three

issue 06

Latrobe Health Services

Sustainability

ServiceNow and SIAM

Spotlight on Jaco Olivier

When it's right to retain

Sentinel review

SDM value

Finding the right partner who combines the best technical skills with an understanding of your business outcomes and a committment to continually redefine service can be challenging ...

Luckily, there is AC3.

AC3

> “Without great people behind making good decisions based on great data, none of this would have happened. We really appreciated all of AC3’s people and all the Laybuy developers and engineers that have contributed to our system.”

- Justin Soong
Chief Technology Officer
Laybuy

ac3.com.au/resources/laybuy

aws partner network
Premier
Consulting
Partner

Contents

AC3

GENERAL MANAGER OF CUSTOMER EXPERIENCE & ALLIANCES
Stephanie Challinor

MARKETING SPECIALIST
Michaela Higham

Level 7, 477 Pitt Street, Haymarket
NSW 2000 Australia
+61 2 9199 0888
info@ac3.com.au

(niche:)

MANAGING EDITOR
Madeleine Swain
madeleine.swain@niche.com.au

PRODUCTION
Production coordinator
Jessica Appleton
jessica.appleton@niche.com.au

DESIGN
Editorial design and digital prepress
Norsham Husaini

CHAIRMAN
Nicholas Dower

MANAGING DIRECTOR AND GROUP PUBLISHER
Paul Lidgerwood

FINANCIAL CONTROLLER
Sonia Jurista

Stock images via Pixelbay, Unsplash

Printing
Southern Impact

Three is a publication
of Niche Media Pty Ltd
ABN 13 064 613 529
15 Paran Place, Glen Iris, VIC 3146
T (03) 9948 4900 F (03) 9948 4999

All unsolicited material should be addressed to the attention of the editor at the address above. Material will only be returned if a postage prepaid self-addressed envelope is supplied. Niche Media Pty Ltd accepts no liability for loss or damage of unsolicited material.

Welcome to Three

Secure by design. It's not a new concept, but it's becoming more and more present in every conversation we have and everything we do. No longer is cyber security an afterthought, but rather a bedrock of any business solution. In this issue of *Three* magazine, we focus on this theme.

From products to automation to governance, you will find valuable insights to help you secure your business. In addition, with such an evolving talent market in the cyber security space, you will find a profile on one of AC3's newest cyber security recruits, joining the workforce as a graduate. Bringing new talent into this field is crucial and he shares his top tips on getting started. Happy reading.

Stephanie Challinor
General Manager of Customer Experience & Alliances

Help where it's needed

The subtle trend towards businesses transforming their IT functions to becoming service providers is understandable, but is it right for your organisation?

By Simon Xistouris, CEO, AC3

Our industry is a rapidly evolving one. And as the technology evolves and progresses, so do the models that we adopt to support business growth. Sometimes these developments are cyclical and sometimes they take us in whole new directions.

Lately, I have noticed a subtle but noticeable shift in our customers transforming their internal IT function to becoming service providers for their own business. I've seen this in both smaller and larger organisations, and adopting this model appears to be prompted by a desire to leverage price, skills or capabilities.

It's important to note that this model may work for some, but it isn't right for everyone. It may seem as if there is a better business case for internal service providers, but the reality can be quite different. Customers at the smaller end of the scale are more likely to lack the specialist knowledge required to support their businesses. They are more likely to be time-poor or stretched for resources. They are also far less likely to have the ability to attract staff with the level of expertise they need. An external managed service provider can more easily address each of these concerns or issues.

But what about larger organisations? Their needs are different, but will also benefit from external resources. Larger customers need scale and deep expertise, and to cover a broad surface area, so using a managed service provider can fill all these gaps.

By shifting to a service provider model, whether internal or external, it gives the IT department the ability to improve its business intimacy and focus on what's most important, providing an outcome to its end customers, whoever these may be.

There are some benefits to using an external service provider that cannot be addressed by an internal provider. These include combating the current skills shortage, as well as managing the quality of the service.

An external provider brings the assurance of governance via the contract, compared to internal OLAs (operational level agreements). Contracts allow for the introduction of SLAs (with financial penalties for non-compliance) covering the most important aspects of the business, with the knowledge that the provider is contractually aligned to those objectives.

It allows businesses to focus on their core and priority services and let go of the less valuable and more commoditised functions.

It's important to remember that using an external provider does not, and should not, mean it's an all or nothing affair. Retaining the core functions like strategy, governance and service management in-house, while outsourcing functions such as cloud or security, can be a sensible division of tasks.

At AC3, we have seen customers adopt this model both in part and in full; for example, engaging specialists solely for specific streams like EUC (end user computing) or security, or bundling each stream together and engaging providers to supply the entire service.

Whichever path is best for your business, it's vital to understand the specifics of what is important for your business and set clear, measurable parameters for success. What does that look like? Is it financial? Performance? Or both?

Finally, always ensure to obtain the best legal advice. A good lawyer will create a contract that delivers on the required outcomes, but is also fair, to provide the right conditions for the supplier or partner to be successful.

SECURITY STATISTICS

Cybersecurity numbers snapshot for 2022.

93%

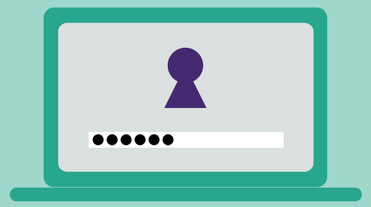
Cloud usage is now at 93 percent in organisations around the globe

SOURCE:.
www.mcafee.com/enterprise/en-us/assets/infographics/infographic-building-trust-cloudy-sky.pdf

US$20 billion

The global cost of ransomware damages in 2021 was US$20 billion, 57 times what it was in 2015.

SOURCE:
cybersecurityventures.com/cybersecurity-almanac-2022



123456

The top most common password in 2022 is '123456', followed by '123456789'. Third is 'qwerty' and fourth is, you guessed it, 'password'.

SOURCE:
cybernews.com/best-password-managers/most-common-passwords

44%

Top of the Allianz Risk Barometer at 44 percent is cyber incidents, followed by business interruption at 42 percent.

SOURCE:
cybersecurityventures.com/cybersecurity-almanac-2022

$750,000

The Australian Federal Court ordered RI Advice should pay the Australian Securities and Investments Commission $750,000 towards costs for contravening the Corporations Act "as a result of its failure to have documentation and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk in respect of cybersecurity and cyber resilience".

SOURCE:
www.aspistrategist.org.au/cybersecurity-rulings-important-for-all-australian-businesse

LATROBE HEALTH SERVICES – REGIONAL MIGRATION

When the Gippsland-based private health insurer needed a re-architecture of its entire IT environment, it found a cultural alignment and much more with AC3.

Kamran Channa has enjoyed a long career in IT, with roles including technical lead, technology manager and, for the last decade or so, as Chief Information Officer with various organisations. But it's an early role outside of IT that perhaps gives a clue to the industry in which he now finds himself.

From 2008 to 2012 he worked as a telephone counsellor for Life Circle, helping callers and their families and friends dealing with life-threatening illnesses. Working so directly with people facing such challenges in that role couldn't help but give him an insight into the issues faced by people on the other end of the services supplied by his current employer, Latrobe Health Services.

Channa has now been with the organisation for three and a half years, responsible for IT-related governance and risk, strategic IT alignment with business goals, best-in-class core IT services and business systems, and the portfolio of member-facing digital services.

Latrobe Health Services, headquartered in Morwell in the Gippsland region of Victoria, is a not-for-profit private health insurance provider that offers hospital and extras products to approximately 81,000 Australians.

It recently celebrated its 70th anniversary and its longevity goes some way to explaining why the organisation's IT was long overdue for an overhaul.

Joining Latrobe in March 2019, Channa says he stepped into a newly created role. After working in IT for over 23 years, mostly in financial services and with a smattering of work in IT

"The advice I would have for others in my position is to not rush decisions. Take deliberate action and consider your options carefully before moving forward." – Kamran Channa

> AC3 worked incredibly closely with us to really understand our regulatory compliance requirements.

services in communications, he says he was faced with an important task right off the bat. “The reason the role was created was to align Latrobe’s regulatory position closely with the expectations of the regulator,” he explains.

“Historically, Latrobe was an organisation where technology played a huge role in driving the direction that the organisation took, as opposed to the organisation considering technology as an enabler of business capability.”

The IT environment as it stood was simply incapable of supporting the organisation’s strategic goals. “We had a sustained period of underinvestment in technology that led to a fast decaying platform,” says Channa. “The immediate focus for me was to work with the team across Latrobe to develop the long-term IT strategy.”

Once this was completed in early 2020, the strategy was then endorsed by the board in March of that year. A request for proposal (RFP) followed, with a number of organisations invited to respond, one of which was AC3.

THE PROJECT

To bring Latrobe’s long-term vision to fruition, a complete re-architecture of its core IT environment was required. All of its systems from the legacy on premise environment needed to be migrated to the cloud. “This also included a replacement of our corporate network and complete redesign and re-architecture of our remote access platform,” says Channa.

Other areas that needed to be improved included security and compliance against the APRA (Australian Prudential Regulation Authority) standards to which insurers are subject, as well as productivity and efficiencies.

WHY AC3?

