



CHANNEL INSIGHTS


SUSTAINING DIGITAL EXCELLENCE

Why professional services are key to accelerating IoT adoption

...eseye



ISSUE | 2022

 AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

SDC-CHANNEL.NEWS

INVESTING IN CHANNEL SUPPORT TO SURVIVE THE EVOLVING SECURITY LANDSCAPE

as workforces are more dispersed and more vulnerable to attacks, security needs to be tighter

HOW TO UNLOCK UP TO 50% PROFIT MARGINS WITH 'BUNDLES'

why the channel (in particular MSPs) needs to consider offering their clients bundled solutions instead of 'single-solution sells' to profit

WHAT IS A CLOUD CENTRE OF EXCELLENCE AND HOW CAN IT HELP CHANNEL PARTNERS

A CCoE is built to support partners, amplifying cloud expertise to ensure they can design and migrate their clients to the cloud safely

SDC CHANNEL SUMMIT

THE 2ND SDC CHANNEL SUMMIT REGISTER FREE TODAY

We are delighted to introduce our second virtual conference. Based on extensive research conducted with attendees at the first event, as well as survey feedback from our Channel data base (based on attendees to the previous SDC Channel Events), we're confident that we've produced an essential education opportunity for the Channel as it seeks to address both the challenges and opportunities of digital change management:



**Channel
Summit
10-11 May**

Over the course of two, consecutive morning sessions (giving attendees plenty of time to run their business as well), we will be providing invaluable insights, advice and recommended actions to help Channel organisations as both they, and their customers, get to grips with what it means to create, develop and optimise a truly digital business.

Topics include:

1. SKILLS + TRAINING
2. SUSTAINABLE BUSINESS DEVELOPMENT
3. SIMPLIFYING THE SOLUTION STACK
4. SELECTING THE RIGHT SECURITY PARTNERS

Register for free here: <https://sdc-channel.com>

Sponsored by:



PARK PLACE
TECHNOLOGIES

In association with:



Editor's view

By Phil Alsop



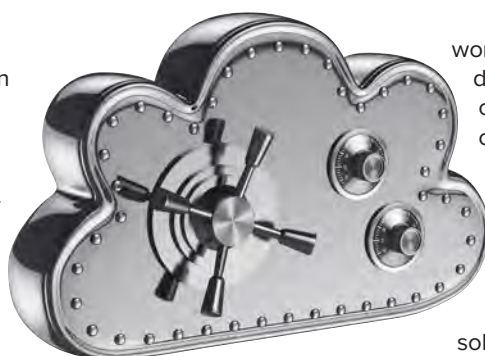
Be confident when it comes to cloud and cybersecurity

MANY OF THE NEWS STORIES in this issue of SDC Channel Insights focus on one of two topics: cloud and security. Cloud seems to be where everything is heading, and security seems to be where everything could grind to a halt.

Channel organisations need no reminder that more and more of their customers are demanding cloud and managed services. Neither does the increasing importance of security come as any surprise. Nonetheless, many channel organisations (the majority?) have yet to develop a coherent, long-term, sustainable strategy for offering their customers the particular blends of hybrid IT which they require (a likely mixture of on-premises, colocation, hyperscale cloud, vendor software-as-a-service solutions and channel-created managed services).

After all, creating such a complex, interdependent, seamless hybrid IT infrastructure is no easy task. That's why end users are turning to the Channel to do it for them – it's a thankless, extremely demanding, time-consuming project which can never ever be completed, because there will always be new solutions arriving which need to be integrated along the way.

Equally complicated and 'impossible' is the problem of managing cybersecurity in such a complex, connected



world. Estimates vary, according to different definitions, but there are almost certainly around a 100 different types of cybersecurity solutions (especially if you add in the data protection aspect of data storage), if not more. Where does an end user start, or, for that matter, a Channel expert, when it comes to understanding all of these cybersecurity nuances, let alone working out which of the 100 solutions are required!

The only sensible way forward would appear to be one of collaboration and partnerships. No one organisation can hope to be expert in everything cloud and cybersecurity. But one Channel organisation can know enough experts, and understand how to build complex solutions, to help their customers on the road to digitalisation. Choosing the right partners and technical solutions is crucial, and there are no short cuts. Long hours spent understanding a range of technologies, and then working out where best to source them, is the only way to be confident that the solutions stack a Channel company assembles is not just fit for purpose, but will exceed customer expectations.

If I had to give one piece of advice when it comes to working out a cloud and cybersecurity strategy? Understanding what you don't want to do, or can't offer your customers, is just as important as working out what it is you can and do want to do.



Editor

Philip Alsop +44 (0)7786 084559

Sales Manager

Peter Davies +44 (0)2476 718970

Sales Executive

Jessica Harrison +44 (0)2476 718970

Director of Logistics

Sharon Cowley +44 (0)1923 690200

Design & Production Manager

Mitch Gaynor +44 (0)1923 690214

Publisher

Jackie Cannon +44 (0)1923 690215

philip.alsop@angelbc.com

peter.davies@angelbc.com

jessica.harrison@angelbc.com

sharon.cowley@angelbc.com

mitch.gaynor@angelbc.com

jackie.cannon@angelbc.com

Circulation & Subscriptions

+44 (0)1923 690214 circ@angelbc.com

Directors

Stephen Whitehurst: Chairman

Scott Adams: Chief Technical Officer

Sukhi Bhadal: Chief Executive Officer

Published by:

Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry

CV5 6SP

T: +44 (0)2476 718970 E: info@angelbc.com



SDC-Channel Insights is published X times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd. © Copyright 2022. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

32

WHY PROFESSIONAL SERVICES ARE KEY TO ACCELERATING IoT ADOPTION

Throughout history we have seen plenty of examples of companies that have failed to adapt when there was a sea change in the prevailing business model

16 Investing in channel support to survive the evolving security landscape

VIPRE explains that as workforces are more dispersed and more vulnerable to attacks, security needs to be tighter

18 How can you unravel complexity to launch a cybersecurity business?

The world of technology and cybersecurity is becoming more and more complex, which is why it is so important that partners simplify things for themselves and their customers.

20 Channel insights: Video exclusives

In addition to the articles in this issue of SDC Channel Insights, you can also watch and listen to a great selection of

exclusive video interviews covering a range of technology and business issues which matter to the Channel.

24 Cybersecurity needs have outpaced the legacy MSSP model...throwing more tools at the problem won't fix it!

Better integration and unified visibility within an open security operation platform model is vital for the channel to adapt to the evolving threat landscape and dynamic customer demand

26 Why it's time for managed service partners to start working for customers, not just with them

As businesses have been forced to embrace remote and now increasingly hybrid working approaches, more

NEWS

- 06 93% of IT industry to adopt cloud tech within five years
- 07 Channel partners failing to realise importance of sustainability credentials when winning new business
- 08 Cloud security report highlights multi-cloud problems and skills shortages
- 09 Zero Trust investments increase
- 10 Research reveals top data management challenges
- 11 Lack of a holistic cloud strategy is causing a cloud boomerang effect
- 12 83% of successful ransomware attacks feature double or triple extortion tactics
- 13 Employees feel 'new normal' has left them more vulnerable to cyberthreats
- 14 Working from home increases 'digital anxiety'

have begun to realise the benefits these can offer when it comes to enabling more decentralised workforces

28 **How to build the customer-centric model your channel partners really want**

Shifting towards a fully customer-centric business can be more challenging than initially believed

30 **Designing data centres for MSPs and IT Service Providers**

Since the start of the pandemic, the Managed Service Provider and IT Service Provider marketplace have radically changed. As the post-pandemic business landscape begins to take shape, it's critical for MSPs and ISPs to choose the right data centre partner

34 **How to unlock up to 50% profit margins with 'bundles'**

Why the channel (in particular MSPs) needs to consider offering their clients bundled solutions instead of 'single-solution sells' to profit.

36 **An edge computing platform has become vital for solution-builders and service-providers**

Partnering with a purpose-built edge platform is becoming essential so service providers and application-builders fully exploit the immense potential of the edge model

38 **What is a cloud centre of excellence and how can it help channel partners?**

A CCoE is built to support partners, amplifying cloud expertise to ensure they can design and migrate their clients to the cloud supported with confidence and without many of the pitfalls that have plagued the industry in recent years



34

93% of IT industry to adopt cloud tech within five years

Survey, conducted by Hornetsecurity, reveals that hybrid cloud solutions are the long-term target for two in three companies.

A HYBRID CLOUD ADOPTION survey of 900+ IT professionals primarily based in North America and Europe found that the majority of businesses (93%) are adopting a hybrid of cloud and on-premise solutions, or migrating fully to the cloud within 5 years.

Half of respondents (51%) reported that they will be 'mostly in the cloud' in 5 years, with one or two workloads remaining on premise. 28% of respondents said they will remain 'mostly on premise', with a workload or two in the cloud.

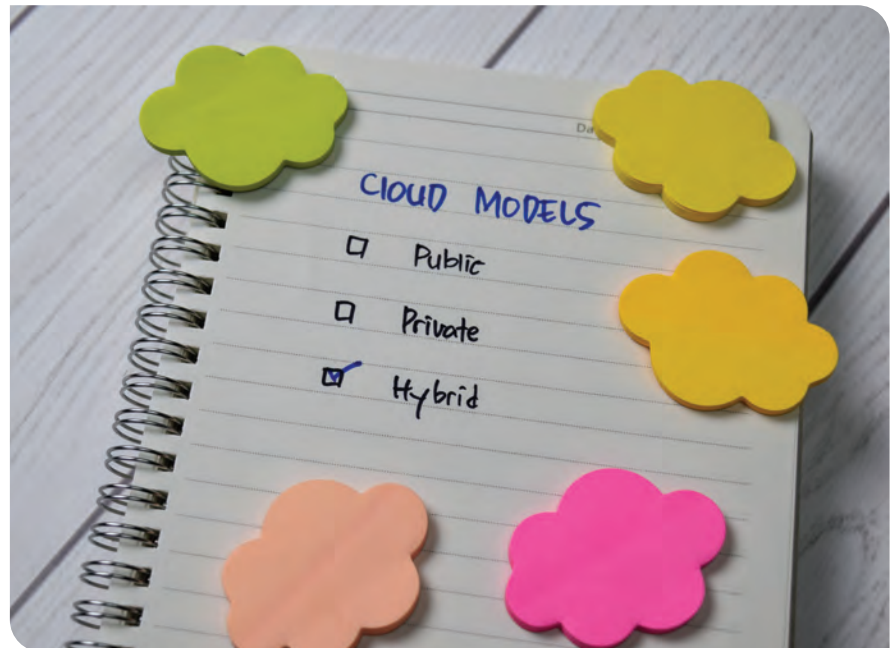
67% of IT professionals see a hybrid cloud solution as a permanent destination

While 29% of respondents said they are using hybrid cloud solutions as a stepping stone to a full cloud environment, 67% of respondents see hybrid as a final destination for their infrastructure due to workloads that must remain on premise. The rest claim to be remaining 100% on premise. When asked why companies were remaining on premise, many respondents cited data control, security, and cost concerns with cloud technology.

34% of companies cite trust issues with cloud as reason for workloads remaining on premise

The hybrid cloud adoption survey also found that trust issues with the public cloud are present within companies of all sizes, with 31-36% of all surveyed company size categories reporting concerns.

The survey also shows that with experience comes more distrust in the public cloud. Respondents with 20+ years of experience were more likely to express concerns with the trustworthiness of cloud platforms (34%) than those with 1-5 years of experience (24%). Half of all respondents mentioned 'legacy systems or software'



as another major reason certain workloads must remain on premise, while 'application compatibility' was reported as a roadblock to cloud migration for 4 in 10 companies. Industry regulations such as GDPR, HIPAA and CMMC among others were also cited as an obstacle for cloud adoption by 29% of respondents.

