strange anomalies that could signal a possible breach. It is not always easy to spot these anomalies – they will likely include activities that could appear normal. A more advanced attacker, who has bypassed security controls and technologies, attempts to pivot and move laterally across networks to get to an objective making it harder to trace his/her 'presence'. In this scenario it is vital to have the right level of expertise that understands an attacker's mind-set, tactics,

techniques and procedures (TTPs) in order to detect, identify and respond to suspicious behaviour. No longer can security teams rely solely on pre-configured rules on devices and wait for static alerts.

As already stated, having the manpower to respond to an alarm, once it is raised, is not the same as having the knowledge or strategies to deal with it. But there is hope. In addition to working with the right partners, the right connections, best practice and knowledge sharing across industries can help create strategic partnerships for businesses to 'mind the skills gap.' For example, partnering with universities can enable businesses to hire bright young talent that can be taught a proactive 'mind-set' for building a secure environment. Alternatively, working with vertical sectors known for their security best practice – such as the military – can help businesses to gain knowledge from some of the best and brightest in the field and set a high bar for security strategies.

*Many businesses feel that they have **two options:** to either **up-skill** the workforce or **out-task** the work.*

# An expert guide

*The right partner can take on this burden whilst also helping ITDMs to carefully assess the threat landscape in which their business performs, understand their threat 'footprint' and how this could evolve over time, aligned with the implementation of new cloud technologies. This information should help the business to establish a risk mitigation strategy that could encompass a number of tactics, optimised for specific business challenges. The right tactics, should clearly define roles and responsibilities in the advent of a breach, helping to vastly reduce the scope and damage that the breach could cause.*

Looking externally for help from trusted experts in the industry should not be seen as a weakness. Industry knowledge and best practice on this topic is limited. For example, it is hard to learn lessons from businesses who have suffered a breach already – many companies would be hard pressed to talk about an incident. Managed cloud services providers have had the opportunity to work with many different companies in different industries to tackle a range of security threats – they are a source of information and expertise that cannot be ignored. ITDMs should stop trying to 'do it all' and stop asking their workforce to be the experts in every area.

# A security first, multi-layered cloud strategy will best ensure risk mitigation

*A proactive multi-layered security strategy is important for every business to help them protect against, and react quickly to, the inevitable security attacks that will come from evolving external security threats and growing internal weaknesses.*

This needs to be made a business priority and really a business strategy, understood by the board and created in agreement with the ITDMs. To navigate the inevitable miscommunications and misaligned expectations surrounding such an ask, ITDMs need to better understand how to speak business language, and put timelines and processes in place that will communicate what the key deliverables are and how they align with business objectives.

A risk mitigation strategy devised with the right managed services provider will enable the

business to tackle both today and tomorrow's priorities, proactively monitor for, alert and remediate breaches, and help to bridge the skills gap caused by the increasing dearth in talent. This should be supplemented by long term industry partnerships that will help to grow tomorrow's talent and share best security practice across industries.

Ultimately, security is about protecting the digital environment. A security first approach will protect the business and ensure that both the knowledge, people, processes and technology is in place to be able to proactively prevent or remediate breaches quickly.

For more information, go to
www.rackspace.com.au/security

or visit the below link:

Selling your cloud migration

# Working with Rackspace

*At Rackspace,* **we look at the outcome** *you're trying to achieve rather than the problem you're trying to solve. We do that through an operational lens so* **we jointly own the outcome with you.**

Whatever you want to do with your cloud, our certified experts have probably done it before. When you put Rackspace to work running your clouds, you don't need space for even one more seat. We architect, migrate, secure and operate your cloud – and continually help you optimise it for tangible business results.

Our Fanatical Experience is the results-obsessed customer service and deep technical expertise that's been part of our DNA since 1999. It's at the core of what we do — it drives our business. We're fanatical about your success, and we'll go above and beyond to support your business around-the-clock.

**rackspace**®

Microsoft
Partner

Gold Cloud Platform

Microsoft

Sales: 1800 722 577
Support: 1800 421 267

www.rackspace.com.au