When undertaking the RFP process, Latrobe liaised with five organisations. Channa says that, while it continued to work with three of them over the course of the RFP, one stood out above the rest. “AC3’s engagement, AC3’s solution, architecture design and maturity of response were a clear standout,” he explains.

Latrobe had a number of criteria that needed to be addressed by a potential partner, but one of the most fundamental was cultural alignment, he adds. “AC3’s response was one that met our requirements most comprehensively. And we felt that its operating culture was much more aligned with our organisation.”

Having that alignment meant the removal of many barriers for successful project execution. “At Latrobe Health Services we value honesty, integrity and transparency,” says Channa. “We felt that over the course of the engagement with AC3 we received the same levels of integrity and honest advice from AC3 that we would offer to our customers.

“AC3 worked incredibly closely with us to really understand our regulatory compliance requirements, and every component of the solution it provided was closely aligned with those needs.”

“If we hadn’t invested in the IT environment, we wouldn’t have been able to support the remote working that was required during the time.” – Kamran Channa

> Productivity certainly has improved greatly. And in the ever-evolving world of cyber security, we are much more confident that our environment is now far more secure than it was in previous years.

CHALLENGES

There were three main areas of concern in executing the re-architecture process. First and foremost, Latrobe Health Services had a long history and belief in investing in technologies in a traditional manner. Cloud technologies, therefore, had not been a part of the mindset. Adopting this technology required a significant focus on challenging staff assumptions and enabling them to easily embrace the new technologies.

The process was daunting from a change management perspective, says Channa. With staff working remotely and having to understand and embrace the changes at the same time required significant consideration. Again, AC3 was able to assist.

"AC3's project managers worked really closely with the Latrobe project managers and the communication back and forth meant that we were able to effectively manage the change," he says.

A further challenge revolved around geography. Latrobe's location means it is a regional organisation and traditionally this has caused issues with factors such as high-speed internet. Implementing the infrastructure for a cloud-based technological environment would require a major upgrade in processes and systems.

Third was a global challenge that of course few saw coming. COVID-19 meant that the project implementation was "coincidentally smack bang in the middle of the pandemic years," says Channa. But while lockdowns and sustained remote working arrangements didn't work in the organisation's favour, he adds, the delivery and execution of the project kept on track. "We never felt that there were parts of the project that were being delayed unnecessarily. While we were moving slightly slower than expected, we were making steady progress."

OUTCOMES

The positive side of this was that the adoption of cloud technologies enabled fundamental changes in operations at Latrobe Health Services. "In hindsight, in context of the pandemic, if we hadn't invested in the IT environment, we wouldn't have been able to support the remote working that was required during the time," says Channa, adding, "I'm very happy to report that now we have 100 percent of our workforce able to work remotely."

Workforce buy-in was also successfully achieved. "Our staff did embrace the rapid shift from the old ways of accessing applications to the new ways," says Channa. "Latrobe Health Services is now an organisation that is ready for adopting new technologies.

"Productivity certainly has improved greatly. And in the ever-evolving world of cyber security, we are much more confident that our environment is now far more secure than it was in previous years," he adds.

"Through the process what we learned was that public cloud-based technologies are far more advanced and mature, and there's no reason a modern organisation couldn't consider a public cloud-first approach."

Despite the restrictions placed on all businesses during the height of the pandemic, in retrospect Channa sees the enforced slow down of Latrobe's strategic plan execution was perhaps a blessing in disguise. "The advice I would have for others in my position is to not rush decisions," he says. "Take deliberate action and consider your options carefully before moving forward."

And he advises really identifying the best possible partnerships to assist organisations taking that next step on the journey to cloud migration. "I would highly recommend AC3's services to any organisation that operates within the financial services industry," he concludes.

The top 10 mistakes of cloud migration

One of the smartest pieces of advice ever shared is 'plan, plan and plan again'. It's applicable for pretty much any event, from a dinner party to a hiking trip to, certainly, cloud migration. But not planning properly is only the first trap organisations can fall into if they're not careful.

Photo by Bruce Mars on Unsplash

NEGLECTING TO PLAN

Of all the mistakes organisations can make when they do decide to migrate to the cloud, a lack of adequate planning is probably the biggest. It's the one from which all the others naturally follow.

MIGRATING FOR THE WRONG REASONS

Migrating to the cloud 'just because everyone else is doing it' is a pathway to failure. A thoroughly thought-out business plan and management model must be created and considered before choosing to migrate. What benefits will the move make for the business and how will they continue after the change has been implemented and in the long term? Will a move to the cloud help the organisation optimise certain tools? Could it assist with improved communication with teams working remotely? Would it mean the

> No matter how skilled and experienced the tech team, it's unlikely they will have the specialist knowledge to implement an end-to-end cloud strategy.

organisation is better placed to take advantage of data storage or cloud-based call centre solutions? If none of these apply and the business could actually see decreased productivity resulting from migration, then doing so would clearly be a mistake.

LACK OF WORKFORCE PREPARATION

Any move as fundamental to the culture and practices of an organisation as a shift in the way work is executed needs to be clearly explained to staff beforehand. Without employee understanding and, importantly, buy-in the road forward will be rocky indeed.

Migrating to the cloud will have impacts across the organisation and will be a major shift for the business – so all stakeholders need to be informed as to why it will be done, how it will be done and what changes it will mean for the organisation.

The first staff to have on board, of course, are the members of the IT department. But it shouldn't be assumed that they can lead the migration. Organisations that take such shortcuts as 'our tech staff are experts and can oversee this move' are risking failure. No matter how skilled and experienced the tech team, it's unlikely they will have the specialist knowledge to implement an end-to-end cloud strategy. On the other hand, if the task is outsourced there's no quicker way to snarl up a smooth transition than by not having the internal team consulted and included in the planning period from the get-go.

IGNORING SECURITY AND COMPLIANCE

With cybercrime increasing at such an alarming rate, organisations need to proactively protect their data from organisations and persons with malicious intent. Considering the security of any data during and post migration is imperative to avoid compromising it. It is also vital to ensure that all legal compliances are adhered to, depending on the specific nature of the data being handled; for instance, if it be financial, health-related, or governmental.

DISMISSING THE IMPORTANCE OF STORAGE LOCATION

Allied to the necessity of ensuring security and compliance adherence in the transfer of data and processes, another mistake organisations can make is failing to identify the most appropriate location for its storage. What region meets your data sovereignty requirements, how secure is it and will there be any other legal considerations that are geographically related? The organisation is responsible for the security of both its own and its clients' confidential and valuable data. A breach could end up costing the organisations untold sums in compensation or insurance claims. So, it's of paramount importance that businesses stay informed about data regulations and know they are subject to any regulatory or compliance requirements.

This entails thorough investigation of the security provisions of any potential cloud platforms to ensure that all applications and data are fully protected, but also remain easily accessible and available for audit at any given time.

MIGRATING THE WRONG APPLICATIONS

'Lifting and shifting' may be one of the simplest and most straightforward methods of migrating to the cloud, but it doesn't mean it's always the most successful. Performing a 'lift and shift' without any form of data optimisation may speed up the process in the short term but could result in a reduction in efficiency down the track. At some point it is likely that the IT administrators will have to go back to the applications and data and optimise it for the cloud. If optimisation is done beforehand, with systems configured to take full advantage of the cloud's unique features, organisations can avoid suffering from 'short-term gain for long-term pain'.

NO ASSESSMENT OF IT AND BUSINESS PERFORMANCE

Migrating to the cloud is a major undertaking for any organisation, so to minimise the disruption to business continuity that it will entail, it's necessary to gain a clear understanding of current application usage. How, when and why do the various business teams use their applications? And how will this be affected by a move to the cloud? If an organisation hasn't fully grasped the realities of its internet connections and usage or the amount of bandwidth it is working with, there could be unpleasant surprises down the line once migration has occurred.

A related common mistake is to not look carefully enough at the current performance and status of IT hardware equipment. A business that has recently invested heavily in updated hardware and then straightaway looks at migration is clearly not making the best decision for its bottom line.

CHOOSING THE WRONG VENDOR

It may seem as if there is no such thing as a wrong cloud vendor, but there may be a wrong provider for a particular organisation. When specific business needs and processes are properly assessed, it will become apparent that different applications have different requirements. In which case, the best-case scenario is often a hybrid cloud approach to provide a range of private and public cloud solutions. In a similar vein, an organisation that contracts the first cab off the rank regarding providers and doesn't do its due diligence regarding such key characteristics as reputation, technical competence, experience in the field, range of service and customer satisfaction could get into trouble. Delving deeper will do more to avoid making an error – checking the quality of the provider's data centres, its approach to data security and safety, the quality of its engineering team, the size of its customer base, its solutions for patch and update management and its level of customer support.

> A related common mistake is to not look carefully enough at the current performance and status of IT hardware equipment.

FAILING TO CONSIDER POST MIGRATION MANAGEMENT

Migration to the cloud is only one step. This is an ongoing process and if organisations don't have procedures in place to continually monitor, upgrade and mitigate issues, this could be the biggest mistake of all.