Multiple challenges blocking cloud adoption

Companies say they are holding back from full cloud migration due to a lack of 'technical knowhow or certified staff' (48%), difficulties with 'application of best practices within the company' (33%), issues with connectivity (33%), and 'secured access' (29%).

The most common workload preventing IT departments from lifting all services to the cloud was 'Print & Imaging Services' (55%). Databases, file storage and application services are also cited as reasons for remaining partially on premise with 50%, 45%, and 43% of respondents indicating such respectively.

Hornetsecurity's survey reveals that hybrid cloud solutions still bring with them several challenges. Chief among them is 'monitoring and security', with half of respondents expressing concerns in this area. 'Networking and connectivity' is another concern shared by nearly half of all respondents (48%). Finally, 'training and certification', 'manageability and tooling', and 'resiliency and data recovery' also factor into the concerns shared by 35%, 35%, and 33% of respondents respectively.

Companies using MSP services more likely to use cloud solutions vs on premise

47% of respondents who form part of internal IT teams reported that they see their workloads 'mostly in the cloud' in 5 years, versus 52% of respondents whose company uses MSP services, and 54% of respondents that work at MSPs. Internal IT departments report a lack of trust in cloud services at almost the same rate as those using MSP services, with 34% and 33% respectively.

Channel partners failing to realise importance of sustainability credentials when winning new business

Survey reveals that 10% of channel respondents have failed to demonstrate sustainability pedigree and have lost business as a result.

DATASOLUTIONS, the specialist distributor of innovative IT and security solutions, has revealed more findings from its 'How sustainable is the UK channel?' survey of UK channel partners and end-user IT decision makers. The latest findings highlight a growing shift in the IT procurement landscape related to sustainability and how channel partners are underestimating how important their credentials will be in the coming years.

Lack of sustainability action impacts the bottom line

The changing IT procurement landscape is already inflicting pain on some organisations across the channel. 10 percent of channel respondents conceding they had lost a contract or tender because they could not demonstrate a sustainability pedigree. With sustainability on the agenda across the IT industry, many predict this will continue to increase in the coming years.

A growing priority for the channel

The survey also asked both channel respondents to rate four criteria (sustainability, price, performance and cost savings) based on their importance when it comes to IT procurement, and how this may change. Sustainability lagged a distant fourth, with channel respondents scoring it an average of 4.9 (on a scale of 0 to 10). This is compared to the three other criteria with price, performance and cost savings achieving average scores of 7.8, 7.9 and 7.3.

The picture changes when respondents are asked about their priorities in the next two years. Channel respondents awarded sustainability a 6.7 average score, compared with 7.6 for price, 7.8 for performance and 7.4 cost savings. Some 10 per cent felt it would be the

single most important criteria by then, with a further 28 per cent awarding it their joint highest score.

The figures above hint not only that sustainability will become an increasingly important consideration for UK end users in the coming years, but also that some resellers and MSPs may be underestimating its relative importance among their customers (both now and in two years' time).

Vendors not moving fast enough

With the likes of Oracle and IBM setting net zero goals, many within the UK channel have asked whether or not vendors are moving fast enough. When asked, just two percent of channel respondents "strongly agreed" that their vendors are doing enough to make their technology more sustainable, with 25 per cent agreeing "somewhat". Clearly more action needs to be taken by vendors, and more quickly.

Techies Go Green

The Techies Go Green initiative, which was founded by DataSolutions, is a movement of IT and tech-oriented

companies committed to decarbonising their businesses. Launched back in March 2021, over 160 signatories have now joined and began their sustainability journey. Signatories include Softcat, Version 1, Sapphire and ColorTokens. DataSolutions intends to double this by the end of 2022.

Michael O'Hara, Group Managing Director, DataSolutions, said: "What our sustainability report has shown is the growing importance of action being taken across the UK IT channel industry. It is no longer enough to pay lip service to this - if you don't act and set an example, this could impact on your bottom line. We feel this is a positive sign that priorities are shifting, and whilst it doesn't factor alongside price and performance just yet, sustainability is increasing in importance when it comes to which companies do business with who. Take us for example, we began our journey by moving our ERP system and other corporate applications to the cloud, adding electrical cars and charging points to the business while cutting down on business travel even after restrictions have eased."



Cloud security report highlights multi-cloud problems and skills shortages

Misconfiguration is the number one cause of cloud-security incidents in 2021.

CHECK POINT® SOFTWARE TECHNOLOGIES has released its 2022 Cloud Security Report. As organizations continue to adopt the cloud, with 35% running more than 50% of their workloads on the likes of Azure, AWS and GCP, they struggle to manage the complexity of securing their cloud infrastructures across multiple cloud platforms, while also suffering a cyber-skills and knowledge shortage.

The global report, based on a survey of 775 cyber security professionals, also revealed that cloud security incidents were up 10% from the previous year with 27% of organizations now citing misconfiguration, way ahead of issues like exposed data or account compromise.

Organizations are struggling to bring security into the DevOps cycle, compounded by a skills shortage witnessed by 45% of companies. Only 16% of respondents said they had comprehensive DevSecOps in place and 37% were just starting to implement

DevSecOps into their cloud application development process.

While perceived cost savings and ease of use were the original drivers for using cloud vendor security, there is an increasing realization that the complexity of managing three or four different security platforms argues in favour of an independent cloud security solution to streamline security across all cloud platforms. In fact, 54% of those surveyed thought that an independent security vendor would be better suited to their needs than the cloud platform provider. A key consideration in making the decision between cloud native and a third-party security vendor was a potential reduction in complexity provided by an integrated solution, cited by 56% of respondents.

Further adding to the complexity of multi-cloud security, respondents ranked ensuring data protection and privacy for each environment at 57%, having the right skills to deploy and manage a complete solution across

all cloud environments at 56%, and understanding service integration options at 50%.

There is also an increasing need to deploy application protection in the cloud with this capability going up by 11% in the last year to become the 3rd highest area of focus, quoted by 53% of the survey sample. According to the report, 57% of respondents say that they expect to run more than half their workloads in the cloud within the next 12 to 18 months and, of those, some 76% were using two or more cloud providers.

As the move to the cloud gathers pace, the ability to streamline cloud security becomes vital, as 75% of organizations are in favour of a single unified security platform with single dashboard, where they can configure all the policies needed to protect data in the cloud. Currently 80% have to juggle three, or more separate security solution dashboards to configure their enterprise cloud footprint.

TJ Gonen, VP of Cloud Security at Check Point, commented: "It is clear from this independent survey that security teams are finding the increased reliance on the cloud a bit of a challenge. Faced with the skills shortage, organizations need to do everything they can to simplify their cloud security management. An integrated third-party solution that covers all cloud platforms with a single management dashboard would relieve much of the pressure and reduce the risk of increasingly common misconfigurations, while also reducing workloads and providing the security environment to develop, deploy and manage applications in the cloud. This was the key driver for Check Point to develop its CloudGuard cloud security suite."



Zero Trust investments increase

Illumio has released new findings of a commissioned study conducted by Forrester Consulting that explore how organizations are approaching their Zero Trust strategies in 2022 to better navigate the remote world brought on by the COVID-19 pandemic and continuing digital transformation initiatives.

THE FORRESTER STUDY, which surveyed decision-makers at large organizations in North America, Europe, the Middle East, Africa (EMEA), and the Asia-Pacific (APAC) region in September 2021, revealed that more than 75 percent of leaders surveyed cited the importance of Zero Trust to combat mounting security threats. The study also discovered that teams are still fighting to catch up with critical initiatives (over 60 percent of respondents say they were unprepared for the rapid pace of cloud transformation and migration) and are increasingly turning to Zero Trust and micro-segmentation to better adapt to today's hybrid realities. Additionally, the study uncovered that security leaders believe:

- Advanced Zero Trust programs pose clear organizational benefits, including increased organizational agility (52 percent), safer cloud migrations (50 percent), and support of digital transformation (48 percent).
- Zero Trust adoption will continue to mature, with 78 percent of firms planning to bolster Zero Trust security operations in the new year.
- Implementing Zero Trust technologies can address emerging security gaps, but most enterprises are still in early stages of adoption. Only 36 percent of organizations have started to deploy Zero Trust solutions, and merely 6 percent of them have fully implemented their Zero Trust projects to date.

Lack of Expertise and Stakeholder Buy-in Compounds Implementation Challenges

Today, security leaders recognize micro-segmentation as a key technology pillar for achieving Zero Trust at scale. In fact, 73 percent of business leaders consider micro-

segmentation and Zero Trust Network Architecture (ZTNA) to be “critical technical foundations” for their organization's Zero Trust strategy.

Despite leaders acknowledging the importance of micro-segmentation, adoption rates are lagging. The top obstacles facing successful micro-segmentation adoption specifically remain a lack of workforce expertise (nearly two-thirds of respondents believe that internal teams lack the time, subject matter expertise, and skills to implement best practices for micro-segmentation), and an inability to identify the right Zero Trust micro-segmentation pilot (44 percent of leaders report their organization needs help in identifying and designing the most appropriate Zero Trust pilot – an important step in demonstrating the value of the technology and making the case for further investment). Additionally, although security leaders understand the value of micro-segmentation, they often have trouble successfully articulating that value-add to organizational stakeholders.

Although there's still a knowledge gap around how to efficiently implement micro-segmentation, 62 percent of organizations attempted to use data center firewall and software-defined networking (SDN), but they took too long to deploy—53 percent found them to be too expensive, and 50 percent said these approaches didn't scale.

“As we watch threats evolve and breaches become more devastating, the need to implement Zero Trust strategies has never been more urgent,” said PJ Kirner, CTO and Co-founder, Illumio. “Micro-segmentation isn't an all-or-nothing strategy, the path to a Zero Trust posture can be broken into



bite-sized phases. Start by gaining visibility to see the risk created by open lateral pathways across your interconnected infrastructure and to the internet. Then, assume breach and secure your data by building security controls that close these risky pathways. This incremental approach is a journey that bolsters your security posture to reduce risk and increase cyber resiliency.”

Greater Zero Trust Adoption and Investment Is Ahead

Organizations are planning to increase their investment in Zero Trust and micro-segmentation in the year ahead. Despite reporting difficulties in obtaining funding, two-thirds of those surveyed say they are planning to expand their Zero Trust budgets in 2022—allocating 36 percent of their total spend to micro-segmentation projects.

Survey findings revealed that security leaders are counting on micro-segmentation to help in a variety of areas crucial to organizational success amid the new business landscape, including bolstering cloud and data center transformations (68 percent), and increasing support for new business and operational models (63 percent).

Research reveals top data management challenges

Research from Quantum and ESG reveals growing cyber threats, data sprawl and storage costs as top challenges in data management.

SURVEY conducted in partnership with ESG Research highlights the challenges and opportunities facing IT leaders: 82% have paid ransoms; 88% say retaining data longer is key to business value creation

Quantum Corporation has released new survey data that reveals the most common challenges organisations struggle with around effective data management, storage and analysis. The survey, conducted by ESG Research in fall 2021, queried hundreds of IT professionals and line-of-business leaders across North America, the UK and Asia-Pacific.

Unstructured data is expanding at massive volumes and remains key to business growth – according to the survey seven out of ten management teams put their data at the core of growth – but there are key trends emerging that will have an impact on the success of capitalising on this data moving forward. The survey findings paint a picture of changing data models that create management challenges, leaving data more vulnerable to security issues, such as ransomware attacks, that can have a devastating impact on businesses.

Key findings from the survey include:

- Unstructured data management, storage complexity and cost remain barriers to adoption, resulting in valuable data being discarded or mismanaged
- Respondents see unstructured data as underleveraged and overly complex: 52% of c-level respondents strongly agree that the opportunity exists for their organisation to better leverage its existing data to create business value. Despite its promise, 38% strongly agreed that the complexity and volume of data produced makes it difficult to understand what data can be used to generate business value.

Data quality and storage costs most often inhibit data management strategies: Ensuring data quality (42%) and data storage costs (38%) are the top two challenges cited when it comes to data management.