SELECTING AN INAPPROPRIATE PARTNER

The best and surest way to navigate the path to a successful cloud migration, and then ongoing strategy, and to not fall into any of the traps mentioned above, is to partner with a cloud migration specialist, which can assist the organisation along every step of the way, ensuring a smooth transition through:

- a migration readiness assessment
- a cloud adoption framework
- monitoring the performance of applications
- ensuring security and compliance
- establishing pivotal KPIs
- the cloud TCO (total cost of ownership)
- benchmarking and optimisation, and
- post migration monitoring and troubleshooting.

The value of an SDM

Utilising the skills of a Service Delivery Manager assists in maximising the end-to-end service and support relationship between customers and their managed service provider.

By Greg Riches, Principal Service Delivery Manager, AC3

Often part of the broader Service Integration and Management (SIAM) practice within an MSP, those drawn to the role are IT minded 'people people' who are passionate about the customer service experience, who are open and truthful with their customers, and love to build a strong rapport. They will also excel when it comes to attention to detail, which is vital for ensuring they understand their customers' contracts inside and out, including the key SLAs and associated service level performance metrics on which the managed service provider is measured.

I refer to my SDMs collectively as the 'HIT team', as Honesty, Integrity and Trust are the team's fundamental guiding principles for delivering a true 'value add' that our customers expect when considering our services.

Customer perception is reality in any service experience. A quality Service Delivery Manager (SDM) will focus on driving actions to mitigate any gaps in service or help to educate customers where a realignment of expectations or an uplift in the contracted services may be required. The SDM is therefore well-versed on the MSP's service catalogue, and the associated service descriptions.

Some other key responsibilities of an SDM include:

- providing comprehensive service management reports, including detailed service level performance reporting
- holding service management reviews and other governance meetings with the key customer stakeholders, as specified in their contract
- focusing on continual service improvement of customer processes, initiatives and service levels, ensuring collaboration within both technical and non-technical teams, and
- being typically engaged at the start of a new or existing customer's onboarding project, working closely with the Project Manager to drive 'service enablement', and ensure a smooth transition from project to 'go live'.

BENEFITS

The SDM acts as the customer's advocate within the MSP, working closely with the other internal practices (particularly the systems operations/ engineering specialists) to drive meaningful progress for the customer.

The primary focus of an SDM is to ensure the customer obtains maximum benefit from the products and services they have purchased.

> The SDM acts as the customer's advocate within the MSP, working closely with the other internal practices to drive meaningful progress for the customer.

Greg Riches, Principal Service Delivery Manager, AC3

The SDM forms a strong relationship with the customer's key contacts (particularly the operational and service management peers), by building an understanding of their requirements and business drivers.

The SDM is also the trusted service management escalation point for operational service and support, complementing the Major Incident Manager where required, to ensure timely communications and high priority issue resolution for their customers. This extends to the delivery and presentation of detailed post incident reports for any major incidents that have impacted customer services.

MAKING THE MOST OF AN SDM

Customers should think of their SDM as their relationship manager for any matters relating to their ongoing service and support experience. The SDM has close ties with the assigned Account Manager and Technical Account Manager, to maximise the customer's engagement experience overall.

And if something should go awry? Unfortunately, it's not a perfect world! If you feel that your service expectations are not being met, or you have a business reason or circumstance for something to be expedited, the Service Delivery Manager is your management escalation point to facilitate the resources for urgent attention.

At AC3, our Service Delivery Managers are also ITIL (Information Technology Infrastructure Library) certified. Speak to your SDM around the adoption of and adherence to ITIL best practices in general. They are part of the SIAM practice within AC3, which means the ITIL service managers and process SMEs (subject matter experts) are all part of our wider team!

How ServiceNow complements SIAM delivery and governance

A broad system of capabilities, ServiceNow supports service integration and management by digitising a suite of essential business processes, including governance, risk and compliance.

Photo by Brands&People on Unsplash

'SIAM' may have once conjured up visions of Yul Brynner and Deborah Kerr butting heads and then dancing in *The King and I*, but that movie is nearly 70 years old, and the country has been called Thailand since 1939. Nowadays, SIAM is much more likely to be used as the acronym for 'Service Integration and Management'.

"Essentially, it's a framework that helps organisations to provide a level of management and governance of their connected ecosystem of suppliers, processes, policies and delivery," explains Dan Marsh, Head of ServiceNow at AC3.

SIAM enables a consistent set of processes, policies and technology with a major focus on trying to drive governance, management of performance and continual improvement in how a business executes its outcomes or the processes it utilises to achieve those outcomes.

In any organisation there are generally two ways in which SIAM is executed, says Marsh. Sometimes, it's through an internal service integration team within the organisation as a retained function, with a senior leader steering the ship, and a team of operations managers and process managers looking after the processes that enable delivery.

> It really drives that integrated ecosystem so that... the flow of work between different teams is executed and orchestrated effectively, and the customer gets the outcome they need.

The alternative is via an outsourced service provider with service integration capability, providing SIAM governance on behalf of the organisation. In either case, the goal remains the same – to improve the performance, delivery and execution of how the ITSM processes are engaged, and also how it truly supports the organisation to deliver optimal outcomes for employees and the people they serve.

One platform that can assist with the effectiveness of SIAM is ServiceNow, as it features a raft of capabilities designed to support the governance aspects of delivering efficient processes. Based in the cloud, ServiceNow has been the market leader for IT service management for over six years, but is expanding exponentially, says Marsh, to further mature the ways in which organisations adopt the platform outside of IT Service Management.

"ServiceNow is a broad ecosystem of capabilities aimed at digitising work," explains Marsh. "It enables the ability to report on KPIs and metrics, whether it be for particular teams, processes or service partners.

"It really drives that integrated ecosystem so that the flow of work between different teams is executed and orchestrated effectively, and the customer gets the outcome they need."

There are several key features that facilitate this and the core one is the IT service management suite. This suite includes all the standardised item processes: incident, problem and knowledge management; change request fulfilment; continual improvement and asset management.

"Each of these capabilities has its own module, the ability to support the delivery of processes across the organisation and a raft of different plugins that support the level of maturity a SIAM framework demands," says Marsh. "And over time each process is essentially continually improved."

One of the biggest factors in ServiceNow is the common service data model (CSDM), which is built on the foundation of a very strong integrated foundational platform. The CSDM provides a framework and guidance on how capabilities, data and processes integrate to truly mature operational delivery, from which any SIAM organisation can benefit.

"This really helps to map the relationships between technical components, business processes and business services... to bridge the gap between the business and IT, and bring that business lens to your technical data."

Some of ServiceNow's key platform capabilities that complement SIAM delivery include Vendor Management Workspace, ITOM (IT operations management) Discovery and Service Mapping, Integrated Risk Management (ServiceNow's governance, risk management and compliance [GRC] capabilities) and Integration Hub.

For organisations looking to participate in ServiceNow integration, there are a few operating models to choose from, reveals Marsh. They could be incorporated into the ServiceNow platform, which means the service partners operate on the customer's platform, or they could be integrated into the platform, in which case the customer will define and govern the process and determine the rules of engagement, spelling out the compliance objective.

Managing a SIAM framework, an organisation has processes and policies to which it must adhere, but also contractual compliance. ServiceNow's GRC capabilities provide the ability to track risks, assign them to delivery teams and enable the remediation of those risks.

WHEN IT'S RIGHT TO RETAIN

When timing or other restraints impede a migration to the cloud, organisations may decide to deploy another of the 'seven Rs' and retain a portion of their applications.

Of all the seven Rs of migration strategies, 'retain' is one of the two so-called passive responses. Unlike refactoring, replatforming, rehosting, relocating and repurchasing, retaining, as the name suggests, means a decision has been made to not migrate an application to the cloud. It should be noted, however, that this may well take the form of a pause or 'point-in-time' strategy, meaning the strategy is to not migrate for the time being, but the decision will be reassessed at a later point.

Despite the many advantages of being in the cloud, there are some circumstances where it may not be a useful strategy or the best business decision.

Reasons to retain an application on-premises or in-house can include:

- It is due for retirement shortly and the business has made an executive decision to ride out its depreciation value to get the maximum financial benefit from the application.
- It will require a significant amount of re-architecting before it is suitable for migration.
- The cost of migration is prohibitive or exceeds allocated budgets.
- Any disruption a migration program may entail is not practical at the given time.
- It is a legacy operating system or application that is not supported by a cloud environment.
- There are real-time latency requirements.
- There is a 'if it ain't broke don't fix it' consideration – an application may be operating so satisfactorily there is no business case to support the cost and disruption of a migration.
- The organisation or industry must adhere to strict compliance regulations requiring it to keep its data on-premises.
- The application requires such high performance it is better suited to remaining on-premises.

It should be stressed, however, that none of the above may be set in stone. The circumstances may evolve and the reasons for retaining an application may change with them. For this reason, it's important to qualify a decision to 'retain' with another 'R' – revisit. It's necessary to revisit the application usage every six months to reappraise the situation. The decision to retain may be a time sensitive one, that there are other factors preventing the migration or there is a lack of important information. When that new information becomes available, a different strategy may be a better option. For instance, companies abiding by compliance regulations may find that the compliance landscape has changed, or those constrained by latency requirements could see technical developments that now make migration to the cloud possible.

THE HYBRID APPROACH

Migration to the cloud does not have to be an all or nothing affair. It's likely that organisations will look to retain portions of their IT portfolio because they are more comfortable having these applications on-premises and under their control. In such cases, they can implement a hybrid or part migration strategy. This is a considered approach for those in industries that are regulated or bound by constitutional rules that require them to store and/or run aspects of their business and services on-premises or even within specific regions.