- Data retention is top of mind: 78% of organisations do not store data on primary storage for the amount of time they would like to. 88% of respondents say retaining more data longer is an avenue to greater business value creation, but 80% of respondents say determining which data to delete and when is complex and time consuming.
- Organisations struggle with when to delete or store data: More than half of the organisations surveyed (58%) feel they have recently eliminated data with value. Privacy protection and compliance related pain points are the top reasons why valuable data is being discarded before it can create business value.

Data sprawl and hybrid cloud models create vulnerable environments

Data continues to be distributed and mobile: 78% of survey respondents said their organisation frequently migrates data between environments (cloud, on-prem, edge), with a plurality opting for a hybrid cloud model that stores most data on a public cloud infrastructure, with some data remaining on-premises. Data sprawl makes management more challenging: 88% of respondents confirmed that distributed data complicates implementing an end-to-end data strategy.

Data migration becomes a security concern: 87% of respondents say securely moving data from one environment to another causes them concern. This trend combined with a lack of formal data retention and destruction strategy – nearly 3 out of 4 organisations represented (74%) have not formalised their data retention/

data destruction strategies – creates an environment rich for ransomware and cyber-attacks.

Growing cybersecurity threats require new approaches

Ransomware attacks in the enterprise are growing: Two out of five respondents reported that their organisation had been a victim of a successful ransomware attack in the last two years, with 82% of organisations defaulting to paying the ransom.

Ransomware can have an impact beyond budgets: In addition to the cost of the ransom itself, attacks can have an impact on organisation productivity – the survey found that the median cost for ransoms was reported as \$375K – which equates to the cost of approximately 2.1 hours of downtime for a mission-critical workload.

Security concerns are growing, but strategy is lacking: Out of those surveyed, 87% of respondents say their executives are concerned about future ransomware attacks and on the other hand, just 6% of organisations impacted could restore from an air-gapped backup solution.

Cost-effective data retention is critical: Storing data longer can increase resiliency and empower data monetisation – 65% of our respondents say their organisation would be better equipped to recover from an attack if they were able to retain their data for longer.

An increase in enterprise security threats, coupled with concerns around data retainment, cost, data sprawl and cloud-based management models, as well as a lack of response strategy, points to an industry-wide need for more comprehensive and cost-effective data management solutions.

Lack of a holistic cloud strategy is causing a cloud boomerang effect amongst some applications

The majority of IT decision makers plan to increase their organization's use of public cloud (78%) and private cloud (72%) infrastructure over the next 18-24 months. This finding comes from the first part of the annual Cloud Impact Study 2022 from Aptum, a hybrid multi-cloud managed service provider. The report, titled *The Balance of Hybrid*, explores the deployment of workloads on different cloud infrastructures and examines the decision-making process behind their placement.

THE STUDY CANVASSED

the opinions of 400 senior IT professionals regarding their approach to cloud technology. Respondents were from organizations with at least 250 employees in the U.S., Canada and UK across industries including financial services, technology, telecommunications, manufacturing, retail, public education and the commercial sector. It found the majority (86%) of respondents say their organization has adopted a hybrid or multi-cloud approach to cloud deployment.

Most also recognized many of the benefits cloud delivers for their organizations, with the majority agreeing it has delivered on expected efficiencies (90%). Respondents also cited the rate of cloud transformation in their organization has had a positive impact on the following areas:

- Innovation (71%)
- Operational efficiency (71%)
- Workforce mobility and enablement (63%)
- IT expenditure (63%)
- Customer experience (63%)

Indeed, when presented with 12 application categories, respondents said cloud is the preferred hosting option for all of them, compared to just two out of nine categories in Aptum's first Cloud Impact Study in 2021. However, despite recognizing the benefits of cloud, not all workloads are destined for cloud platforms, and some organizations are experiencing a 'cloud boomerang effect' amongst specific



applications. Almost half (47%) of respondents anticipate an increase in their organization's use of traditional (non-cloud-based) infrastructure over the next 18-24 months, up from just under a quarter (23%) in 2021

The study identifies one of the causes of the shift back to legacy infrastructure to be rooted in a lack of strategy. Only 20% of respondents said they have a holistic cloud computing strategy. Additionally, integration of cloud with on-premises systems was cited as the top challenge an organization would face when operating in cloud environments, tied first with data privacy and security challenges.

"When the pandemic hit, many organizations reacted hastily to move applications to the cloud and neglected some workload considerations that have since become apparent. So, while organizations see benefits from the cloud, they could have been more successful in their endeavours when the shift first took place if the requirements of each application were carefully evaluated," explains Chris David, Aptum's Senior Cloud Product Leader. "Contrary to popular belief, the cloud boomerang effect isn't simply about moving workloads from cloud platforms back to traditional infrastructure. More accurately, the

boomerang is the movement of applications between development and operations teams."

The primary focus of development teams is on the creation of new versions of applications, meaning limited time can be spent on administrative duties required to refactor workloads for cloud. Due to this, the onus often shifts back to the operations teams to manage this, and they often lack the necessary skills or resources. If the operations teams lack skills, tools, cloud governance policies, or operational practices to enforce operational standards, these workloads will often come back to legacy platforms.

"To overcome these challenges, organizations need to have a holistic cloud strategy guided by an experienced Managed Service Provider (MSP)," says David. "They can help businesses understand the characteristics that need to be assessed when deciding where each application should be hosted and help them avoid the mistakes that lead to cloud boomerang."

The survey results call for organizations to look at ecosystems, with business objectives and optimization in mind, to avoid placing workloads in inappropriate locations. To save time, money and resources and to increase interoperability, businesses should look to hybrid and multi-cloud specialist providers, with the skills and experience to assist in those decisions.

83% of successful ransomware attacks feature double or triple extortion tactics

New Venafi research shows that ransomware attackers are regularly exfiltrating data, circumventing 'restore from backup' safety measures.

VENAFI has published the findings of a global survey of IT decision-makers looking into the use of double and triple extortion as part of ransomware attacks. The data reveals that 83% of successful ransomware attacks now include alternative extortion methods, such as using the stolen data to extort customers (38%), exposing data on the dark web (35%), and informing customers that their data has been stolen (32%).

Just 17% of successful attacks solely asked for a ransom in return for a decryption key, meaning that many new forms of extortion are now more common than traditional methods. As data is now being exfiltrated, having a back-up of data – while still essential for recovery from an attack – is no longer effective for containing a breach.

The data also shows that cybercriminals are following through with these extortions, often even after a ransom has been paid:

- Almost a fifth (18%) of victims paid the ransom but still had their data exposed on the dark web

- This is more than the 16% that refused to pay the ransom and had their data exposed
- Almost one-in-ten companies (8%) refused to pay the ransom, and the attackers tried to extort their customers
- Over a third (35%) of victims paid the ransom but were still unable to retrieve their data

“Ransomware attacks have become much more dangerous. They have evolved beyond basic security defenses and business continuity techniques like next-gen antivirus and backups,” said Kevin Bocek, vice president of business development and threat intelligence at Venafi. “Organizations are unprepared to defend against ransomware that exfiltrates data, so they pay the ransom, but this only motivates attackers to seek more. The bad news is that attackers are following through on extortion threats, even after the ransom has been paid! This means CISOs are under much more pressure because a successful attack is much more likely to create a full-scale service disruption that affects customers.”

When asked about the evolution of extortion in ransomware attacks, 71% of those polled believe that double and triple extortion has grown in popularity over the last 12 months, and 65% agree that these new threats make it much harder to say no to ransom demands.

This is creating problems for the industry. 72% of IT decision-makers agree that ransomware attacks are evolving faster than the security controls needed to protect against them, and 74% agree that ransomware should now be considered a matter of national security. As a result, 76% of companies are planning on spending more in 2022 on ransomware-specific controls due to the threat of double and triple extortion.

Wider than internal measures, two-thirds (67%) of IT decision-makers agree that public reporting of ransomware attacks will help to slow down its growth. A further 77% agree that governments should do more to help private companies to defend themselves from ransomware.



Employees feel 'new normal' has left them more vulnerable to cyberthreats

A fifth of employees believe their organisation has held back from modernising its processes with new technologies during the pandemic.

ACCORDING to new research published by Advanced, one of the UK's largest software and services providers, nearly two-thirds (57%) of employees believe that the switch to hybrid working has made them more vulnerable to cyberattacks.

Fear of change holding security back

As detailed in the report, 20% of employees feel that their employer is deliberately holding back when it comes to implementing new technologies that might make them feel more secure. Yet, despite this, more than a third (34%) of employees claimed that they would be "concerned" about any changes taking place that might threaten their current working processes.

According to the report, it is this fear of adapting to new technologies and processes, among businesses and some of their staff, that has resulted in 62% of employees seeing their current technology limited when it comes to supporting remote or hybrid working.

The Advanced 2021/22 Trends Report, which surveyed more than 1,000 employees about their experiences working in a post-pandemic environment, comes amid growing concern over how businesses are adapting security policies and technologies to suit the cultural and practical changes many have undergone to maintain productivity levels during the crisis.

Cloud adoption has skyrocketed to cater for a new era of hybrid and remote working, in a change that some analysts believe might now be permanent. While businesses are arguably more agile than they have ever been, they are also more vulnerable, with an increasing number



of remote endpoints contributing to a rapidly expanding attack surface area.

Embedded security essential for 'new normal' productivity

When asked about security, 42% of respondents said that embedded security was the most important form of security when adopting new technologies such as those used in remote working.

Justin Young, Director of Security and Compliance at Advanced, said "Cloud-based technology can provide much higher levels of security than on-site, legacy systems, but only when deployed correctly and implemented alongside adequate staff training and knowledge sharing.

These findings show that, as well as deploying effective technology solutions, there is more that businesses can and should be doing to prepare, educate and reassure their teams for the 'new normal'."

Security as part of a workplace culture

Global consultancy firm, Gartner, published figures at the very beginning of the pandemic that suggested 95% of security failures during 2020 would be down to human error, such as lack of understanding or awareness of security best practices.

Advanced's report suggests that, with hybrid working now a permanent feature of the working landscape rather than a temporary fix to deal with the pandemic, staff education and training is something businesses must tackle head-on.

The report concludes that effectively implementing cloud-based security is really only half the battle when it comes to increasing a company's risk posture. Employees need to be educated and prompted when it comes to best practice security hygiene such as changing passwords, securely storing files, enabling automatic security updates and using multi-factor authentication.

Working from home increases ‘digital anxiety’

Two-thirds of remote workers reported worrying about their online security and privacy, even if nothing is wrong.

WORKING FROM HOME has spiked since the onset of the Covid-19 pandemic in March of 2020. This effort to reduce health risks may have limited the spread of the virus, but according to a new analysis by cyber security provider F-Secure, it may also have helped increase digital anxiety for those working remotely.

In a recent survey,* 67% of internet users who work from home reported they increasingly worry about their online security and privacy even if nothing is wrong, compared to 58% of other users.

Senior Lecturer in Cyberpsychology at Nottingham Trent University Dr. Lee Hadlington, who's research interests include employees' adherence to workplace cyber security practices, said it makes sense that people's sudden shift to telecommuting increased their anxieties about online threats.

"It is not surprising that individuals have started to worry more about cyber security, particularly when working from home. Many individuals were thrust into the 'new normal' of home working with very little preparation, training, or equipment.

Let's not forget, for most individuals in a workplace environment, cyber security is generally a second thought, and is usually something that is seen as the responsibility of someone else in the company.

This, coupled with the fact that many home workers have less than perfect home working environments (e.g. desks in busy parts of the house, limited/poor internet connection, limited working knowledge of internet-based technology), means that these cyber security fears could be symptomatic of a combination of factors," he said.



While worries about online security and privacy were prevalent among all survey respondents, remote workers reported elevated concerns about a myriad of issues, including:

- 65% of those who work from home said the internet is becoming a more dangerous place, compared to 54% of other respondents.
- 63% of remote workers said concerns about data privacy have changed how they use the internet, compared to 48% of other respondents.
- 71% of remote workers said they worry that new internet connected devices – such as wearables and connected home appliances – could lead to a violation of their privacy, compared to 64% of non-remote workers.
- 70% of remote workers felt increasingly uncomfortable connecting to public WiFi due to security risks compared to 63% of other respondents.

"Working from home could also have meant that individuals may have had more time to focus on other aspects of their working life and spent more time engaging in self-reflection and aspects of self-improvement; this could have included a re-assessment of cyber risks in their daily lives. The pandemic also meant people were isolated, with many turned to the one thing they did have access to – the Internet. Of course, spending more time engaged in one activity could lead to an increase in perceptions of risk, particularly when people are being subjected to negative news stories about cyber security related issues," Dr. Hadlington explained.

According to F-Secure Security Consultant Tom Gaffney, managing security while working remotely takes technical security measures that protect data and devices, but also steps to keep people's personal and professional lives separate.

SDC CHANNEL SUMMIT

THE 2ND SDC CHANNEL SUMMIT REGISTER FREE TODAY

We are delighted to introduce our second virtual conference. Based on extensive research conducted with attendees at the first event, as well as survey feedback from our Channel data base (based on attendees to the previous SDC Channel Events), we're confident that we've produced an essential education opportunity for the Channel as it seeks to address both the challenges and opportunities of digital change management:



**Channel
Summit
10-11 May**

Over the course of two, consecutive morning sessions (giving attendees plenty of time to run their business as well), we will be providing invaluable insights, advice and recommended actions to help Channel organisations as both they, and their customers, get to grips with what it means to create, develop and optimise a truly digital business.

Topics include:

- 1. SKILLS + TRAINING**
- 2. SUSTAINABLE BUSINESS DEVELOPMENT**
- 3. SIMPLIFYING THE SOLUTION STACK**
- 4. SELECTING THE RIGHT SECURITY PARTNERS**

Register for free here: <https://sdc-channel.com>

Sponsored by:



PARK PLACE
TECHNOLOGIES

In association with:



Investing in channel support to survive the evolving security landscape

MIKE FOSTER, CHANNEL MANAGER, [VIPRE](#), explains that as workforces are more dispersed and more vulnerable to attacks, security needs to be tighter. They can do this through partnering with an established Managed Service Provider (MSP) who can act as a trusted advisor to create a solid cyber security strategy, SMBs can benefit from the knowledge, skills and solutions available within the channel.



SECURITY is a growing concern across every industry, particularly now with the growth of dispersed workforces around the world. Cyberattacks continue to increase and become more sophisticated, with businesses of all sizes needing to invest in the right support. This is even more crucial for small and medium-sized businesses (SMBs), who may lack the adequate internal resources and teams to protect themselves against such threats.

But, by partnering with an established Managed Service Provider (MSP) who can act as a trusted advisor to create a solid cyber security strategy, SMBs can benefit from the knowledge, skills and solutions available within the channel. MSPs, therefore, need to ensure they leverage this opportunity to support their end customers, while businesses crucially make the necessary investment to keep their network, data and people secure.

COVID-19 transforms the market

With businesses accelerating their digital transformation during the COVID-19 pandemic to ensure business survival and continuity, there has been a knock-on effect on cybersecurity strategies, which now must be prioritised and invested in. Over the past eighteen months, organisations have had to transition to working securely and efficiently from home, and then splitting their time between the office and remote work, in turn, creating new security challenges. This has demonstrated the crucial need for organisations to become more agile and have the ability to scale both up and down when regional rules change.

The importance of a secure and flexible workforce, one which is protected through layers of security and best practice, is key. This can be executed successfully by identifying existing weaknesses or gaps in infrastructure, which can be easily spotted by channel partners who specialise in cybersecurity. By leaning on an MSP, businesses can benefit from having access to the right support and advice, and MSPs, in turn, can offer the correct solutions to combat the challenges their clients face. This has led to organisations questioning issues such as; are the emergency measures put in place during the peak of the pandemic sufficient for long term secure and agile working practices? What tools do customers need to remain secure in the new modern hybrid working environment? It is clear that now is the time for businesses to reassess and build a flexible, future-proof plan.

The trusted advisor to SMBs

Smaller and medium-sized businesses often do not have the resources, time or dedicated teams to focus on their IT needs, while ensuring they have the right solutions in place to defend themselves



against cyberattacks. They also do not think they are as much of a target for hackers, as they may not have as much revenue or data compared to larger and more corporate organisations, with 66% believing a cyberattack would be unlikely. However, according to Accenture's Cost of Cybercrime Study, 43% of cyberattacks are aimed at small businesses, and only 14% are prepared to defend themselves.

Instead, by partnering with an MSP who can act as an external security partner for the SMB to help them achieve cyber resilience, the pressure and responsibility of defending the business against cyber threats will lay with the expert in the channel. This creates a unique opportunity for MSPs to guide customers on their cybersecurity journey and ensure they are receiving relevant education and have the right technology and tools in place to protect the business. It also helps the MSP to differentiate themselves from the ever-growing and competitive channel market, enabling them to become trusted IT security advisors for the businesses they support.

Critical support partner

Whether a business is big or small, investing in its cybersecurity foundations is not optional – it's business-critical, especially in today's threat landscape. By identifying the gaps in their cyber needs, or allowing an MSP to make these judgments, a strong infrastructure can be built upon the businesses existing setup. These solutions can be custom-built and tailored to each individual organisation, including email and endpoint protection, ongoing end-user training, as well as access services, such as ZTNA solutions.

With security breaches showing no signs of slowing down, MSPs must be constantly vigilant and develop cyber resilience approaches that go beyond deploying security solutions. This means having not only the market-leading technology available, but also the technical expertise to support business security plans and growth. MSPs must take a proactive role in understanding the current state of a customer's ability to protect against, prevent and respond to modern cyber threats when recommending the best approaches to true cyber resilience.

For example, MSPs who roll out Office365 to their client base are not tapping into their customers' needs for peace of mind when it comes to cybersecurity. Instead, they should add value to the partnership by emphasising good cyber security practices, providing the right tools and technologies and looking at specialist vendors – rather than providing a one-size-fits-all solution. Channel partners can both capitalise and draw on the importance of demonstrating to customers the benefits they bring by continuing their role as trusted advisors – resulting in growing their revenue while ensuring their key partner status.

Investing in Technology

An MSP's portfolio should provide the correct tools and solutions businesses need to survive and thrive in the new normal. Businesses of all sizes prioritised their move to digital workspaces during COVID-19, including remote teamwork, learning and critical cloud infrastructure, with Microsoft's Chief Executive saying that they've seen two years' worth of digital transformation in two months. Innovative technologies can form the backbone of a workforce's security foundations by adding layers of technology protection alongside employee tools and security awareness. Solutions can be embedded to prompt users to double-check their emails before a mistake is about to be made, for example, mitigating the risk of accidental data loss. Additionally, security awareness training within businesses has become a security necessity. Without peer review or IT supervision, organisations need their users to be empowered to make good security decisions. Rather than a once-a-year cyber awareness course – often used to tick a compliance box – today's businesses must invest in ongoing training, phishing simulations and solutions to help their employees make the right decisions – wherever they are working.

This is an important point for channel partners to take on board, as they have the power to ensure their customers' end users are sufficiently trained in the threat landscape. Have they engaged in phishing penetration testing? Is sending an email to the wrong person an embarrassing mistake or a data breach? These are just some of the key questions MSPs should be asking when they look to fulfil their trusted advisor role. This is an area where partners will see real growth as businesses have woken up to the idea that with the right solutions, they can switch their employees from IT risks to IT assets, and the channel needs to ensure they have the necessary training and tools in place to help their clients make these decisions.

Conclusion

Organisations cannot be expected to stay one step ahead of cybercriminals and adapt to new threats on their own. Within the evolving cybersecurity landscape, it's essential for businesses, especially SMBs, to find a partner that offers a varied portfolio of security offerings, as well as the knowledge and support, to keep their business data, workforces and networks secure.

By addressing pain points and providing assurance around the security of their working environments, channel partners can build and strengthen their existing relationship with their customers, while recognising the opportunity of additional revenue streams for their businesses. In turn, businesses can feel confident that they have the right technology, education and tools in place to combat the risk of cyberattacks and a trusted partnership they can rely on to keep them secure and agile.



How can you unravel complexity to launch a cybersecurity business?

The world of technology and cybersecurity is becoming more and more complex, which is why it is so important that partners simplify things for themselves and their customers.

BY ALEX RYALS, GLOBAL VP, SECURITY SOLUTIONS AT **TECH DATA**



AS SOMEONE who has a passion for flying planes, people often ask if I am ever nervous about taking to the skies in small aircraft and trusting I will stay there. I always say no. The reason, I explain, is because planes are actually very reliable pieces of machinery. Indeed, it is in fact human error that is normally to blame when things go wrong.

The same, I am afraid to say, can be said about cybersecurity. On the whole, cybersecurity technology is effective, and we certainly do not want for a lack of solutions to the different challenges

organisations face. Indeed, one of the biggest issues facing any partner is deciding which technologies you are going to use. They have to factor in their client's needs, decide on the controls that are required, and then consider local regulatory and compliance requirements, while also sifting through a mountain of vendors solutions and acronyms.

This picture is being further complicated by the shift many organisations have made to the cloud, particularly as organisations adopt a multi-cloud approach; some of whom without meaning to. Cloud

security requires that organisations think about the external and internal threats facing their business, and that they think about securing the connectivity between their cloud and on-premise infrastructure. A typical mistake that many organisations make is that they assume that the cloud provider will take care of the security for them. While providers of cloud infrastructure and services do secure their own infrastructure, it is up to those using or managing the service to secure everything from the operating system up. Different cloud providers have slightly different terms when it comes to the level of responsibility they take on and the expectations put on end users. As such, in multi-cloud environments, it is critical that partners understand the different responsibilities that come with each cloud provider and know how each must be configured alongside one another. Whether single- or multi-cloud, failure to understand the level of security provided and to properly configure security controls is one of the primary ways that threat actors gain entry into a cloud environment.

You have to start somewhere

The first step in assessing how secure your cloud environment is configured is to audit it. Having a clear picture of the various cloud environments an organisation has, the systems running on them, and the data stored within each is critical to assessing the risks facing that organisation. As part of this process, it is important to identify any shadow IT across the organisation. One of the most effective ways to do this is to analyse the records of your secure web gateway or Secure Access Service Edge (SASE) solution, depending on which is used.

Once you have a clear picture of the data and systems involved, you can then conduct a risk assessment that sets out which systems are the most critical to a business' operations and the quantitative impact upon that business should they be hacked. At this stage, an appropriate security environment can be designed and implemented, and penetration testers brought in three or four times a year to ensure issues within the environment are being resolved.

In a small or medium enterprise (SME), the list of actions above might look completely out of reach, but there are steps that can be taken to ensure that they are more secure. The choice of personnel is particularly important. Too often SMEs give IT people responsibility for security. Giving someone responsibility for implementation and security might seem to make sense, but that is usually not the case. Deploying technology and securing it are two very different skillsets, based on entirely opposite ways of thinking about technology; implementers follow the rules to make sure technology operates properly, whereas security people have to think about the many ways those rules might be broken and guard against that. Whether in-house or, more likely, from a managed service provider, it is

critical that SMEs ensure they have someone with a security mindset looking at their organisation's infrastructure. Another mistake that SMEs make is assuming that they are too insignificant for a hacker to target. There is this assumption that hackers are spending their time looking for specific targets, when in reality an automated programme is scouring the internet for weaknesses. With this in mind, and given that a cyberattack is much more likely to be catastrophic for a smaller business than a larger one, SMEs need to make sure that they have configured their cloud environments and taken steps to secure their most critical systems and data.