Photo by Campaign Creators on Unsplash

> The decision to retain may be a time sensitive one, that there are other factors preventing the migration or there is a lack of important information.

Jaco Olivier – a passion for the platform

From Pretoria to Pitt Street, Jaco Olivier has travelled across the globe to pursue his love of cloud technology and bring his expertise and passion to AC3.

> Technology exists because there is a business problem and for me it's always about trying to work through what the business problem is and how I can solve it.

Born and bred in South Africa, Jaco Olivier, Hyperscale Solutions Architect and Platforms Manager at AC3, headed for Australia about 10 years ago, when the opportunities for both his family and career were just too good to pass up.

His interest in technology and computer software goes back to childhood, he says.

"I was introduced to computers by a friend whose dad had one for his business," he recalls. "It was many years ago and I think XTs and 286s still existed. I became interested in the mechanics of how computers worked, from the operating systems to being able to control them."

Olivier's father enrolled him into a crash course at a local high school, even though he was still in primary school. "I was very young, probably in about year four."

Fascinated by coding – changing it and breaking it – he eventually wound up studying a BSc in information technology. He picked this as one of the three IT options available because it was focused on business information systems. "So a lot of my electives were around business management," he says.

And it's this aspect that has been the throughline of his career to date, despite his various roles that cover the gamut from analyst to developer and beyond. "Programming was important, but I always said, 'how does it support the business?'," he explains.

"Technology exists because there is a business problem and for me it's always about trying to work through what the business problem is and how I can solve it. That may be technology, or it may not. With my career and background, it used to be technology most of the time but then I moved up."

CROSSING THE INDIAN OCEAN

After various developer and systems analyst roles in South Africa, his Australian career began at the hospitality tech start-up Kounta (now Lightspeed), where he was a lead systems analyst. He later spent six years at Healthdirect Australia as a solutions architect, where he focused on the architecture and development management of web applications supported by cloud native information management solutions deployed on Amazon Web Services (AWS), implementing semantic reference models and delivering high-speed search services through Apache Solr and Elasticsearch.

He believes his preference for AWS is largely historical, as this was the first cloud service he was exposed to. "It was the more dominant and mature cloud service provider at the time, and it just naturally evolved from there. AWS does offer a very rich set of services.

"Also, the layout and breadth of documentation and training that AWS provides, for me, is excellent."

His affinity with the cloud services provider saw him develop into a subject matter expert in all things AWS and a self-proclaimed cloud evangelist, which eventually led him to join AC3 in 2019 as AWS practice lead at the organisation's Pitt Street office in Sydney. "It was all around how do we manage the relationship with AWS and how do we promote AWS within the organisation and get buy-in?" he says.

At the same time, he was doing solution architecture for key and larger

> It's not just about how elegant your solution can be and how quickly and accurately you can present data to an end-user, but also how economically or eco-sensitive your solution is.

> Sometimes I say, 'it's not a job, it's a lifestyle'. You need to love what you do.

enterprise customers, setting up the frameworks, standards and blueprints that his team could utilise in their customer engagements.

His primary focus remained, as always, on potential business outcomes. Olivier now straddles the business versus the core technology developments at AC3. His titles of Hyperscale Solutions Architect and Platforms Manager see him wearing more than one hat.

"During a normal week I'm managing a team of cloud solution architects and making sure they have appropriate support to deliver world-class services to our customers," he says. "And then I do consulting for some customers and engagements with them.

"On the other side, I lead a team of platform engineers and together we reimagine cloud native solutions and build new business services to support the AC3 hyperscale business, which translates to a better experience for our customers."

CHALLENGES

Apart from juggling a few hats, Olivier says his concerns today and, in the future, will still revolve around business outcomes, but now they also have to incorporate sustainability facets. "It's not just about how elegant your solution can be and how quickly and accurately you can present data to an end-user, but also how economically or eco-sensitive your solution is.

"They'll want all the processing that comes with a cloud compute, but also be constantly considering the carbon footprint and lowering their environmental impact."

"It's going to be a big design thinking evolution of information technology architecture," he adds. "You'll have cost optimisation but also carbon footprint optimisation."

He further sees a future of decision intelligence where organisations of all sizes will be adopting machine learning and data analytics, either as home grown or SaaS solutions to optimise organisational decision-making processes to near real-time levels.

HIGHLIGHTS

In a career that has developed rapidly to adapt to changing circumstances, Olivier says there have been some notable achievements. One of the most memorable stems from his tenure as lead architect at Healthdirect's consumer services business unit. The project, which delivered a key organisational solution and is still fully operational today, was creating the organisation's Medicines Finder.

Consolidating multiple data sources, and ultimately a vast amount of data from Australia's TGA (Therapeutic Goods Administration), the project enables users to type any medicine name or active ingredient into a searchable database, and it will quickly list all the brand names in Australia that are part of the Australian Register of Therapeutic Goods (ARTG).

"You as a consumer can say, 'here is a known brand name, so I can easily understand what is available in the market as a substitute for a specific brand name of medicine'," explains Olivier. "It also offers images of how the pills or tablets look and the Consumer Medicines Information (CMI) leaflet that is commonly misplaced the second the package is opened."

It was a huge undertaking – a six-month project utilising a multi-skilled team of engineers and medical taxonomy subject matter experts, and requiring the design of complex user interfaces, graph database backed APIs and a data-caching solution with impressive capabilities.

As another proud accomplishment, Olivier also nominates a more recent AC3 project in which he built up the company's standard methodology and framework for how public cloud migrations are approached. The project established a standard approach that is now being used for small engagements all the way up to enterprise level engagements, working through the well-defined stages and processes to complete a successful migration.

ADVICE

And for those looking to follow a similar career path, Olivier has some salient advice. "Sometimes I say, 'it's not a job, it's a lifestyle'. You need to love what you do."

If you don't, boredom beckons, he believes. And you quickly lose touch with the fast rate of technological evolution. "Whatever information sources you utilise to remain ahead of the pack, ensure they are factual and can be trusted. Have a good grasp of new technologies and how they impact, disrupt or can improve business processes. Having a view that addresses both the technology and business facets keeps you well respected among engineering teams, technologists and, most importantly, business users.

"Being able to have a solution conversation with various stakeholders at the technology layer, and then a deep dive into business benefits and impacts is what makes a solution architect or a solution architect manager fairly well respected and utilised in any organisation."

Evolution with ServiceNow as a customer and partner

Dan Marsh leads up the ServiceNow Practice at AC3. He talks to Three *about his experiences with the platform and its growth within the organisation.*

Tell us a bit about your background and experience with ServiceNow.
I've worked in the ServiceNow platform since 2015, having worked in large environments like Qantas and Origin Energy as they adopted ServiceNow and transformed how they operate. I joined AC3 in 2019 as the ServiceNow Practice was gaining momentum. My background lies heavily in IT service management, SIAM (service integration and management) and technology transformation, which set me up to progress further as the ServiceNow Platform started to grow and mature, and adoption was accelerated.

What is ServiceNow and how has AC3 established its ServiceNow Practice?
ServiceNow is a technology platform that aims to digitise, integrate and automate the flow of work throughout an organisation. For a long time, there was a misconception that ServiceNow was just another Service Desk tool, but over the years it truly has become the platform of platforms, with solutions spanning IT, HR, finance, facilities, procurement, project and portfolio management, governance risk and compliance, customer service management… and the list goes on.

ServiceNow segments its capabilities into various product lines – IT Workflows, Employee Workflows and Customer Workflows. More recently, ServiceNow is starting to mature in offering solutions based on industry segments, as it aims to truly evolve the ways in which highly regulated industries operate.

AC3 started its ServiceNow journey back in 2015. We adopted ServiceNow as an internal tool to service our customers, but soon had customers enquire if we offered ServiceNow services. As such, being a growing managed service provider across IT, we assessed and established Domain Separation within our AC3 ServiceNow instance and started onboarding customers to leverage the platform's power. This approach involves carving out a protected section (domain) of our ServiceNow instance for a specific customer. It's particularly beneficial for customers who don't want their own instance, don't meet ServiceNow Minimum Annual Contract Value guidelines or want to tap into a best practice solution with no effort based on AC3's best practice ITIL Processes. In 2018/19, a decision was made to move our ServiceNow capabilities into its own practice due to increasing market adoption, and I joined the organisation in April 2019 with the core goal of growing and scaling our capabilities.

When I joined, we were playing heavily in the IT service management capabilities of ServiceNow and were a 'Specialised' partner of ServiceNow. We soon moved to Bronze partnership status in 2019 and, as the partnership model evolved, we moved to Premier. We are now sitting at Elite partnership status, which is as high as we can go without being a multinational.

Over the past few years, our focus has been on broadening our skillsets through certification, platform coverage and what we offer to our customers. We have implemented capabilities across a large portion of the platform, and this continues to grow as the platform expands on the back of ServiceNow acquisitions and innovation to broaden platform capabilities.

What does AC3 do in the way of ServiceNow and how does it help organisations within the ServiceNow Platform?
Being an IT managed services provider, our highest volume of work and what we truly excel at are the areas associated with enabling IT service management,

SIAM, IT operations management (ITOM), strategic portfolio management (previously ITBM), security operations and strategic platform integrations. This is our sweet spot, as it aligns closely with our core business. We have had the pleasure of contributing to the enablement of large transformations in these areas to enable our customers as they evolve their operating models, and harness more of ServiceNow to unlock that journey.

We are seeing a growing focus for our customers in driving greater governance, technology life cycle management, cyber resilience, efficiencies in delivery and cost management in IT functions. We are also seeing increasing demand for the SecOps suite and have completed multiple deployments of vulnerability response to aid in cyber security processes.

Plus, we deliver a lot of solutions via the ServiceNow app engine. These are generally to meet bespoke requirements for line of business teams, and harness the ServiceNow workflow engine to digitise the way in which they operate. We migrate teams away from legacy ways of working – email-driven work assignment, shared mailboxes, paper forms, disparate knowledge management sources – and arm them with capabilities that aid in the flow of work, greater customer engagement, the ability to truly report on demand, performance and decision-making.

We also deliver managed services for the ServiceNow platform to support organisations in driving greater adoption of what they are licensed for, keeping the lights on and driving ongoing iterative change in ServiceNow to underpin continual improvement efforts. Our managed services are a growing

> We migrate teams away from legacy ways of working... and arm them with capabilities that aid in the flow of work, greater customer engagement, the ability to truly report on demand, performance and decision-making.

part of what we do as organisations look to get more out of the platform and to digitise ways of working. This is offered for a customer's own ServiceNow environment, or within the AC3 ServiceNow environment where a customer may maintain a tenancy and adopt AC3's best practice processes.

What are some of the most common challenges you see in how organisations leverage ServiceNow?
Quite often, we enter an already established ServiceNow platform, and it isn't in a healthy state. It is heavily customised, the security posture of the platform is low and there isn't any real governance of how the platform is managed and maintained. These issues are the direct result of not aligning to ServiceNow best practices and have a material impact on the future adoption of new features and drawn-out upgrade processes.

How do integrations into ServiceNow help to add more value to AC3's customers?
We see ourselves as a specialist integration partner within ServiceNow, having integrated over 50 different technology platforms into it. ServiceNow makes it really easy to establish seamless integrations between platforms with pre-built APIs and service graph connectors to enable integrations quicker than ever before. It has never been easier to support the flow of work between technology systems and to enable a federated environment – be it internally or with service providers. Quite often, we help customers on the journey to enable a 360-degree view of their operations and performance, whether it be by ingesting data into ServiceNow or by extracting data from ServiceNow into a broader data solution or data lake to consolidate data-sets.

Where do you see organisations maximising value from the ServiceNow platform over the coming years?
As ServiceNow continues to acquire organisations that contribute to its product stack within ServiceNow, we'll see an increasing use of machine learning and AI driven capabilities across the market. As ServiceNow continues to factor these capabilities into the platform, this will also make them easier to use. It may mean organisations will need to adopt a higher level of licensing for certain capabilities, which unfortunately is often a hinderance to adoption. I believe, though, we will see organisations weighing up the opportunity cost of not pursuing these AI and machine learning capabilities so that their people can focus on the work that isn't as administration heavy, and has higher value for the people they serve. The market is dictating organisations to do more with less, and automation is the best way to achieve this to remain competitive.

What are you most proud of since joining AC3 and leading up the ServiceNow Practice?
Without a doubt, I'm most proud of what the team have achieved as a collective. As the AC3 ServiceNow Practice has scaled and broadened our platform coverage, we've had to adapt and evolve how we operate as a team and constantly challenge the status quo, and we've been recognised in the industry for our work in the way of an ARN Innovation Award and also named as a Rising Star by ISG in the ServiceNow ecosystem. It hasn't been easy, and we've had to do a lot of things for the first time within this fast-moving platform, but we've remained determined and held true to our culture and values. My team inspire me every day through their actions and interactions with our customers. They truly represent what we are about at AC3.

Optimising licensed workloads for the cloud

Licence optimisation is of most relevance to organisations that are planning to migrate to the cloud and need licensing optimisation as part of that journey.

Photo by Andras Vas from Unsplash

When moving workloads to the public cloud like AWS and considering your licensing needs, and the associated budgetary impacts, the first step is to look at the size of your infrastructure footprint. You may have a large organisation but a comparatively small footprint. Understandably, however, it's more common that the bigger the organisation, the greater number of servers they will have.

And it's the larger footprints that have a greater challenge to address regarding whether they take a Bring Your Own Licence (BYOL) route or choose to use cloud service-included hourly licensing. For small to medium sized organisations, the decision is a little easier, as their initial licence investment will generally be lower. In this case, shifting to a cloud-based hourly licensing model provides an efficient way to adopt cloud services without having to deal with the complexity involved in licence management.

Larger organisations, however, may have significant fleets of licensed workload components, with major investments and volume discount arrangements already in place. If this describes your organisation, it is highly recommended that you take the time to properly analyse the details of any previously purchased volume licensing and entitlements.

To the untrained, the BYOL model is most frequently associated with complex licence mobility rules and entitlements of the product or product release version.

During a cloud migration project, Microsoft licensing for Windows Server and SQL Server will frequently be the sole focus of a licence optimisation exercise; however, other vendors may impose similar licence decision points. For example, Oracle's products may require careful consideration to determine the impact on licence entitlements and how to maintain the workload performance versus the compute core (vCPU [virtual central processing unit] or CPU) allowance.

BUSINESS BENEFITS

The end goal of a licence optimisation is to reduce the IT operating costs, although there may be hidden benefits that need to be taken into account before any decisions are made. One key component that may have a significant impact during an Optimisation and Licensing Assessment (OLA) is a rightsizing exercise. Assessing the current on-premises utilisation (CPU, memory and disk) will help with recommendation of a cloud-based rightsized instance/virtual machine type. Rightsizing in terms of provisioned storage may further reduce backup volumes or backup licensing expenditure.

TIPS AND TRICKS TO OPTIMISING LICENSED WORKLOADS:

- When opting for BYOL SQL Server licensing to run on your own shared AWS EC2 instance, the licence packs are sold in four-core packs per instance, irrespective of the number of vCPUs. This means that when a right-sizing exercise indicates that some of your four-vCPU servers can be downsized to two-vCPU servers and maintain the same performance, consolidating two databases on the same server will offer a reduction of one SQL Server licence and one Windows Server licence. Such a simple exercise lowers the overall maintenance effort, backup agent, anti-virus and even managed services fees.
- If you're considering a BYOL model, don't forget that since 1 October 2019 additional constraints have been placed on Microsoft and SQL Server licences purchased after that date.
- Licence optimisation for a SQL Server may go a step further in most public cloud environments. For example, if the SQL Server Enterprise was used exclusively to provide Transparent Data Encryption (TDE) for regulatory compliance, taking a moment to reassess the technology position will highlight that TDE is now a standard offering within both Amazon and Azure.
- AWS's OLA is an assessment program offered by Amazon Web Services to aid migrating customers in making rightsized and well-informed decisions on cloud licensing. On average, an assessment is conducted over a six-week period, and encompasses all infrastructure, operating systems, database engines and server utilisation.
- The AWS OLA provides cost models for running Microsoft workloads on AWS, optimised for both licensing and compute. Using the complete set of infrastructure utilisation metrics, an AWS consulting partner can advise on the most appropriate target state infrastructure and build a total cost of ownership (TCO) model for your organisation's cloud ecosystem.
- An OLA engagement may also provide a key set of inputs to help build your organisation's cloud migration business case.

Learning on the job

"I was shown that I hold the cards, as much as I put in is what I get out."

Daniel Babaian is someone who knows how to make the most out of opportunities. As a gamer, he has long had an interest in computers, but it wasn't until he was at university and not enjoying his double degree in business administration and IT at ACU that he really started to consider a career in the IT industry.

His father suggested a change of tack towards cyber security and the idea appealed.

Being drawn to technology and confident he could learn the associated skills, Babaian switched to a Bachelor degree course in cyber security at Macquarie University and loved it. He is due to graduate in September 2022, but has been juggling his study with a full-time role in his chosen field at AC3. He says that makes him unlike the rest of his cohort. "Most of them have the standard casual job, but no one that I've met has a full-time job as well."

The role came about after he was able to secure a three-month internship at the firm. However, Babaian impressed his team leader so much that at the end of the internship he was offered a position as a SOC analyst. He went full-time at the beginning of 2022, while continuing to study. "It's a bit challenging, but nothing hard work can't do," he says.

His experiences so far have not only taught him a huge amount of practical knowledge, but also how much of his career aspirations are in his own hands. "I was shown that I hold the cards," he says, regarding his manager's encouragement, "as much as I put in is what I get out."

He was offered various training courses and quickly learned that working in cyber security means going the extra mile to keep abreast of an ever-evolving industry. "I learned that if I want to excel I have to study, even after work, because every day it changes."

Some of the first skills he learned were incident handling and alert triaging, along with digital forensics. "This teaches you how to understand and break down incidents," he says, "how to read code and put together what's going on. We have to be like detectives and it's actually something that really can't be taught in a book.

"You have to see it and apply your knowledge and critical thinking."

It's been a steep learning curve for Babaian as he had very little IT experience starting out. He describes it as starting from zero, and says the hardest thing for him was having to get across basic systems administration knowledge to really understand how networks and computers work.

It's the sort of background most would cover in their first two years of training, before moving on to cybersecurity. "For me it was just head first," he says. But he clearly loved the challenge. "Once I got into the routine of making it not just a job but a lifestyle, then it really picked up and I started to understand things in a different way."

DANIEL'S TOP THREE CERTIFICATIONS

- Microsoft Certified: Security Operations Analyst Associate
- Splunk Core Certified User
- Splunk Core Certified Power User

REPAIRING THE BREACH

In late 2021, Babaian learned the benefits of proactively looking for breaches, when he was part of a team that was able to identify and remediate a serious breach for a major organisation.

The manager of that team is one of the reasons Babaian doesn't regret his decision to be full-time at work and only study in his free time. "My manager makes a very big effort to ensure all team members are on the same wavelength," he says, adding that he doesn't miss the social life university can provide, and not only because it has been so restricted by COVID over the duration of his course so far. "I really love the social life at AC3. We have a very good team, and we all get along. And I can also learn so much from my co-workers."

He reiterates the value of education when asked about his future aspirations. "I've only been here for a year, I still have a decent amount to learn," he says. "A year from now, I may start thinking 'can I climb to a higher position, such as team lead?' or potentially even go out to do my own thing on a smaller scale."

> "Once I got into the routine of making it not just a job but a lifestyle, then it really picked up and I started to understand things in a different way."

In the meantime, he has some good advice for other graduates considering a similar pathway. "Learn your basic networking and systems administration skills first, because they're really foundational. And it'll save you so much time in the long run. I was learning about C and how it applies before I'd even learned about A and B!

"I'd also recommend for those thinking of joining that it's not like a normal job. Security is 24/7. It's always changing and can be stressful, but every day there is something different. That's what I really enjoy the most. At AC3, I have found both mentors and a team that consistently encourages, supports and teaches me, providing so much opportunity to grow and learn great skills."

Automating security

The ever-increasing threat landscape in cyber security is leading to teams feeling overwhelmed and under-supported, but the pressures of their workload can be aided by automation, says VMware's Darren Reid.

A recent Forbes report revealed that there was a 50 percent increase in cyber attacks on businesses per week during 2021 compared to previous years. VMware research suggests this translates to an organisation incurring a cyber attack every 11 seconds.

The situation has been exacerbated by the pressures of the last couple of years, says Darren Reid, Director, Security Business Unit Australia/New Zealand, VMware, as companies had to quickly pivot to enable their employees to work remotely. "Previously companies used to have a big moat around them. They'd have people walking into the office on a known device. The company would control the network and they'd be able to secure that and ensure only people that were allowed on the network could get on it…

"What we now have is people on any device, coming across literally any network – from a home NBN connection to a coffee shop, to a library, to a mobile connection. And they're accessing applications that the organisations no longer really control because they're sitting in the cloud."

Add to this the increased geopolitical unrest with nation state actors behind ever more sophisticated threats and the situation is even more alarming. "These are very well-funded, very motivated actors who are targeting very specific industries. "Companies in critical infrastructure, such as food, water, utilities or other core infrastructure, have seen monumental increases in the attacks that they're receiving. And the attacks are sustained, they're not one-offs," says Reid.

Against this backdrop, it is understandable that SOC teams, as people who work in cyber security operation centres, are reporting growing levels of stress and burnout. This is being compounded by a shortage of skills.

MITIGATION STRATEGIES

To mitigate increasing 'SOC fatigue', says Reid, education and ensuring staff are vigilant is imperative. However, inherently trusting Australians fall victim to scams more often than most, he says. "It comes down to automation and technology. If your security operations team – however big or small, and whether it's in-house or outsourced – is already overwhelmed by the sheer volume of issues, then you need to help them filter through all of the various telemetry notifications to help them understand the ones that they really need to be paying attention to."

The danger here is that it's possible to inadvertently block legitimate access, which is why it's important to consider each business and its operations individually and then ask relevant questions. Software like VMware Carbon Black is able to determine whether a particular activity is the sort that would normally be allowed. When an operation or user behaviour has been identified as out of the ordinary or odd, the team will be alerted. "We then start to carefully narrow the border around this particular user, until we see them doing either the right thing or the wrong thing," explains Reid.

Implementing enterprise detection and response (EDR) software can ease the burdens of overwhelmed SOCs by taking a significant slice of their security responsibilities out of their hands and giving them more time to focus on other tasks. Implementing a set of tools that already has responses for the most common security attacks (as per a framework such as MITRE), while also utilising existing knowledge and skills, can enable an infrastructure person to take action on the network to reduce the movement of the attack at the same time as the security team is taking action to contain the threat to a single device or application.

> "Companies in critical infrastructure, such as food, water, utilities or other core infrastructure, have seen monumental increases in the attacks that they're receiving."

Photo by Andrea Piacquadio from Pexels

"Because it's unlikely that a malicious actor is going to attack just a single machine," says Reid. "They're likely to be doing it to multiple staff members."

Software like VMware Carbon Black allows users to automatically scan and see where else the attack may be happening in the same environment and take action there too.

Plus, a framework like MITRE is updated regularly to recognise and address the many different types of potential attacks being committed.

PRIORITIES

Reid also advises considering the issue from an escalation viewpoint by identifying an organisation's most important pieces of data, whether that be R&D, customer data or credit card information. "Then work your way out," he says. "Protect your crown jewels first and then work out what happens next. What's the next most important?"

The same applies to ransomware – one locked laptop may not have too much of an impact, but a company being locked out of its entire database is a much bigger problem, he says, so security measures should be prioritised accordingly.

Adopting the Australian Government's Essential Eight mitigation strategies, educating staff and implementing the best fit-for-purpose software won't stop the cyber attacks, but it may go some way to prevent SOC team burnout and distress.

AC3 powers towards carbon neutral

AC3 has formed a partnership with HP that will launch a certified carbon neutral option for AC3's products and services, as well as reduce its carbon footprint to net zero over the next four years.

"In our personal lives, it's centric – you see global warming everywhere," says Jessica Handley, Partner Alliances Coordinator, AC3. "You see a lot of communication about saving the planet, but I've never really seen much communication about it in the corporate sense. That's what we're starting the conversation around – how can we be a better and more mature company in this space?"

General Manager of Finance and Corporate Services, James Meharg, agrees. "At the deepest level, climate change is an existential threat that affects the world and AC3 has a part in that, through emissions not just from doing business, but offering our products and services," he says.

There is one notable area of concern that AC3 is looking to address, they say. "The emissions from our industry and data centres in particular are huge. And it's growing," says Meharg. "Emissions from data centres are equivalent to all emissions from air travel... but we want to be setting an example among our peers and our customers in terms of doing something about it."

And they are. AC3's current strategy is two-pronged. First, it is working with the Australian Government's Climate Active program to achieve a carbon neutral certification. "We're looking to not only offer carbon neutral products and services in the coming months, but to have the whole business of AC3 certified as carbon neutral in the next four years," says Meharg. The government program has a process that enables AC3 to calculate its emissions. It will undertake measures to avoid and reduce these as much as possible, says Meharg, and any that can't be reduced will be offset. When certification is gained, AC3 will be able to offer the carbon neutral product or service to its customers.

"We're targeting the two largest services we offer," says Meharg. "Our private data centre and our at-scale offering."

REFRESHING HARDWARE

With data centres a major target, upgrading hardware can make a huge impact, says Meharg. "As time goes on, IT equipment becomes more and more energy efficient. Really old IT equipment in data centres draw a lot more electricity than brand new kit, so upgrading and refreshing the equipment stack is the biggest contribution we can make to reducing our footprint," he says.

"Our data centres are also built on HPE technology, underscoring the joint commitment both organisations have in helping AC3 achieve its carbon neutral goals."

With equipment becoming cheaper and budgets put in place for capital expenditure on cyclical renewal, the result is more energy efficient hardware, he adds.

And the old equipment? Does that get added to the ever-growing mountain of e-waste threatening the planet? No, says Meharg.

AC3's partnership with HP means it can take full advantage of its Asset Lifecycle Solutions. "They either reuse it or they deconstruct it and recycle a huge percentage of the materials," explains Meharg. "It's something they're really proud of and we are proud to be part of the program."

> We're looking to not only offer carbon neutral products and services, but to have the whole business of AC3 certified as carbon neutral in the next four years. *James Meharg*

HP PARTNERSHIP

The second pillar of the strategy is enrolling in HP's Amplify Impact program, which was launched in 2021 with the goal of driving "meaningful change across the global IT industry", according to HP's website. Signing up for the program for a financial year, HP's partners can access the organisation's extensive resources and experience to improve their own sustainability goals and performance. HP has vowed to attempt to enrol at least half of its partners in the voluntary program by 2025.

For its part, AC3 has already formed its own internal committee as part of the program. It's a CSR (corporate social responsibility) group, says Handley, but is in essence a sustainability committee. Heading it up, she and Meharg say they've been encouraged by the positive response so far. "We discovered a lot of our employees already have interest in sustainability," she says, noting that several staff members revealed previous experiences and qualifications in the area.

"The purpose of the committee is to get that validity. Is AC3 going in the right direction for our staff and customers?" she says. There are currently 12 members, with each business unit encouraged to provide one person so that the discussion isn't limited to the executive or senior leadership level of the company. "We're trying to get that engagement across every aspect of the business," says Handley

"We're very surprised and happy with the response we received. We had different ages, different demographics and everyone is really engaged and asking productive questions."

Photo by Alena Koval from Pexels

PASSING ON THE BENEFITS

The upshot of AC3's strategy is that every step it takes toward carbon neutrality is a positive step forward for its customers too.

"When our customers calculate their emissions from their partners and suppliers, they have to take into account the emissions from AC3's products and services. By being able to offer a certified caron neutral option for our product or service, then we are helping customers to reduce emissions as well," says Meharg.

"If you're a customer of ours and you've got your own targets for reducing your emissions, then you don't have to worry about the issues from the work you do with AC3, because we've got that covered," says Meharg.

HPE: where reduce, reuse, recycle is not just lip service

HPE has a long-established commitment to sustainability. Here, Three *speaks to HPE Financial Services, Damien Whelan about the organisation's approach to lessening its impact on the planet's ecology.*

In mid-May 2022, Brisbane's *Courier Mail* ran a story titled 'why it's good practice to look at the big picture with ESG [Environmental, Social and Governance] issues' exploring how organisations with good ESG credentials are feeling the business and bottom line benefits.

Damien Whelan is APJ Director of Asset Life Cycle Solutions and HPEFS Enterprise Sales Director – South Pacific at Hewlett Packard Enterprise (HPE) and says his company is way ahead of the curve on this one.

HPE has had a long-established commitment to sustainability and knows how good ESG practices also make sense from a business point of view. It would be fair to say it was a pioneer in this space – for over a decade HPE has been continually listed in the Dow Jones Sustainability Index, receiving the highest scores for its climate strategy. It's also been a long-time member of the Ellen MacArthur Foundation, aligning with its circular economy principles.

It's a huge topic, but one that is in the organisation's DNA, says Whelan.

"From a HPE perspective, it includes everything from the way a product is designed and put together to renewables, recyclables, looking at the design phase and saying, 'how can we design products that are going to stay in the circle for as long as possible, that are going to use lower amounts of energy and have renewables as part of the design process?'" he says. "Then, once they're within a customer's site, how do they help reduce their footprint, their energy and their impact on the environment?"

> "How can we design products that are going to stay in the circle for as long as possible, that are going to use lower amounts of energy and have renewables as part of the design process?"
> *Damien Whelan, APJ Director of Asset Life Cycle Solutions and HPEFS Enterprise Sales Director – South Pacific, HPE*

Where HPE Financial Services comes into the mix is in the pathways it offers to ensure the assets stay in the circle even longer. These pathways include various investment solutions, leasing programs, asset upcycling programs and certified pre-owned programs. "It's putting them into secondary and tertiary environments where they're still functional and still providing value to customers," says Whelan.

On the back of this, there is an information gathering process, which HPE feeds back to its customers, letting them know exactly how much carbon emissions and landfill they've avoided and how much energy they've saved or avoided using. It's not just lip service or the organisation spruiking its credentials, says Whelan. "It's backed up by a science-based approach, which is audited. It's an independent body that has helped to put it together."

HPE's customers use these reports internally, he adds, in their own sustainability reports, their annual reports and their marketing. This includes AC3.

"We've given AC3 a report that tells them exactly what they've saved through their partnership with us," says Whelan.

STRONGER TOGETHER

"When people think of core leasing services, they don't instantly think of sustainability," says Whelan, "but that's exactly what it is."

HPE has partnered with AC3, providing it with core leasing services, for nearly a decade. The relationship has continued during the different evolutions AC3 has experienced over the period, says Whelan, and reams of data has been fed back to AC3 regarding its ecological footprint.

HPE's Circular Economy Report details environmental impact statistics including energy savings equivalent to the annual consumption of more than 17,000 households, carbon dioxide emissions saved of more than 42,000 cars, plastic returned for recycling equivalent to more than 140 million plastic bottles and waste kept from landfill equivalent to around 350,000 moving boxes.

AC3 also takes advantage of the GreenLake offering. This edge-to-cloud platform is a sustainability focused consumption model that saves, on average, 30 percent of total costs. "You use the asset when you need the asset, you don't have to build out extra space on your data centre," says Whelan. "You don't have to power up assets that are going to sit idle, and then when you've used those assets for a period of time, you return them to HPE and they redeploy them."

AC3's joint commitment to advancing sustainability then flows on to its customers, as there is hard data that can be passed along the supply chain, explains Whelan. "The majority of AC3's customers will have a sustainability agenda. They'll have statements and targets." This is the first step, he says, followed by a more detailed investigation of underlying assets and undertaking the change from a 'use and dispose' methodology to a circular one.

After analysing an asset, how long it will be needed for and what business benefit it will afford, organisations could consider non-traditional models like GreenLake, says Whelan, "to make sure they're getting what they need from the asset, but also making sure it then gets deployed and doesn't negatively impact the environment," he adds.

Combining the benefits of a product like GreenLake and the HPEFS Circular Economy report is a great way to spread the green message, he adds, a message that he believes most IT departments are keen to embrace.

"It's probably the most tangible way a CIO (chief information officer) can say, 'this is what I'm doing to help contribute towards our organisation's sustainability initiatives," he concludes.

Cyber attacks and prevention

As incidences of cybersecurity attacks grow daily, relying on response and mitigation must give way to preemption and prevention.

By Mark Troselj, Group Vice President for Australia and New Zealand, Splunk

Studies indicate that cyber attacks are increasing. Data breaches and costly ransomware infections are leaving security teams exhausted in their ongoing battle to mitigate the risks, leading to concerning headlines across the globe.

There is, at least, some good news for the local region. Compared to other countries, Australia and New Zealand reported fewer cyber attacks in the last two years, including data breaches (35 percent, compared to 49 percent of organisations in other countries), business email compromise (33 percent versus 52 percent) and successful phishing attacks (33 percent as opposed to 48 percent). On a bright note, while many organisations face cyber security skills shortages, only 22 percent of staff in the region reported that they were considering leaving their position, compared to 38 percent of respondents elsewhere.

Unfortunately, these nuggets are outweighed by other, grimmer statistics – such as the revelation from the Australian Cyber Security Centre (ACSC) that Australia had to deal with a cyber attack every eight minutes in the 2020-21 financial year – and insights gleaned from Splunk's recently released 'State of Security 2022' report. The report was conducted in January and February 2022, and included responses from over 1200 security leaders and practitioners working in 11 different regions – Australia, Canada, France, Germany, India, Japan, the Netherlands, New Zealand, Singapore, the UK and the US. It reveals two alarming trends:

- *Cyber crime is rising dramatically across the globe – 49 percent of organisations reported suffering a data breach in the last two years (compared to 39 percent previously), with 79 percent encountering ransomware attacks and 35 percent losing access to data and systems due to such attacks.*
- *The so-called 'great resignation' is having an impact – along with fresh security challenges associated with remote working, experienced security personnel leaving the industry has exacerbated the ongoing talent shortage in the industry (73 percent of respondents noted workers resigning because of burnout).*

And while the situation in Australia and New Zealand may seem less grave, with 'only' 72 percent of respondents finding the security landscape more difficult, compared to 86 percent globally, it has become very clear that tackling cyber crime, and ransomware attacks in particular must be an absolute priority for any organisation. One positive sign is that over two-thirds (67 percent) of global organisations are investing in advanced analytics and security operations automation to address the growing problem of cyber crime.

Traditionally targeting specific businesses, ransomware is now capable of disrupting critical infrastructure across countries and has even become another warfare tool.

Mark Troselj

FIGHTING BACK

Splunk's recently launched strategic cyber security arm, SURGe, has conducted research into ransomware, with the aim of providing defenders with actionable knowledge.

Analysing 10 major ransomware strains, including Lockbit, REvil and Blackmatter, it discovered that, while speeds vary between ransomware types, the rapidity of encryption (up to 60GB in under 45 minutes) means an organisation can potentially lose access to critical customer data, IP and employee information in less than an hour. And that's just the average speed. LockBit, one of the most prolific ransomware families, can encrypt 100GB in under six minutes. This means there is simply no time for counteraction.

> Experienced security personnel leaving the industry has exacerbated the ongoing talent shortage in the industry.

Added to this is the factor that organisations typically take three days to discover that they have a ransomware infection (Mandiant's '2021 M-Trends report').

Above all, SURGe's research demonstrates that organisations need to stop relying on response and mitigation strategies, and focus on preventing infections, utilising such practical steps as better patching, network segmentation, centralised logging, comprehensive asset inventory, MFA (multi-factor authentication) and proactively seeking ransomware actors on the network before they can deploy their ransomware binaries.

Pathway to cloud governance

Of the many considerations organisations must address when migrating to the cloud, financial governance and cloud economics are key. The AWS Cloud Economics program can provide vital assistance.

Photo by Towfiqu barbhuiya from Unsplash

While the cloud's value extends far beyond the total cost of ownership (TCO) to encompass factors like flexibility, scalability, staff productivity and operational resilience, it is important that organisations adhere to an appropriate governance policy to validate and monitor their cloud spend.

The AWS Cloud Economics program can be an invaluable guide in delivering an effective migration strategy and business case.

While the AWS Cloud Economics program is useful for all sorts of different businesses and different business sizes, it's primarily aimed at those organisations looking to implement large-scale cloud migrations, such as enterprise or government. It's a program that provides a comprehensive set of tools to facilitate that journey, while exploring the cost considerations of the migration, because there are multiple pathways to migrate, and each will require different financial input. Fundamental to the exercise is deciding the most suitable migration approach for each key workload as well as rightsizing, working out which is the most suitable pathway for any individual organisation to take.

To optimise the journey to migration, particularly large-scale migrations, the AWS Cloud Economics program comprises the following steps:

READINESS

This is where the assessment of the situation takes place, when the AWS partner team and the customer determine how ready the business is to begin its migration journey by examining the current workload and the overall operations. More than a simple check from a budgeting perspective, this is where the levels of support for the migration and the current agility of both the organisation as a whole and the ICT services will be assessed. Potentially, all the business's relevant stakeholders will be involved in a series of workshops to gather the necessary information.

TOOLING AIDED ASSESSMENT

Larger migrations may benefit more from using this approach, with multiple tools being utilised. AWS has a number of appropriate products, including its Migration Portfolio Assessment (MPA) tool, and there are also partnering companies that provide specialised software probes and tools to intelligently collect useful data regarding workflows and other processes from the customer's environment.

GENERATE THE BUSINESS CASE

Collating and analysing the data gleaned from the previous stages – as well as the workshops, additional manual collection and business priority input – enables the creation of the business case, which will highlight the projected savings the migration is projected to realise.

RUN THE PILOT

A pilot of the migration may take up to four months, or longer, depending on the nature of the applications and the workloads. The more forensic the planning and pilot stages, with any identified wrinkles ironed out and every detail verified, the smoother the actual migration is likely to be. Confident that all the risks have already been managed and mitigated, it's a simpler task to leverage the scalable automatic migration tools to perform a large-scale migration more quickly and efficiently.

CONTINUAL IMPROVEMENT

The actual migration is not the end of the journey for the Cloud Economics program. In fact, even while the migration is rolling out, the question of whether it can be reduced should be asked. If it's possible to shorten the migration's duration, this will directly influence the outcome of the business case. While the migration is running, there is also the parallel run of the current on-premises data centres, compute, and storage still operating and incurring costs. This is a great opportunity to efficiently reduce the parallel run, to enable a more economic model.

And once the migration is complete, there is always more opportunity to review and possibly perform further optimisation; for example, using a more efficient compute type to replace the current one, or using a cloud native database service.

Running around the regions

When embarking on your AWS cloud migration journey, having settled the 'which' question, the next consideration is the 'where' – is running a single AWS region or multi-region the best option for your organisation?

Once you have made the decision to migrate to either a public or hybrid cloud solution utilising the services of AWS (Amazon Web Services), one of the next elements to consider is where your solution will be located. There are a few options available for organisations in Australia and New Zealand, and each has its own advantages and disadvantages.

At its most basic, it comes down to a trade-off between risk appetite, accessibility and availability versus cost.

CHOOSING AN AWS REGION

The AWS EC2 is hosted in multiple locations worldwide. The locations comprise regions, availability zones, local zones, AWS outposts and wavelength zones. Each region is a separate geographic area and AWS has 26 different geographic regions around the world, with plans announced for a further eight in Australia, New Zealand, Canada, India, Israel, Spain, Switzerland and UAE.

An AWS account provides users with the ability to launch Amazon EC2 instances in locations that meet their requirements, but the specifics of that account will determine which regions are accessible. Global or multinational organisations may be physically located in one region, but choose to launch instances in Europe, for example, to be closer to their customers based on that continent or to comply with certain legal requirements.

"The recommendation is to place the workload where it is closest to the majority of its users," says Greg Cockburn, Head of Hyperscale Cloud at AC3. "Most of our clients stick to the ap-southeast-2, which is Asia Pacific (Sydney).

"Each region has an entry point in the closest location. So, if users are located in Sydney and have access to the Sydney end point, they will have a better response time."

The seven other Asia Pacific locations are ap-east-1 (Hong Kong), ap-southeast-3 (Jakarta), ap-south-1 (Mumbai), ap-northeast-3 (Osaka), ap-northeast-2 (Seoul), ap-southeast-1 (Singapore) and ap-northeast-1 (Tokyo).

The potential downside of selecting just one of the locations to host your infrastructure relates to availability. "If the whole region goes down, then nothing works and all of the organisation's workloads also go down," says Cockburn.

MULTI-REGION SOLUTION

It is the potential for such an incident that is the main reason an organisation may choose to select more than one region, primarily for disaster recovery. If something happens on the AWS data centre network program or storage program and the host region becomes unresponsive, users will be unable to access the servers.

An alternative infrastructure that creates the same workflows, load balancers and database in a different region means there is a script available to switch over to the next region if necessary. Simply put, it's a safety device and the great advantages of multi-region solutions are reliability and high availability.

ON THE OTHER HAND...

The trade-off is cost. If you double your infrastructure, you will double the cost. However, just as a car with four wheels will only have one spare, a potential way forward is to limit the disaster recovery footprint.

"One of our clients has five servers in its main region, but only one server in its disaster recovery region," says Cockburn. "If a switchover happens, they can spin up more servers in the region to solve the workload issue."

In a normal, everyday situation, the customer will save costs by running a minimally sized instance, and scaling up if and when it becomes necessary.

"You do have to keep everything in sync all the time, however, because you never know when you may need to switch over," warns Cockburn. "This means continual backups, database synching or application version syncing. You need to ensure you are running the same version of an application in each different region."

"If a switchover happens, they can spin up more servers in the region to solve the workload issue."

Photo by Tima Miroshnichenko from Pexels

SERVICING SENTINEL

Microsoft Sentinel is among the most advanced of SIEM solutions and AC3 offers various pathways to assist organisations looking to take advantage of its many benefits.

Previously known as Azure Sentinel, the scalable, cloud native, SIEM (security information and event management) and SOAR (security orchestration, automation and response) solution is now called Microsoft Sentinel.

It delivers security analytics and threat intelligence across enterprises, providing a single solution for attack detection, threat visibility, proactive hunting and threat response. It's a solution that is deeply infused with machine learning (ML), which means it delivers powerful built-in ML analytics, covering all the prevalent threats and data types connected to the specific SIEM.

It also offers support for users to build their own ML within the technology.

As a cloud native technology, Sentinel naturally integrates with the wide array of Azure and Microsoft technologies and security solutions, such as endpoint protection platforms, endpoint detection and response (EDR) solutions and cloud access security brokers (CASBs). Microsoft's large ecosystem of security and other IT solutions that natively integrate with the platform includes 365 Defender, Azure Defender, Office 365 and Azure.

Sentinel does not only support Microsoft services, however, it also integrates with a large catalogue of vendor and community provided connectors that cover all major cloud platforms, hardware and software solutions.

"Where it probably makes most sense would be if the customer has some aspect of Microsoft in their hybrid typology, but they don't need to be 100 percent in," says Jonathan Black, Lead Enterprise Architect at AC3.

AC3's Microsoft Sentinel Design and Build program provides customers with an experienced cyber security expert who will workshop, design and build the platform in line with Microsoft best practices.

> "Where it probably makes most sense would be if the customer hassome aspect of Microsoft in their hybrid typology, but they don't need to be 100 percent in.
> **Jonathan Black, Lead Enterprise Architect, AC3**

Sentinel's robust API interface allows for flexible interfaces based on the user's requirements, which makes it an appealing solution for organisations looking to interface with the technology using different methods, and not solely via Sentinel's own workspace interface.

"As with all security products there is customisation and configuration of alert rules and thresholds," says Black.

It's a relatively easy process to start, he adds, but requires expert guidance. Once installed, it is possible to build in automation to create remedies and other processes.

COSTINGS

As with most SIEM solutions, price depends on the volume of logs and events ingested daily, measured in gigabytes – the more gigabytes required, the greater the financial investment.

HOW AC3 CAN HELP YOU LEVERAGE SENTINEL

Professional services:

- Microsoft Sentinel Best Practice Assessment – one-off analysis on Sentinel environment and business security practices
- Microsoft Sentinel Design and Build – one-off project to design and build fresh Sentinel instance

Managed services:

- SIEM Platform Management – entire SIEM platform management
- Managed Detection and Response for SIEM – security alert management and advice of incidents
- SecOps – customisable response purchased in committed hours per month

Choosing between reserved capacity (or committed tiers) and pay as you go, customers can access extended services such as extra storage, automation or 'build your own ML' for an additional cost.

"If you're selective on what you're sending to the platform, it can be fairly cost-efficient," says Black. "If you throw everything at it, your prices are going to increase."

Microsoft also includes allowances for certain M365 user licences, which allow for up to 5MB per user per day to be ingested, along with free ingestion from certain Microsoft Data Sources such as Azure and Office 365 activity and audit logs. AC3 also offers a best practice review for organisations that have already stood up Sentinel but aren't sure whether they are getting optimisation from the platform.

Enjoying *Three*?

Did you know that you can also read and subscribe to *Three* online?

Visit **ac3.com.au/Three** for the digital version.