Identifying the right opportunity

Having read about the growth of the cyber sector and the opportunities for businesses in the market, many partners believe that they see an opportunity to engage and build a security practice.

While this is definitely true, partners need to make sure that they go about building their business in the right way. So often, we see partners hire a cybersecurity leader and start selling complex, high value security solutions that are completely analogous to their current offering. For example, if you typically sell servers and storage, then Identity Access Management is probably not the place to start because it is software focused, very complex and requires a specific type of services capability. Instead, maybe you want to start with selling endpoint security because it will protect the servers you are selling. Taking this approach of looking at your sales organisation and aligning with current expertise is a much more reliable way of building out a cybersecurity practice successfully.

Partners should also consider the other types of support that they can access. It is impractical, for example, for a partner to maintain the in-house resource to deliver all of the possible services that they sell. In these instances, working with distributors and solutions aggregators who can supplement their offerings will be key, allowing them to focus on the higher value offerings from which they derive better returns. Training and enablement are incredibly important as a partner builds out a cybersecurity offering, helping to provide its technical and sales staff with the knowledge they need to work alongside customers successfully.

Fly high

The world of technology and cybersecurity is becoming more and more complex, which is why it is so important that partners simplify things for themselves and their customers. Hybrid and multi-cloud bring with them new challenges around compliance and require a broader range of skills, but that should not put partners off. By focusing on their own strengths and using that as a solid foundation from which to build their cybersecurity specialism, there is a clear path to success for themselves and their customers.

Channel insights: Video exclusives

In addition to the articles in this issue of SDC Channel Insights, you can also watch and listen to a great selection of exclusive video interviews covering a range of technology and business issues which matter to the Channel.

Sustainability becoming a major channel focus

Michael O'Hara, Group Managing Director of DataSolutions, a distributor of transformational IT solutions, talks through the results of the company's Channel sustainability stock-take survey, revealing how companies are losing out on contracts if they can't demonstrate their environmental credentials, how the Channel is beginning to address its sustainability responsibilities and highlights the success of DataSolutions' Techies Go Green initiative.



[SDC Channel Insights \(sdc-channel.news\)](https://www.sdc-channel.news)



[Digitalisation World](https://www.digitalisationworld.com)

Step change required when it comes to IT sustainability?

Coeus Consulting, an independent IT advisory focused on delivering strategic change, recently published the findings of its report: 'The critical role of technology leaders in delivering on sustainability targets'. Graeme Trevayne, Associate Director at Coeus Consulting, talks through the survey results, highlighting the progress which has already been made, whilst suggesting that there is much more that can be done, not least when it comes to the need for some commonly agreed, IT sustainability objectives and the accompanying metrics.

Sustainability sums – understanding your IT investment

Ragnar Agnell, Partner at Centigo and Sanjiv Sachdev, Director, Strategic Business Value Consulting at Serviceware, discuss how – through the right technology – CTOs and CIOs can lead the charge against climate change in their companies whilst also balancing the urgent need to optimise business costs amid a turbulent financial climate.



[Digitalisation World](https://www.digitalisationworld.com)

A sustainable future for fibre - Prysmian

Prysmian Group's Executive Vice President of Telecoms, Philippe Vanhille, discusses the company's focus on the importance of sustainability as a key consideration in the design, production and installation of fibre cables, giving examples of what's been achieved to date and what we can expect over the coming years.



[Digitalisation World](#)



<https://digitalisationworld.com/videos/4276/sustainable-data-centre-expansion-programme-a-vantage-perspective>

Sustainable data centre expansion programme – a Vantage perspective

Antoine Boniface, President EMEA, Vantage Data Centers, outlines the company's ongoing expansion programme, which has seen it increase its presence in Africa, Asia and Europe in recent months, through a mixture of acquisitions and greenfield construction. With the company committed to achieving NetZero carbon emissions by 2030, Antoine has some valuable insights into how the data centre industry needs to move forward collectively to meet its sustainability objectives. (This interview took place at the end of 2021).

What matters most to MSPs?

Jason Beal, Senior Vice President, Global Channel and Partner Ecosystems, AvePoint, talks through the results of the company's first MSP Global Preference Survey, with security, governance and cloud migration ranking as top priorities. MSPs are also wanting to both consolidate the number of vendors with which they deal while also bringing on board new solutions. Jason also offers some valuable advice to MSPs in terms of some key business development objectives.



[Digitalisation World](#)



<https://sdc-channel.news/videos/4272/helping-the-channel-negotiate-the-bc-dr-maze>

Helping the Channel negotiate the BC/DR 'maze'

Richard May, Managing Director of virtualDCS, offers some great insights as to the challenges and opportunities for the Channel as it seeks to help its customers address their business continuity/disaster recovery needs. In a market where many continue to hold on to the 'comfort' of legacy applications, Richard believes that the virtualDCS CloudCover solutions portfolio, built around the company's longstanding partnership with Veeam, offers a great opportunity for Channel companies to make a real difference when it comes to providing optimised BC/DR.

DevOps for the digital age

Chris Wey, President of the Power Systems Business Unit, Rocket Software, talks through the tell-tale signs of a DevOps programme that isn't delivering, before outlining the key components of a truly 'modern' DevOps solution, with some major benefits for end users.



[Digitalisation World](#)



[Digitalisation World](#)

Merger delivers on unified data resiliency

The coming together of Arcserve and StorageCraft means an expanded solutions portfolio, offering both simplification and agility to Channel partners, designed to provide end users with a comprehensive approach to the backup and recovery challenges of the digital world. SDC Channel talks to Arcserve's Vice President Sales, EMEA, Richard Massey and Acting Chief Marketing Officer, Florian Malecki.

Better backup and recovery in a hybrid world

Mark Jow, EMEA Vice President - Sales Engineering, Commvault, talks through the success of the company's Metallic Software-as-a-Service Backup offering, a year on from the European launch, as well detailing the AWS availability of Commvault Backup & Recovery, and providing some great insight into a recent customer win at Syncreon.



[SDC Channel Insights \(sdc-channel.news\)](#)



[SDC Channel Insights \(sdc-channel.news\)](#)

Apple devices in the security spotlight

Addigy's Founder and CEO, Jason Dettbarn, explains how Apple devices are attracting increasing levels of security attacks, and what measures the company takes to counter these threats, as well as outlining how Addigy can help its customers to be confident and secure when using its Apple-based solutions.

The role of AI in tackling the threat of cybercrime

James Brodhurst, Principal Consultant at Resistant.ai, discusses the significant, increasing threat posed to consumers and businesses by ever more sophisticated and agile cyber-criminals. The good news is that there's a range of technology solutions available to mitigate the risks posed by cybercrime, Resistant.ai's identity forensics being one of them.



[Digitalisation World](#)



[Digitalisation World](#)

Shapeshifting Druid and cloud databases!

Imply has recently launched the Polaris cloud database service. Imply's Vice President of Product Marketing, David Wang, puts the launch in context as he details the company's Project Shapeshift work around Apache Druid, going on to explain how today's analytics opportunities require the very latest and best database solutions.

Ydentic platform offers 'simple' IT management

Jorn Wittendorp, Founder and CEO of Ydentic, explains how the company's platform helps MSPs and their customers to optimise the management of workplaces, accounts, access rights and passwords from one, central location. The company is expanding from its Netherlands base, looking to develop partners in Germany, the UK and the Nordics.



[Digitalisation World](#)

angel  tech

CS INTERNATIONAL CONFERENCE

PIC INTERNATIONAL CONFERENCE

SSI INTERNATIONAL CONFERENCE

Talk to us about sponsorship **NOW** as it will be another full house

Contact us at: info@angel-tech.net

Or call us on +44 (0)2476 718970 and speak to

Sukhi Bhadal or **Stephen Whitehurst**

SAVE THE DATE

28-29 JUNE

SHERATON BRUSSELS
AIRPORT HOTEL BELGIUM

Cybersecurity needs have outpaced the legacy MSSP model...throwing more tools at the problem won't fix it!

Better integration and unified visibility within an open security operation platform model is vital for the channel to adapt to the evolving threat landscape and dynamic customer demand

BY ASHOK SANKAR, VP OF PRODUCT AND SOLUTIONS MARKETING, [RELIAQUEST](#)



AS ORGANISATIONS looked for external assistance to manage their growing cybersecurity portfolio, Managed Security Services Providers (MSSPs) were the first generation to answer the call. The logic was simple. As businesses ranging from sole traders to huge multinationals consistently moved towards IT as a service for customer management, payroll, and productivity software – security as a service was a natural extension. Today, it is one of the fastest growing sectors of IT and MSSPs have done well with initial offerings such as managed firewalls, endpoints, and vulnerability management.

Unfortunately, the initial services that fit the bill for simple controls, are often failing to meet the needs of today's evolving business landscape. The rise of advanced persistent threats, supply chain issues and the dynamic nature of security operations is exposing weaknesses within the first generation of MSSPs.

Beyond tools

Effective cyber security is more than just managing different point products like firewalls, antivirus, or vulnerability scanners. In this evolving threat landscape, detection and response are critical. To accurately detect threats quickly and respond to them requires a

holistic approach, underpinned by singular visibility across the ecosystem that span on-premises, and cloud environments, to wherever digital assets of a modern enterprise reside. For an MSSP to truly offer a full spectrum cyber security service, it needs to gain visibility by ingesting telemetry from all security and business solutions, not just the popular ones, and aggregating threat data into a unified view for analysts to investigate and respond in a timely manner.

However, every end-user organisation has a heterogenous set of cyber security tools and technologies from different vendors across their environment. With over 500 security vendors in the market, an MSSP would find it almost impossible to manually integrate every cyber security tool into a multi-tenanted Security Operation Center (SoC).

MDR bandage

So, as a progressive MSSP, what's the solution? You could try and convince your customers to move to the dozen or so security vendors your SoC typically supports. A few might, but good luck with that as a long-term strategy! You could pull as much data from the systems you can integrate and simply ignore the ones you don't support – often called the 'head in the sand approach' which never ends well.

To overcome some of the limitations of a legacy MSSP model, many are turning to Managed Detection and Response (MDR) that promises a more holistic incident response approach. While they do offer a better option than doing nothing, they still fall short of helping achieve successful security outcomes given their black box and cookie-cutter nature. Additionally, this methodology does not scale and is



limited in the technologies they support. Customers want an MSSP to support them where they are – not be forced to change to meet the strictures of an MDR offering.

Open thinking

The answer to these conundrums requires the MSSP to focus on managing the growing volume of disparate security tools along with driving automation along the incident response processes. This approach is vital if MSSPs want to scale and overcome the Infosec talent shortage that is hampering their ability to deliver more effective cyber security. A recent ISMG survey that included an evaluation of cyber security buying trends of larger enterprises in Western Europe found that the main cause of complexity for 47% of enterprises is due to “too many tools that don’t integrate easily,” an issue that extends across all infrastructure with only 35% saying that they have detailed visibility across their on-premises and cloud environments. The survey indicated that although 87% said they expect increased or level funding for cybersecurity; when asked about strategy - only 11% stated that new tools were their number one priority. In fact, a higher number (12%) stated that a reduction in cyber security tools and/or vendors was a primary aim.

The survey sentiments suggest that customers are no longer prepared to just throw more cyber security tools at the problem. MSSPs must take note and start helping them to address the underlying issues of gaining more visibility and getting more effectiveness out of the tools they already have.

Integration is key

The data also shows that customers want the flexibility to only invest in security vendor products they see as fit for purpose. For cyber security as a service to be most effective, the service provider needs to overcome tool disparity and integrate them across the security stack to drive singular visibility. This means getting telemetry from any solution, on-premises or in one or more clouds together to deliver a single, complete view of threats. However, most integration platforms are monolithic stacks provided by a single vendor that tend to only integrate their own products.

Instead, a true security operations platform that is built from the ground-up with openness as one of the principal tenets is vital for solving this inherent problem. MSSPs need to deploy platforms with a vested interest in working with and integrating as many vendors into a unified stack as possible. Where a vendor specific solution might support just its own portfolio plus a handful of rival market leaders, an open platform will support tens of vendors. For example, ReliaQuest GreyMatter, supports over 70 vendors – and the number is growing continually as it has no commercial vested interests in steering customers into using a particular set of tools.



An open security operations platform means that managed security providers can finally overcome the issue of trying to get their customers to standardise on only the cyber security products that they support. Instead, customers retain what they have with true flexibility over future investments.

Longer term strategy

The overarching consideration for the channel is that customer’s value cyber security outcomes not what tools an MSSP can sell them! A business model that does not fundamentally do a better job at protecting them from attacks is short sighted and will ultimately fail.

Openness by itself is not a magic bullet that will fix all the cyber security challenges that security providers and enterprise customers face. However, for MSSPs to meet the growing threats, they need to better address the strategic direction of travel for their business. This means a fundamental shift towards ‘doing more by better integrating with what customers already have’ – rather than papering over the cracks of a fundamentally flawed premise by simply adding more standalone cyber security tools. One final stat to take away comes from a Ponemon Institute survey commissioned by IBM in 2020 that found the average enterprise deploys 45 cybersecurity-related tools on their network.

However, the study found that enterprises that deployed over 50 tools ranked themselves 8% lower in their ability to detect threats, and 7% lower in defensive capabilities, than other firms employing fewer toolsets. The message is clear, for MSSPs to deliver the level of services that enterprises expect, they must move past legacy tool monitoring and management. Getting better at using what you already have through an open and integrated approach will be the difference between the MSSPs that succeed and those that fail.

Why it's time for managed service partners to start working for customers, not just with them

As businesses have been forced to embrace remote and now increasingly hybrid working approaches, more have begun to realise the benefits these can offer when it comes to enabling more decentralised workforces, which can help to overcome internal skills gaps. As such, there is an increasing demand from organisations for more distributed, on-demand and specialised talent.

BY MAHESH DESAI, CHIEF RELATIONSHIP OFFICER, **RACKSPACE TECHNOLOGY**



THIS IS ESPECIALLY TRUE in light of the fact that more businesses are embracing a cloud native approach, meaning their teams are increasingly transforming towards DevOps-focused operating models. With DevOps approaches, the boundaries between infrastructure and applications, and “build” and “operate”, have become a little blurry. At the same time, large monolithic outsourcing contracts are unable to provide the flexibility required for modern cloud adoption, leading to stagnation and inefficient use of cloud technologies.

In response to these trends, organisations are coming to realise they need more customised engineering and operations capabilities from their partners.

When vacancies outweigh talent

Not only is technology itself becoming more sophisticated, but businesses have quickly evolved in their digital transformation journeys over

the past year – particularly when it comes to cloud. In fact, there is now an abundance of research to show that digital transformation journeys that would previously have been expected to take a number of years have been completed in a matter of months.

But many of these technologies were implemented in urgency and under pressurised conditions, when businesses had little time to think of anything other than how they'd keep the company afloat remotely. So, as organisations' use of these emerging

technologies becomes more complex, and more specialised knowledge is required to help implement and run them, it is becoming increasingly difficult for internal IT teams to keep up.

On top of this, many businesses were forced to scale back resources as a result of the pandemic.

Thanks to renewed optimism around the



immediate future and with a clearer roadmap to normality set out by the UK government, most are now beginning to scale back up and are setting out on huge hiring sprees. But this has left UK vacancies at an all-time high, and experts suggest businesses could be facing skills shortages for many years to come.

As such, UK organisations have been left with smaller teams than they are used to across the entire company, including IT. While these smaller, internal IT teams possess a broad knowledge of the technology space, they do often lack the specialist expertise that is required to enable a cloud native approach. Although it is harder than ever to find the talent required to fulfil these business needs – especially at short notice – businesses can simply not afford to wait.

Leaning on third parties for support isn't enough. Having the opportunity to be flexible and agile is the way forward in terms of how we all work is going to evolve, and businesses are already learning to embrace their new-found flexibility by implementing variations of the hybrid working approach. But being flexible involves more than just implementing new policies and perks for in-house staff, it's also about embracing the notion of building out internal teams with third party support.

Businesses need to learn and realise that customers gain the most from cloud technologies when workloads, teams, and processes are transformed to a more cloud native and agile operating model. And working with a third party to reach cloud nativity is going to be vital for businesses going forward.

However, simply working with a third party alone isn't necessarily enough any longer because traditional managed services can struggle to deliver on customer goals in these environments. This is largely due to an inherent lack of flexibility within agreed scopes of work and contract structures. That's why it's time for managed service providers to start working for their customers – not just with them. This means offering flexible, on-demand and dedicated support as and when their customers need it throughout their cloud journeys.



The future of work is on-demand and flexible. These dedicated customer teams that managed service providers should be creating will become entirely familiar with their partners' and customers' businesses so that they are able to simply work as an extension of the internal team, instead of an external third party with a lack of detailed knowledge about the project.

In doing so, they will be able to help deliver transformative, best-practice-led engineering and operations services. Meanwhile, businesses don't have to worry about lengthy and expensive recruitment drives for specialist skills that can ultimately put their cloud journeys on hold. So, while hybrid working is a great place to start, post-pandemic flexibility is about so much more than that. It's about a total mindset shift and casting the net for talent much wider than existing and prospective internal talent. The war for talent is bigger than ever, and it's time for businesses to start embracing external, third-party support. In doing so, MSPs also have a big transformation on their hands to become partners that can act as a true extension of their customers' business and their internal teams.

Businesses need to learn and realise that customers gain the most from cloud technologies when workloads, teams, and processes are transformed to a more cloud native and agile operating model. And working with a third party to reach cloud nativity is going to be vital for businesses going forward

How to build the customer-centric model your channel partners really want



Shifting towards a fully customer-centric business can be more challenging than initially believed.

BY RICHARD EGLON, CHIEF MARKETING OFFICER AT **AGILITAS**



COMPANIES are constantly on the lookout for ways to successfully adopt a customer-centric business model. Having been faced with many obstacles and barriers in recent years, it has been much more challenging to firstly identify solutions and secondly, implement them quickly and effectively.

For example, in our digital society, businesses are flooded with a high volume of customer data and some companies do not have the correct systems in place to effectively process and analyse information. Ultimately, there is a shortage of technological capabilities that allow businesses to intelligently evaluate customer data to deliver a far richer customer experience.

This is not the only concern, as company culture also plays a vital role in customer-centricity. Many organisations can remain product-focused and prioritise sales over its people. However, to successfully implement a customer-oriented model, Channel businesses must start within and have a culture that aligns with its customers' expectations. Leaders and decision-makers need to become role

models and demonstrate to the wider team the company values and morals it wants to be known for - therefore delivering to customers the experience they expect.

Customer orientation can provide a solid foundation for a customer-centric business which, when championed and embraced by employees, can drive success. This culture will also result in more positive customer outcomes and will keep employees motivated, reinforcing effective relationships with partners.

Putting your channel partners first

Customer-centricity is all about prioritising the customer. Having this model at the heart of any business will allow the end-user to have a positive experience from the very beginning of the purchasing journey and will enable them to build a long-term relationship with the company. With the advancements in technology, a business can measure its success with its customers. This is extremely valuable data because it is possible to have a wider understanding of customer needs,

interests and how they engage with an organisation. By identifying these key trends, businesses can offer its channel partners customisable services and promote them to other potential customers.

Customer retention and lifetime loyalty are where a company will exceed in profits and values. Subsequently, if a customer doesn't receive the correct experiences, competitors can end up being the first choice. Therefore, organisations must focus on delivering a positive customer experience - even when issues can occur. This may result in adjustments to services and offerings, but once in place will see a massive shift in customer activity. In order to successfully do this, businesses will need to rethink structure and culture.

Globally, businesses have seen a change in past and present relationships and how they interact with its customers. The pandemic has encouraged customers to return to the businesses that have made changes within the organisation and who have altered services to fit its current demand. Also, being digitally available has been vital during a time of limited face-to-face collaboration. In fact, this has changed the way customers interact with brands, which is a huge part of the customer journey. An important consideration is that customer-centricity has evolved to become all about the customer demand and how they want to interact with the business, rather than a business's products and offerings.

Achieving customer-centricity

Following a customer-centric approach will allow businesses to anticipate what channel partner customers want. Creating not only services and offerings that suit the current needs, but ones that are designed to help its partners as well. This will be key to growing an organisation.

In today's workplace, employees are shaping cultures, rather than employees. This will determine the overall customer experience, so aligning customer-centric thinking employees to front-facing roles will be very important and impact the level of customer service for a business. The adage that 'people buy from people' has never been more

crucial and it is essential that employees treat partners as customers, rather than sales numbers. Developing a relationship with each and every customer will bring significant benefits to a business and will establish a strong foundation for more successful leads.

To encourage and connect a culture that achieves positive partnerships, decision-makers should motivate a customer-centric strategy by implementing benefits and supporting its employees. After all, a business that is struggling to become customer-centric can become a negative working environment, especially in the sales and marketing teams. Alignment between culture and customer needs is crucial for synchronicity and must be addressed as a priority.

Shifting towards a fully customer-centric business can be more challenging than initially believed. However, looking to make the smallest changes and implementing the correct policies can create significant benefits for both employees and customers. Becoming a customer-centric business will be the key to unlocking employees' true potential and creating customer loyalty. If employees are empowered to be empathetic to partners' needs, customer satisfaction and business growth will soon follow.



Designing data centres for MSPs and IT service providers

Since the start of the pandemic, the Managed Service Provider (MSP) and IT Service Provider marketplace have radically changed. As the post-pandemic business landscape begins to take shape, it's critical for MSPs and ISPs to choose the right data centre partner to support growth.

BY AMY YOUNG, SALES DIRECTOR AT **CUSTODIAN DATA CENTRES**



AS MANY BUSINESSES begin to re-draw their digital transformation roadmaps in the wake of Covid-19, today's end-users are looking to evolve how they structure their IT services, and more critically, streamline whom they buy these services from. For the MSPs and ISPs responsible for such digital strategies, agile, resilient and secure data centre capacity is crucial – especially for those delivering disaster recovery, business continuity and cloud services. Here, the role of the data centre operator is, in many respects, simple but critical.

Their primary requirement is to deliver power, cooling, connectivity, and secure physical infrastructure to support MSP service delivery.

Challenges in the face of digital transformation

In recent years much has changed. MSPs and ISPs are faced with a host of challenges, including the need to keep pace with the speed of constant technological change. There's also a highly competitive marketplace to contend with, where often vendors and other service providers, even those that a business is partnered with, can compete on the same tenders.

Other challenges include the need for greater resilience of the IT facet and thereby increased levels of due diligence, where customers will want to see their whitespace before signing contractual agreements. Finally, with accelerated digital transformation, there is a need to future proof while meeting strict SLAs regarding data, security, and uptime. The role of the data centre operator has, therefore, become even more critical for MSPs and ISPs planning to scale and grow.

And with more end-users now looking to their external suppliers as trusted advisors, in-house technical expertise, agile critical infrastructure and dynamic service have become key differentiators for those providers in the channel.

Digital architectures are changing According to research from Accenture, over three-quarters (77%) of executives state that their technology architecture is becoming critical to the overall success of their organisation.



One key area of growth for all MSPs is digital security, and research from Datto into the impact COVID-19 found 84% of MSPs report advanced endpoint security, data loss protection (79%) and password management policies (72%) as the most requested services by their customers. Having a partner that specialises in state-of-the-art physical infrastructure and security is vital for MSPs, and will likely form a major component of their services, especially those around zero trust approaches to data security.

Research from Gartner also states that by 2025, 85% of infrastructure strategies will integrate on-premises, colocation, cloud and edge delivery options, compared with 20% in 2020. This dramatic shift in IT infrastructure is redefining how MSPs are delivering end-user services.

Mission-critical IT, whether deployed on-premises, hosted in a colo, or indeed at the edge of the network is, therefore, paramount for end-user digital transformation. Now, as more MSPs and IT Service Providers are called upon to expand their service portfolios with capacity for AI, machine learning and edge infrastructure, all of which require integration with cloud services, the support of specialist colocation providers have become vital. But what are the considerations for choosing a colo?

Key considerations for outsourcing

As with any service provider, cost is a key aspect of the decision-making process. MSPs cannot, however, put a price on reputation, so reliability, connectivity, security, and efficiency all play important factors. Efficiency, especially in the form of power usage, can be critical, and the more energy efficient a data centre provider can be, the lower the total cost of ownership (TCO) for the user.

A data centre provider with a lower PUE can provide a cost-effective and scalable platform to support MSP growth, something highly appealing where cost and consolidation are influential.

Diverse connectivity and low latency are also determining factors, and MSPs will often seek out carrier-neutral colocation providers who have access to dark fibre rings, 100Gb wavelengths, and who can deliver enterprise-level connectivity solutions. Many end-users are moving towards hybrid IT environments with a mix of on-premise infrastructure and cloud, so real-time access to data and application availability are indeed business-critical.

Size, in terms of scalability, alongside physical security and customer experience, are also crucial. Many MSPs are looking to partner with operators that have a demonstrable track record in supporting their key customer demographics.

Further, with human error, network, and power failures key causes of outages there is also a need to meet strict compliance and regulatory standards,

and to provide policies for zero downtime. For any service provider, it pays to have a data centre partner who can consistently meet strict SLAs.

Finally, speed of deployment and dynamic service is crucial. Any Managed Service or IT Service Provider will tell you that adding value, or the having ability to go the extra mile, can be the very difference between a customer renewing their service agreement or migrating to another provider. The trust that a data centre operator can act as an extension of your team, can understand complex infrastructure deployments, or who can meet strict timescales, especially where speed of installation, security and operational reliability are concerned.

The need for new partnerships

As the business landscape continues to change, so have the ways in which data centres are looking to support the MSP and ISP communities. Cost predictability is always a key factor, but so too are the pressing needs to consider technical competence, alongside environmental factors - especially as sustainability moves to the top of the business agenda.

In the wake of Covid-19, MSPs are looking to their data centre providers as trusted advisors, and often, as an extension of their technical or sales teams. The right operator can help an MSP win business, answer complex technical questions, and instil confidence in the end-user at every stage of the journey.

Further, transactional relationships have become a thing of the past, and long-term collaboration has become a focal point of business discussions. As such, many MSPs are looking for providers that can support their growth across different geographical regions and can continue to do so in a low cost and environmentally sustainable way.

Finally, trust and transparency are vital, especially in a channel where tenders are often taken in-house, and where partners can find out that they are competing on the same bids. In essence, by partnering with a data centre operator that focuses solely on colocation, and without its own services division, MSPs can avoid many of the complications associated with challenging tender processes, while developing mutually beneficial relationships that are designed to support long-term growth.

At Custodian we're dedicated to setting a new standard in dynamic, multi-site colocation services. Our agile-mission-critical data centres have been expertly designed to underpin MSP and IT Service provider growth - combining expert technical insight with unparalleled customer service and a reputation for industry-leading uptime. We believe that in the era of digital transformation, MSPs deserve a new kind of partner that can help them diversify and grow, and we are committed to making that vision a reality.

Why professional services are key to accelerating IoT adoption

Throughout history we have seen plenty of examples of companies that have failed to adapt when there was a sea change in the prevailing business model. Consider the companies that fell by the wayside when the software industry switched from a per-license pricing model to SaaS. Now in the rapidly evolving digital world, we're on the verge of a similar sea change within IoT with companies increasingly looking at taking the plunge into IoT implementation.

BY BRIAN CASTO, SVP OF GLOBAL PROFESSIONAL SERVICES AT **ESEYE**



IN FACT, BY 2025, over 271 billion IoT devices are expected to be deployed globally. This accelerated growth also aligns with the findings from our State of IoT Adoption research, undertaken in April 2021, in which 500 decision makers in the UK and US revealed their commitment to ramping up IoT investment, with 49% planning new projects in the next two to three years and 89% planning budget increases.

However, many companies lack the resources and skills needed to architect, integrate and maintain a connected solution in their enterprise environment.

And, without an experienced technical team, project costs can quickly escalate into unanticipated risks which may ultimately threaten the overall success of the project.

IoT projects fail to reach their full potential

As mentioned above, many organisations lack the specialist skills internally to develop and deploy IoT-based solutions. Often companies don't have the in-house expertise or the resources to manage multiple vendor relationships for various components of an IoT solution. Without a doubt there is a lot of complexity associated with IoT devices, such as connectivity issues – an IoT solution should provide reliable and secure connectivity that overcomes any international or local restrictions. It should be robust and well-designed and in today's world of escalating threats security considerations need to be factored in from the outset.

There are also logistical challenges - particularly for global or multi-region roll-outs, and the ongoing management and co-ordination of multiple vendors, and many other challenges for companies to deal with. Our research showed that respondents were struggling with security, connectivity, and device onboarding, all of which were cited as top challenges; 39% said security was their biggest hurdle, while for 35% device onboarding, testing and certification, and cellular connectivity across multiple countries and regions had also proved difficult. As a result, 77% of respondents said that IoT projects



embarked upon in the last 12 months had failed to reach their full potential.

To tackle this vast unknown world of IoT, many organisations have turned to global system integrators to bring physical assets onto the Internet and build the network infrastructure required to manage devices and data. However, the diversity of use cases and nature of extreme use cases means that a one-size fits all approach cannot be adopted and rolled out. Often enterprises realise they need a specialist provider rather than a generalist. Frequently, companies find that they need to develop a unique solution for projects and often they must build this from the ground up. For example, Cisco estimates that 75% of IoT projects fail, often at the proof-of-concept stage, and that is because most IoT devices are hand-built for the use case.

Why companies need ubiquitous connectivity

Additionally, many service providers, SIs and mobile operators talk about their ability to provide global coverage, but often this isn't equivalent to ubiquitous connectivity. Roaming agreements might be in place to help devices connect to compatible networks when travelling across borders. Nevertheless, they don't guarantee that the connectivity is accessible or consistently reliable everywhere, which again can cause challenges for the company.

Then there are compliance considerations across markets and different mobile network operators. Companies often turn to IoT to capture previously untapped data that can transform their operations and give them a competitive edge. But due to the business-critical nature of these data streams, any security breach means that the organisation could incur severe financial and reputational damages. On top of this, compliance with rigorous data protection frameworks is often a critical business requirement. As such, many organisations will favour an on-premises or hybrid IoT deployment over a cloud-driven one to retain complete data and security control and mitigate risk. And if they are looking at cloud integration or cloud migration, they will be seeking an ultra-simplified but highly secure way to integrate their data into the cloud.

When it comes to mission-critical infrastructures and IoT devices, companies naturally strive for near-100% network uptime, even in times of crisis, and any IoT solution should provide reliable and secure connectivity that overcomes any availability issues throughout the device's lifecycle in the field.

Helping enterprises meet the IoT challenge

Taking these challenges into consideration, what enterprise customers really need is an advisory service when embarking on an IoT initiative to ensure their initiative reaches the goals of the

business. Here at Eseye, we have rethought how we can provide a managed-services approach to organisations, offering customers a blend of consulting services, hardware design and connectivity to help guide them on their IoT journey.

Today we work with thousands of customers from every industry vertical, working side-by-side every step of the way from initial concept through to providing IoT device design, cellular connectivity, hardware, technical consultancy, and round-the-clock support. Additionally, our team of solution architects and technical solution consultants ensures that any IoT initiative has the necessary rigour in place and is delivered to market on time and on budget, helping customers to realise their desired business outcomes from the project.

Right from the outset, our IoT advisory services help organisations future proof their project, by ensuring product and strategy will deliver long term success. We offer specialist device design and prototyping to accelerate project progress from concept to deployment. As our research shows, device onboarding is always problematic, and we provide robust testing techniques to ensure the device is fit for purpose.

When it comes to mission-critical infrastructures and IoT devices, companies naturally strive for near-100% network uptime, even in times of crisis

We also provide specialist consultancy to ensure the devices meet any required certification, and our deployment services mean that the end-to-end experience, from pilot to commercial deployment, is a success. Without an experienced team IoT project costs can quickly escalate and our round-the-clock technical support team ensures maximum uptime for every global deployment.

Growth of IoT is set to accelerate

With the anticipated growth of IoT over the coming years, companies need to be confident that their IoT initiative is not going to fail, as so many have done in the past. Without a doubt the IoT ecosystem is complex, and enterprises are finding it much harder to achieve success with their IoT ventures than anticipated. Our dedicated professional services team leads customers through a proven methodology to define their appropriate IoT strategy that supports the development of a solution that meet the goals of the business, enabling organisations to deliver enterprise-scale global IoT solutions that work, every time, everywhere.



How to unlock up to 50% profit margins with ‘bundles’

Why the channel (in particular MSPs) needs to consider offering their clients bundled solutions instead of ‘single-solution sells’ to profit.

BY ROB HANCOCK, HEAD OF PLATFORM AT [GIACOM](#)

OVER THE LAST 20 months, many SMBs and MSPs have had a tough time, no thanks to the pandemic. Throughout this period, many SMBs have done their upmost best to survive against backbreaking market conditions. But, equally, some MSPs have faced similar growth concerns and challenges, as they’ve strived to support their customers.

One issue that some MSPs may face, is being limited by their lack of solution offerings. Without being able to cater for a wider range of customers and expanding on their expertise, these MSPs will struggle to increase their profitability over time.

If we take into consideration that 34 percent of MSPs are kept up at night by concerns over competition, 27 percent are worried about revenue

growth, and 23 percent are having sleepless nights over acquiring new customers; this shows the channel has a lot to think about when comes to growing their businesses.

The market demands complete solutions

Today, when SMBs purchase technology from the channel, they tend to start by pointing out they only want an email inbox. But in fact, at that point of sale, there is more opportunity available to MSPs to consult and offer comprehensive solutions.

This is because, nowadays, when SMBs develop their technology stacks, they actually need to buy their technology solutions according to the wider demands of the business.

For example, while they might think that an email inbox is all that they need, their requirements are actually greater than this. When buying technology, SMBs don't fully appreciate this. And, in light of the pandemic, what many SMBs actually require is the capability to adopt new digital ways of working and / or hybrid working – not just in the short term, but long-term too. Further, in a recent YouGov poll 70% of people predict that workers would «never return to offices at the same rate» post-pandemic. This makes an ongoing case for digital / hybrid working technology.

In these situations, while a single-solution sell to pre-pandemic customers might have made sense, supporting the new need for the SMBs' more complex requirements demands a different kind of proposition and sell. It requires that the MSP market considers providing customers with forms of bundled technology options to offer to their customers, or that they assess how to evolve their existing bundles for more modern ones.

Another factor to consider is the contingent of SMBs that panic bought technology through the pandemic, without realising that their organisations actually need more sophisticated bundled technology solutions (e.g. greater digital transformation/hybrid working). In these cases, MSPs have the opportunity to upgrade their offering to customers and provide bundled solutions instead.

Bundling can unlock up to 50% profit margins. These days, hybrid working bundles are vital. They typically include cloud connectivity, productivity solutions, email security and backup. Anecdotally, the evidence for offering bundled solutions is strong too: for instance, Giacom found that customers can unlock 50 percent profit margins by offering a unique software bundle. They're not alone either, up to 70% of MSPs are offering 'service' bundles of various solutions to customers too (Kaseya's Global Pricing Survey).

What's more, thanks to how the cloud has propelled technology forward, it means that SMBs can benefit from enterprise-grade solution-sells in bundle form from MSPs too. In the past, these sort of broader solution sales were thought to be the preserve of the enterprise market. Cloud democratised this and made it possible for CSPs, with strong technology partnerships and roadmaps, to enable MSPs to offer SMB clients powerful technology options (though bundles).

Moreover, since cloud is entirely scalable, bundled propositions can enable MSPs to work with clients to develop their own bespoke technology roadmap, perhaps phasing in different kinds of technology in stages where it makes sense, based on the best of breed technology available to them from their CSPs. With the right supplier relationship in place, CSPs and MSPs can partner effectively and

provide flexible service level agreements that work in everyone's favour. This reduces financial risk, especially for the end customers.

Tied in with the effectiveness of offering bundled solutions to customers is 'marketing'. As MSPs consider bundled solutions, they should work closely with their CSPs on the right kind of marketing that is required to sell these solutions too. Bundles can enable MSPs to differentiate themselves in the market, so it will be important to communicate the benefits of these solutions to the market effectively. Which is why MSPs should evaluate how their partner CSPs can support with messaging and positioning to end customers.

Aside from market differentiation, packaging more than one software product together from suppliers to offer to the market, can enable MSPs to save money and offer greater price flexibility. This approach could also enhance operational efficiencies and help prevent customers from talking to competitor MSPs or tech suppliers

Conclusion

Aside from market differentiation, packaging more than one software product together from suppliers to offer to the market, can enable MSPs to save money and offer greater price flexibility. This approach could also enhance operational efficiencies (e.g. savings on overhead cost), and help prevent customers from talking to competitor MSPs or tech suppliers.

In addition to this, stringing together compatible cloud solutions in bundles enables MSPs' to deploy more capable and effective hybrid ways of working for end customers. Customers will benefit from cloud's accessibility and availability, the collaboration options it offers, as well as flexibility, security and the fact it's always up-to-date.

Finally, with the current shift towards solution-based selling, led by bundled propositions, the time is now for MSPs to align with proven CSPs – who can support them on their journey towards bundling not only solutions and sales, but also the profitability into their business.



An edge computing platform has become vital for solution-builders and service-providers

Partnering with a purpose-built edge platform is becoming essential so service providers and application-builders fully exploit the immense potential of the edge model.

BY SIMON MICHIE, CTO, **PULSANT**



THE RELOCATION of computing power much closer to end-users is one of the most far-reaching changes in the use and consumption of data. This departure from the standard public cloud model eliminates the latency constraints of distance from the main hubs, enabling a vast range of new SaaS applications, use cases and business opportunities that were previously unfeasible. The business opportunity created by this redistribution of computing power to the regions is immense. Statista estimates the worldwide edge market will grow to \$250.6bn as soon as 2024.

This rapid market expansion will be driven by the combination of edge platforms, 5G technology, fibre-to-the-premises, and artificial intelligence (AI). Together they deliver advanced, high-speed, high-capacity services to organisations and end-users regardless of location.

Suppliers of online services and companies building new applications and subscription models will have access to many more customers and a platform for higher levels of performance and innovation.

Everybody gets to access latency computing. The edge is transformative for service and solution-providers because it brings low latency connectivity to businesses and consumers even if they are hundreds of miles from the metropolitan data centres of the major cloud companies. Businesses across the UK can deploy applications that consume masses of data, reducing their need to transfer heavy volumes to the public cloud. One of the benefits of this new model is reduced backhaul costs to the public cloud.

Whereas it was previously impossible to sustain high-speed data transfers necessary for AI, edge enables applications to run analytics locally once models have been trained on masses of data in the public cloud. These advanced capabilities open the door to industrial IoT applications that reshape manufacturing and logistics operations or to advanced automation that transforms the efficiency of extraction and refining processes, even in isolated sites. This is how, for example, oil and gas businesses or pharmaceutical manufacturers can implement industrial digital twin technologies that enable innovation in highly complex processes. In healthcare, edge computing will enable sophisticated remote diagnostics, 3D-imaging, and monitoring.

In the consumer sector, edge will vastly expand the range of products and services businesses can provide to new and existing customers. In gaming, for example, multi-player contests will be possible in any location, as will streaming services, augmented reality-enhanced shopping or learning experiences, and real-time smart home applications.

Choosing the right edge

However, the success of this major shift in computing capability depends on any edge platform having certain vital attributes. These include a broad, functioning ecosystem that encompasses the telecommunications service providers, along with the public cloud providers and specialists in microservices, containerisation and virtualisation and related fields.

Any edge platform must be scalable and have a network of data centres that provides genuinely national coverage to ensure every end-user, regardless of location has low latency, high-bandwidth connections to all their workloads. This should be the case, whether workloads are in the edge centre, public or private cloud.

Edge data centres should be perfectly positioned

Edge data centres need to sit between the on-ramp to the public cloud and network-to-network telecoms interfaces, positioning them perfectly to enable cloud service providers to expand coverage. This is already available. The better-prepared edge providers are also aware that customers want

flexibility and control and have therefore equipped themselves to facilitate hybrid and multi-cloud models, giving enterprise customers access to the cost, performance and security advantages of different providers and environments.

For all businesses using edge computing, it is critical they avoid congestion as network traffic increases. Market intelligence company IDC expects the number of installed IoT-connected devices to hit 40 billion by 2025, for example, and the number of daily data interactions per person to rise from 601 in 2020 to almost 5,000.

For all businesses using edge computing, it is critical they avoid congestion as network traffic increases

Any edge computing platform must be scalable and have a high-speed network to ensure the sub-five-second latency necessary for many applications such as IoT or gaming. The need to select best-of-breed partners to ensure maximal performance and avoid reliance on a single vendor should focus the minds of service providers when they consider how to adopt edge and adapt it to their own requirements. A nationwide edge computing platform deploying a high-speed fibre network with route diversity and resilient connections to the full range of public cloud vendors is a necessity.

It is also vital to partner with established edge platforms that have ubiquitous coverage and high-speed fibre connections between centres. The more advanced edge platforms spread the load across several regional data centres, not only processing data closer to each end-user but also reducing the backhaul congestion that damages performance. Once they have access to a fully-edge-ready national platform, application-builders can deliver their solutions far more easily, using edge orchestration platforms to support workloads.

The range of new capabilities at their fingertips will open up almost limitless markets. In other words, partnering with a purpose-built edge platform is becoming essential so service providers and application-builders fully exploit the immense potential of the edge model.

What is a cloud centre of excellence and how can it help channel partners?



A CCoE is built to support partners, amplifying cloud expertise to ensure they can design and migrate their clients to the cloud supported with confidence and without many of the pitfalls that have plagued the industry in recent years.

BY TIAGO FERNANDES, DIRECTOR CLOUD CENTRE OF EXCELLENCE,
EUROPE AT **TECH DATA**



THE CLOUD is one of today's most demanded forms of technology, rapidly evolving with new services and updates every other week. According to IDC's latest cloud forecast, "whole cloud" spending will surpass \$1.3 trillion by 2025. In a similar vein, Canals recently reported that spending on cloud services in the third quarter of 2021 increased 35% to \$49.4 billion. This trend is a testament to the recognised advantages business leaders see in the cloud.

As well as being in high demand, the cloud might also be one of the more misunderstood

technologies on the market. Initially, businesses had utopic visions of simplified IT environments with reduced running costs, but many have not found that to be the case. That is not to say that it cannot, and indeed ought not, be the case. However, it is not as simple as was once made out due to the hundreds of clouds services available and their constant evolution.

As cloud adoption grows, particularly in terms of multi-cloud environments, more organisations are grappling with the complexity that needs to be overcome before the benefits can be truly realised.

Organisations are turning to the channel to help them manage this complexity, and so this issue of keeping up with all the latest developments is being outsourced to partners. As such, it is becoming their problem. To help overcome this challenge, cloud centres of excellence (CCoE) exist to help support partners and spread cloud expertise through the market. This means that partners draw on the expertise they need, when they need it, as they work with their customers to reduce their IT complexity and costs whilst making their business more scalable.

A constantly changing picture

Public cloud vendors are constantly bringing new innovations to their solutions. It has been known that each of these cloud vendors have more than 300 cloud services (from IaaS, PaaS and SaaS) and these services get updated constantly with new feature developments to be launched in a matter of a couple of weeks. This means that channel partners are persistently supporting their customers in assessing which features are most useful to them, how they can optimise them, and what changes they need to make to their cloud environments to do so. Compounding this, the move to cloud means that people's skills are no longer aligned to managing networking, compute, or storage in vendor silos. Cloud environments require a broader knowledge base, and this is difficult for partners to attain in the face of a skills shortage. With a CCoE, highly knowledgeable cloud architects can be called upon to augment a partner's team, supporting them across a range of topics from leading IaaS platforms to application specific workloads. This ensures that partners know that they can always access the knowledge they need to meet a customer's requirements.

Increase in flexibility

Partners can also work with a CCoE to triage undesirable cloud outcomes as and when they happen, ultimately covering their skills gap while delivering projects to their end customers. For instance, by using dashboards and monitoring businesses can facilitate communication and manage the cloud environment. Without proper configurations, security gaps might put an organisation's data at risk. Businesses can now mitigate these risks through an experienced team of experts.

Speed matters

For large organisations looking to adopt cloud solutions, a CCoE can help achieve the velocity required for a smooth transition to cloud as opposed to trial-and-error efforts. As businesses accelerate innovation and migration efforts, the CCoE will work with partners to properly design, deploy and configure new and existing multi-cloud environments to ensure minimal costs and increased business agility. Without the right expertise, it is very easy for these multi-cloud environments to

become highly complex and, by extension, costly, as many organisations have found to their cost in recent years. The CCoE can provide the guidance to help teams complete these large and complicated projects faster and more effectively.

How can this work in practice?

As more systems are being integrated, it is vital businesses are armed to cope with this level of complexity otherwise they will face performance and security issues. This is placing significant demand on the channel as they work to meet the unique needs of their clients. However, having all the skills to meet this need is not a given, whilst gaining the broad range of skills necessary can be a difficult transition for those partners who have developed a deep specialism in specific technologies and vendors. Our goal is to research and architect cloud solutions that empower partners to achieve great outcomes with technology.

If you are a partner and your customer wants to migrate to the cloud, there are many requirements and business outcomes to consider and a long journey to take. Does the customer want an IaaS or PaaS platform? A high availability? Who will understand your current infrastructure and design the new future environment? Do you need POC to get familiar with technology and prove its value for your business? Who will migrate the workloads? In helping to match the unique requirements and characteristics necessary for their customer, partners can work alongside a centre of excellence to address these queries and deliver the full end-to-end solution, enabling the partner to secure the deal.

Ultimately, the pandemic has accelerated the supply side demand for cloud service. This is a major market opportunity, but also a challenge as this puts pressure on partners to meet unique needs of each of their clients. A CCoE is built to support partners, amplifying cloud expertise to ensure they can design and migrate their clients to the cloud supported with confidence and without many of the pitfalls that have plagued the industry in recent years.



SDC CHANNEL SUMMIT

THE 2ND SDC CHANNEL SUMMIT REGISTER FREE TODAY

We are delighted to introduce our second virtual conference. Based on extensive research conducted with attendees at the first event, as well as survey feedback from our Channel data base (based on attendees to the previous SDC Channel Events), we're confident that we've produced an essential education opportunity for the Channel as it seeks to address both the challenges and opportunities of digital change management:



**Channel
Summit
10-11 May**

Over the course of two, consecutive morning sessions (giving attendees plenty of time to run their business as well), we will be providing invaluable insights, advice and recommended actions to help Channel organisations as both they, and their customers, get to grips with what it means to create, develop and optimise a truly digital business.

Topics include:

- 1. SKILLS + TRAINING**
- 2. SUSTAINABLE BUSINESS DEVELOPMENT**
- 3. SIMPLIFYING THE SOLUTION STACK**
- 4. SELECTING THE RIGHT SECURITY PARTNERS**

Register for free here: <https://sdc-channel.com>

Sponsored by:



PARK PLACE
TECHNOLOGIES

In association with:

