DIGITALISATION WORLD

MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE IV 2023

DIGITALISATIONWORLD.COM

Why aren't businesses baselining their security?

By prism infosec

AIOps | Apps + DevOps | Artificial Intelligence | Big Data + Analytics | Cloud + MS
DC Facilities + Colo Digital Business | IT Management + Service | Networks + Telecoms
Open Source | Security + Compliance | Storage + Servers

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

APC

Just say where you want it...

We'll take care of the rest.

EcoStruxure™ Micro data centres from Schneider Electric™ bring together power, cooling, physical security, and management software and services into pre-packaged rack solutions that can be deployed globally in any environment.

- Allows for rapid IT deployment wherever and whenever it is needed in weeks, not months.
- Reduce service visits and downtime.
- Securely manage system from anywhere.

Explore EcoStruxure™ Micro Data Centre from Schneider Electric

apc.com/uk

Life Is On Schneider Electric

VIEWPOINT

By Phil Alsop, Editor

The genie is out of the bottle – end of story!

If it wasn't so serious, it would be borderline hilarious – the IT industry, which has rushed headlong into all manner of technology innovations which have, to put it bluntly, completely re-engineered society – and not obviously for the better (but I appreciate there's a debate to be had), now finds the prospect of unfettered AI a horror too far. Why the sudden squeamishness?

Cynics would point out that those protesting the loudest are the organisations who are playing catch-up in the (sophisticated) AI space. If they can persuade everyone to take some timeout, they can no doubt work away in the background, catch up, and then pretend that either they never called for the pause in the first place, or, more likely, that, after careful consideration, AI should be allowed to develop unfettered.

And even non-cynics would have to concede that, having had almost zero interest in the growth of the IT and social media giants, and still spectacularly failing to regulate them in the way in which almost every other industry is (ie strict rules of behaviour), the chances of governments across the globe getting to grips with what's required are negligible. Like it or not, AI is here to stay, for better or, almost certainly, worse. I've not met anyone who thinks that trying to resolve a customer service issue with a chatbot is in any way whatsoever an improvement on speaking to a real human being. However, as it's almost impossible to speak to a human being these days, we are left with those painful conversations:

'In a few words, please tell me about your enquiry"
"I want to pay a bill'
"You want to take out a mortgage?"
"No, I want to pay a bill"
"You want to take out a mortgage, is that correct?"
"No, I just want to pay a bill"
"I'm sorry, but I do not understand what want"

I exaggerate slightly for effect, but the truth is, in so many ways, AI is a poor substitute for human interaction, and always will be. However, if AI users can replace a load of expensive employees with less expensive machines, and they all do it, choice disappears and the notion of quality customer service goes out of the window...unless, of course, AI is used to really understand a customer, and makes their purchasing decisions and transactions easier and faster as a result. In other words, the where and when of AI use is critically important for the whole transaction supply chain. And consumers have as much power to shape this future as the vendors. After all, if we all stopped shopping online, ecommerce wouldn't work very well!

So, rather than wring our hands as to whether or not AI should be allowed, time would be better spent ensuring that AI and AI-using organisations, are held to account. And made to understand that the cost of abusing the technology, and customers, might just make the idea of employing human beings a viable financial option.

DIGITALISATION WORLD

Editor
Philip Alsop
+44 (0)7786 084559
philip.alsop@angelbc.com

Sales & Marketing Manager
Shezhad Munshi
+44 (0)1923690215
shehzad.munshi@angelbc.com

Senior B2B Event & Media Executive
Mark Hinds
+44 (0)2476 718971
mark.hinds@angelbc.com

Director of Logistics
Sharon Cowley
+44 (0)1923 690200
sharon.cowley@angelbc.com

Design & Production Manager
Mitch Gaynor
+44 (0)1923 690214
mitch.gaynor@angelbc.com

Publisher
Jackie Cannon
+44 (0)1923 690215
jackie.cannon@angelbc.com

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

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO

Published by: Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry CV5 6SP
T: +44 (0)2476 718970 E: info@angelbc.com

Angel BUSINESS COMMUNICATIONS

Digitalisation World is published 10 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.

ISSN 2396-9016 (Online)

DW DIGITALISATION WORLD

Why aren't businesses baselining their security?

Baselining security is a great way to implement a foundational set of controls that aligns with the sensitivity of your data.

24

THE ANALYST

CYBERSECURITY

Nine in ten businesses are using AI-driven personalisation to drive growth

81% of businesses believe recent AI technology has the potential to positively impact customer experiences.

BUSINESSES WORLDWIDE are embracing the potential for artificial intelligence (AI) to provide personalised customer experiences, but customers remain cynical. That's according to the fourth annual State of Personalisation Report from Twilio (NYSE: TWLO), the customer engagement platform that drives real-time, personalised experiences for today's leading brands. This year's report shines a light on how businesses are experimenting with AI to differentiate and drive business growth, and provides guidance on how to get this right, starting with the critical need to raise consumer confidence in the technology.

Stark disconnect in AI confidence

To power even more sophisticated real-time customer experiences, businesses are turning to AI to harness high volumes of real-time data and power their personalisation efforts.

According to the report, 92% of global businesses are now using AI-driven personalisation to drive business growth. Four in five (81%) organisations also believe recent AI technology has the potential to positively impact customer experiences.

However, a disconnect exists between this enthusiasm and the comfort level of consumers: only 36% of European consumers are comfortable with companies using AI to personalise their experiences, and under half (49%) trust brands to keep their personal data secure and use it responsibly.

Quality and Privacy: Getting AI-driven personalisation right

AI-driven personalisation is only as good as its underlying dataset and, without robust data, customer experiences will likely miss the mark for consumers. It's a real challenge: half (50%) of global companies report that getting accurate data for personalisation is a struggle, an increase of ten percentage points compared to 2022, and 31% of businesses cite poor quality data as a major obstacle in leveraging AI. Further, four in ten (42%) European business leaders cited data silos as one of the biggest challenges to personalisation, compared to 26% globally.

Encouragingly, almost all the companies surveyed (97%) are taking steps to address consumer privacy concerns, demonstrating a commitment to responsible data use. The most popular step is investing in better technology, such as Customer Data Platforms, to manage customer data.

To maximise the potential of AI thoughtfully and responsibly, companies need to invest in data quality, leveraging effective, real-time data management tools and continuing to increase their use of first-party data. Sam Richardson, Customer Engagement Consultant at Twilio comments:

"AI has the potential to enhance the toolkit of every marketer and CX professional so they can meet growing customer demand for personalisation. However, there is still a lot of work to do for brands to reassure consumers and they must prioritise building trust and transparency. Real-time, first-party data will be key here for brands to maximise the potential of AI thoughtfully and responsibly."

Appetite for AI: Gen Z call for AI-infused experiences

As digital natives, Gen Z are both more influenced by personalisation and more willing to embrace AI. In fact, a third of Gen Z consumers already expect AI to be used in their experiences with brands. For example, nearly three

quarters (72%) of Gen Z consumers say that personalised experiences have influenced them to make a purchase. This compares to 66% of millennials, 57% of gen X and 42% of boomers. Meanwhile, only 15% of Gen Z consumers report being uncomfortable with AI being used to help brands personalise their experiences. This is notably lower than millennials (24%), gen X (34%) and boomers (43%).

The benefits of AI-driven personalisation

This year's report underscores the value of an AI-driven personalisation strategy for brands looking to both retain existing customers and acquire new ones, especially in today's competitive market. Sixty-two percent of business leaders cite customer retention as a top benefit of personalisation, while nearly 60% say personalisation is an effective strategy for acquiring new customers. Consumers also increasingly confirm the value of personalisation, with over half (51%) of European respondents saying they will become repeat buyers after a personalised experience. Richardson concludes: "There is a big opportunity for brands to build customer loyalty and lifetime value by engaging consumers with tailored experiences. And, ultimately, companies that provide a clear understanding of how customer data is being used will be best equipped to establish a strong foundation for successful personalisation efforts."

Decision-makers question sustainability strategies

New enterprise survey from CCS Insight shows that 58% of decision-makers are concerned about their company's sustainability strategy.

DESPITE the widespread focus on sustainability, organizations struggle to define what the term really means to them and how best to approach it, reveals a new survey into sustainability in enterprise, conducted by CCS Insight with NTT DATA as a partner. The survey of more than 1,000 senior roles shows that 58% of decision-makers are concerned about the strength of their company's sustainability strategy. This jeopardizes their ability to respond to appetite from customers and employees and to widespread enthusiasm for sustainability action.

The research firm's study exposes a variety of obstacles holding organizations back, with over a quarter of respondents naming costs and insufficient return on investment as major challenges to their sustainability initiatives. More troubling is that less than a third of decision-makers are confident that suppliers provide adequate metrics about their environmental efforts, and a further 70% don't believe their partners do enough to communicate their commitment. Although the environment dominates focus, many businesses prioritize economic, social and governance concerns. These decisions are a board-level responsibility, according to the survey, and the primary motivation for investment is to improve reputation, cited by 32% of senior leaders, followed closely by the need to comply with regulation, highlighted by 30%. Among UK executives, however, compliance with regulation and cost-cutting prove to be stronger pulls, cited by 46% and 34% respectively.

"Sustainability is starting to shift from aspiration to reality, with the foundations for corporate viability firmly in sight, along with hurdles that threaten to slow progress", commented Bola Rotibi, Chief of Enterprise Research at CCS Insight. "Over 60% of respondents said that customers are happy to pay more for sustainable products, yet less than 50% believe their firm should be paying more for sustainable materials and services — a dichotomy that shows the need for government incentives like tax breaks and grants to make sustainability more accessible and achievable", she added.

The findings validate the potential of technology to support different facets of sustainability. Improvements in renewable energy along with modernized infrastructure, application systems and IT operating processes were both named as critical investments for achieving sustainability goals. But respondents believe accurate measurement is where technology has the greatest opportunity, with 29% prioritizing intelligent measurement services that track carbon emissions in real time.

This message goes hand in hand with the need to demonstrate the credibility of companies' efforts: for 33% of respondents, the single most convincing action businesses can take to prove their commitment and avoid accusations of greenwashing is to provide transparent reporting. "Sustainability audits and materiality assessments are vital for decision-makers to understand priorities", said Maria Bell, Senior Analyst at CCS Insight. "They act as the framework for engaging, measuring and improving, and the basis for formulating and articulating the return on investment for the organization". Almost half of the respondents in the study use these assessments regularly, with a further 43% using them on an ad hoc basis. "Realizing a sustainable future is the top priority for NTT DATA, and it requires a mix of individual actions, clear leadership and strategically applied technology solutions. However, organizations are grappling with defining return on investment and evolving their sustainability strategies, said Robb Rasmussen, Senior Vice President, NTT DATA. "The results of this study will help organizations to define actions and priorities for creating a more sustainable, inclusive and equitable future".

The CCS Insight survey provides valuable insights into sustainability investments and directions, the constraints holding back operations and the trajectory of the sustainability market. "Sustainability isn't a service to buy, nor a box to tick, but a strategy to pursue", noted James Sanders, Principal Analyst of Cloud and Infrastructure at CCS Insight. "To thrive, organizations must navigate the available financial incentives, surface the most appropriate regulations for their operations, provide visibility into cost implications and demonstrate innovation".

95% of global businesses fail to fully optimise IT budgets

A study of more than 2000 IT professionals across 18 countries uncovers the pressure businesses are under to cut IT spend.

The latest annual study from Crayon and SAPIO Research has discovered that, because of this pressure, 90% of businesses list IT cost optimisation as a high priority for the business. This number increases even further in developing nations like the Philippines (97%) and South Africa (98%). Despite this, only 5% of businesses believe their IT budget is currently being fully optimised.

The research also found that 35% of global businesses are either actively assessing their IT spend or looking to cut it. This raises questions about where businesses will spend their budgets and how they plan to get the most out of their tech stack moving forward.

Prioritising the right business areas

Since the pandemic, business spending on technology has surged, with 56% of businesses spending more than USD 1 million per year on the public cloud alone. In the US, as many as 75% of businesses are spending at least this much, and in Norway, 12% of organisations are spending more than USD 25 million each year.

The report shows that the majority of this spend is on the technologies

needed to support existing infrastructure across security (83%), data (81%), and cloud departments (76%) - highlighting priority business areas.

“The economic landscape is proving incredibly difficult for almost every business across the globe,” says Hayley Mooney, General Manager, Crayon. “Our research highlights that business leaders everywhere are struggling to find a solution that will help them to remain competitive while cutting costs. We know too that when it comes to IT spending, many businesses do not give it the same kind of scrutiny as other major line items.”

Overcoming obstacles

The research found that one in five (20%) global businesses leave IT cost decisions to CFOs and finance teams. This rises to over a third (38%) of businesses in Switzerland.

Meanwhile, three in five businesses are implementing a FinOps practice, an evolving financial discipline that encourages business departments to collaborate on data-driven spending decisions. This practice is being widely adopted in the likes of Singapore (84%), Saudi Arabia (76%), Denmark (75%), the US (74%), and Norway (73%), highlighting the importance of cost optimisation across the entire business and suggests that organisations are trying to be more rigorous about extracting value from technology investments.

Despite this shift in focus, the biggest obstacle when it comes to optimising IT costs is a lack of time among senior decision-makers (31%).

This is followed by a lack of knowledge on how best to cut costs (28%), and a lack of visibility across the organisation’s spending (28%).

Digital boost, but barriers remain

NEW RESEARCH shows that businesses have faith in technology to boost their productivity but are facing major knowledge and skill barriers to complete their digital transformation projects. European businesses expect technology digital transformation projects to boost their productivity by an average of 38% in just 3 years with overall Return on Investment (ROI) expected in just under 5 years, senior decision makers have reported. But so far, on average only 15% of organisations have completed their digital transformation projects.

Almost 40% of respondents said they felt their organisation was lagging behind competitors when it came to digital transformation. The major barriers to deploying digital transformation technologies were: Lack of internal knowledge (35%), lack of internal IT people resource and skills (32%), concerns about the interoperability with existing IT infrastructure (30%) and a lack of external specialist IT support or awareness of specialist providers (30%).

“This research shows that European businesses understand that the latest technology solutions can transform their business operations and help them take major strides forward in productivity but for many there are still obvious barriers to overcome,” said Jan Kaempfer, Marketing Director for Panasonic Connect Europe.

Innovation leaders are 2.2X more likely to accelerate their way through economic uncertainty

Overall, businesses are optimistic about the strength of their business and innovation.

THE DELL TECHNOLOGIES INNOVATION INDEX, a new study polling 6,600 employees across 45+ countries, reveals that businesses are confident in the strength of their innovation in the face of global challenges. Over three quarters (84%) say that they agree their business has a vibrant culture of innovation, but the research shows a clear 'innovation gap' between perception and realisation.

Respondents were placed on an innovation maturity benchmark ranging from Innovation Leaders to Innovation Laggards to understand organisations' innovation maturity globally. This reveals an innovation perception gap, as the results show, despite the optimistic view of innovative business cultures, only 18% of organisations worldwide can be defined as Innovation Leaders and Adopters. In the UK, this figure is lower at only 5%.

This is important, as Innovation Leaders and Adopters are 2.2X more likely to accelerate their innovation during a recession than Innovation Followers and Laggards (who are more likely to decelerate). The good news is that the Innovation Index is a snapshot in time, and organisations can improve by priming their people, processes and technology for innovation.

Organisations need help to develop an innovation culture where all ideas can make a difference and learning through failure is encouraged. Businesses recognise this and are confident in their ability to deliver: in the UK, 56% believe that, in part, people join their company because they believe they'll be empowered to innovate. Globally, this figure is over three quarters (78%). However, they need to ensure that they fix the innovation gap. In the UK, half (50%) of respondents believe people also leave their company because they haven't been able to innovate as much as they hoped. At a global level, this figure is 59%. And in the UK, many (63%) respondents say aspects of their company's culture hold them back from being as innovative as they want to / can be. Furthermore, of those respondents based in the UK, 68% believe that their leaders are more inclined to favour their own ideas, which can hinder the development of an innovation-based culture within an organisation.

The report also gives businesses a guide on how they can course-correct these issues, highlighting the opportunities to innovate more and the barriers that impact innovation. For example, over half (51%) of respondents in the UK feel recognition by senior leaders would incentivise them to innovate more.

In addition to people-specific changes, businesses should also look at how they can improve their processes around innovation. For example, 74% of UK respondents say their leaders are more focused on the day-to-day running of the business than innovation, with 59% feeling that workload and a lack of time to innovate are hindering their teams' abilities. The prime barrier to innovation for respondents' teams is a lack of time to innovate, underscoring the importance of senior leaders modelling prioritisation. Without genuine, visible commitment at a leadership level, ambitious, skilled individuals can't achieve their full potential in innovation.

Providing more structure around innovation can also lead to better outcomes. While by its nature, innovation may be seen as an organic, ad-hoc pursuit, 63% of Innovation Leaders and Adopters say special, dedicated projects drive their

innovation. Half (50%) of Innovation Leaders and Adopters in the UK agree. Equally, 89% of UK businesses classed as 'Innovation Laggards and Followers' agree that they could automate more to free up band-with and enable teams to innovate more. Similarly, a significant number of respondents in the UK called for improvements to their organisation's ideation stage of innovation (77%).

The study findings point to the power of technology to enable innovation and the consequences of falling behind. At a global level, most (86%) actively seek technologies to help them realise their innovation goal. Conversely, 57% globally believe their technology is not cutting-edge and fear they will fall behind their competitors. Looking at the UK specifically, for example, the study revealed that only 19% of ITDMs have an AI/ML platform connected to the data warehouse, enabling predictive analytics and forecasting.

The study also explores where organisations are making gains and facing obstacles across five technology catalysts for innovation: multicloud, edge, modern data infrastructure, anywhere-work and cybersecurity. In nearly all areas, complexity is the most significant stumbling block to unlocking that potential.

Distributed workforce growth is redefining global business

SOTI warns of need to better manage rapid expansion of devices or risk losing out on efficiency and competitiveness.

THE DISTRIBUTED workforce now exists beyond the rise of hybrid, flexible or remote working environments, and it is having a significant impact on business operations in industries around the world. New global research from SOTI, "When Work is Anywhere: Managing Technology's Role in the Distributed Workforce," has revealed that organisations in healthcare, transportation and logistics (T&L) and retail are increasing their investment in new technology and devices as workforces and infrastructure become more widely distributed.

SOTI's research suggests that the distributed workforce is expanding beyond the rise of hybrid, flexible or remote working environments and is increasingly creating significant implications for industries that are not traditionally office based. As businesses expand, the report emphasises the need to better manage the ever-broadening scope of devices and technologies used if leaders want to avoid security risks and maximise efficiency and productivity gains.

Number of Devices in the Field Continues to Increase

Advancements in the Internet of Things (IoT), e-commerce, real-time supply chain visibility and critical communications across a global landscape have resulted in a seismic shift to more distributed operations. SOTI's research has revealed that in the UK, over one-third (36%) of respondents reported substantial growth in the number of devices being deployed across companies in the last year.

Additionally, 35% of UK organizations have seen an increase in the mix of device types (including smartphones, barcode scanners, rugged handsets, mobile computers, etc.).

As Devices and Data Grow, So Do Security Threats

As a result of this growth in device use, more data is being collected, processed and stored than ever before, fostering the need for data management security and compliance. The report found that over the last year, 44% of UK respondents cited the need for better access control to protect their IT network, while 32% increased their spend on mobile technology security. "The distributed workforce brings with it the potential for heightened productivity and flexibility, but it also creates more data challenges and complexity for businesses as the number of devices and applications increases," said Stefan Spendrup, VP of Sales, Northern and Western Europe at SOTI. "In addition to managing elevated data security concerns, organisations must consider the need for seamless visibility and device health monitoring. Our research shows that many larger businesses are already doing this very well, but smaller businesses that are still adapting to more distributed and remote workforces will need to invest more in device oversight going forward."

Outdated Processes Threaten Data Integrity

While digital workflows are becoming more common practice, manually enacted workflows continue to play a significant role. Over the past 12 months, 26% of all manually enacted workflows in UK businesses were done on paper, while 38% were managed via email. This unstructured method is especially concerning in the healthcare sector where the manual information and data is likely to be patient related and therefore unsecured.

The report found that 54% of UK respondents' workflows are managed manually. Globally, healthcare

organisations were the most likely to manage workflows manually at 61%, with retail (59%) being the second most likely. The report also found that U.S. (70%) and Australia (67%) respondents used manual processes most frequently.

With many organisations across various industries and regions continuing to use outdated, paper-based processes, this creates an elevated risk of sensitive data, such as patient and consumer payment information, falling into the wrong hands.

"Outdated legacy processes and software pose significant risks to organisations' data integrity and security. As workforces continue to become more widely distributed and device numbers grow, organisations need to move to prioritise overhauls of outdated systems or risk exacerbating the vulnerabilities that legacy processes pose," adds Spendrup. "Robust management of data in this increasingly dispersed workforce landscape is critical to ensuring a businesses' overall health and success. It can help enhance productivity, prevent malware attacks or breaches and even help address employee retention."

Business benefits for data mature companies

BMC has released findings from its global survey – "Profitable Outcomes Linked to Data-Driven Maturity" – which examines the relationship between data-driven practices and investment, and an outcome-based DataOps strategy.

THE NEED to unlock greater business value from data is clear, and a well-defined DataOps strategy is emerging as the key to manage and integrate analytics to uncover new opportunities, quickly respond to issues, and even respond to previously unforeseen challenges.

For organizations using DataOps methodology to support all data-driven activities, 41% strongly agree that their organization can apply data-driven insights to drive business goals compared to only 13% of respondents from organizations that do not.

Automation is necessary to scale up efforts around data use in an enterprise-wide, democratized data scenario, and a lack of automation (40%), along with data privacy and security requirements (38%) and data quality concerns (38%), are persistent pain points. However, organizations with more mature data-driven practices, DataOps strategies, and strategic technology investments were shown to deliver better results.

There are multiple reasons to pursue data-driven practices and data-driven maturity. The business outcomes that organizations cited they are most focused on improving through the

effective use of data are increased revenue (68%), customer satisfaction (55%), and cost reduction (50%).

- Seventy-seven percent of respondents with highly mature DataOps programs report that customer satisfaction has been an area of greatest impact in their organizations' use of data.
- Fifty-five percent of respondents state customer satisfaction as an effective data usage-related spending and strategy goal. Yet, only 39% say they are highly effective at using data for customer-facing processes.
- The top drivers for organizational adoption of data management tools and processes are data quality and integrity initiatives (57%), business insights that drive new revenue (53%), and cloud migration initiatives (50%).

"Organizations recognize that they are in the midst of a data conundrum and that deeper investments in their data strategies equate to improved business outcomes," said Ram Chakravarti, chief technology officer at BMC. "Enterprises will gain immense value by considering the entire flow and use of data from sources to insights and action, and having the right tools play a critical role in ensuring that success. Further, BMC's Autonomous Digital Enterprise framework encompasses the data-driven business as a key tenet, to help our customers thrive now and in the future."

Increase in breaches attributed to lack of security skills

New Fortinet research reveals escalating cyber risks due to the ongoing talent shortage while the number of organisations experiencing five or more breaches jumped by 53%.

FORTINET has released its 2023 Global Cybersecurity Skills Gap Report, which reveals ongoing challenges related to the cybersecurity skills shortage affecting organisations worldwide. Key findings from the global report include:

- The cybersecurity skills shortage has contributed to critical IT positions not being filled, which increases organisations' cyber risks, such as breaches.
- Cybersecurity remains a priority for boards of directors and there is executive demand for increased IT security headcount.
- Technology-focused certifications are highly regarded by employers, serving as validation of skill sets.
- Organisations recognise the advantage of recruiting and retaining diverse talent to help address the skills shortage, but doing so has presented a challenge.

The Costly Reality of the Increasing Cybersecurity Skills Gap

An estimated 3.4 million professionals are needed to fill the global cybersecurity workforce gap. At the same time, the 2023 Global Cybersecurity Skills Gap Report found that the number of organisations experiencing five or more breaches jumped by 53% from 2021 to 2022. One repercussion of this is that many short-staffed cybersecurity teams are burdened and strained as they try to keep up with thousands of daily threat alerts and attempt to manage disparate solutions to properly protect their organisation's devices and data.

Additionally, as a result of unfilled IT positions due to the cyber skills shortage, the report also found that 68% of organisations indicate they face additional cyber risks. Other findings highlighting increased cyber risks that could be partially attributed to the talent shortage include:

- Security intrusions are increasing: One resulting cyber risk is increased breaches, with 84% of organisations experiencing one or more cybersecurity intrusions in the past 12 months, up from 80% from last year.
- More organisations were impacted financially due to breaches: Nearly 50% of organisations suffered breaches in the past 12 months that cost more than $1 million to remediate, which is up from 38% of organisations compared to last year's report.
- Cyberattacks will continue to increase: At the same time, 65% of organisations expect the number of cyberattacks to increase over the next 12 months, further compounding the need to fill crucial cyber positions to help strengthen organisations' security postures.
- The skills gap is a top concern for boards of directors: The report demonstrated that more than 90% of boards (93%) are asking how the organisation is protecting against cyberattacks. At the same time, 83% of boards are advocating for hiring more IT security staff, emphasising the demand for security talent.

Upskilling Security Professionals and Developing More Talent with Training

The report also suggested that employers recognise how training and certifications can benefit their organisation in addressing the skills gap, while also serving as an advantage for anyone looking to advance in their current security profession, as well as for individuals considering transitioning into the field. Below are additional highlights from the report around training:

- Certifications are sought after by employers: Beyond experience, employers view certifications and training as reliable validation of an individual's skill set with 90% of business leaders preferring to hire individuals with technology-focused certifications, up from 81% the year before. Additionally, 90% of respondents would pay for an employee to get a cybersecurity certification.
- Certifications benefit both organisations and individuals. More than 80% of report respondents (82%) indicated their organisation would benefit from cybersecurity certifications and 95% of business leaders have experienced positive results from either their team or themselves being certified.
- Not enough professionals are certified: While certifications are highly regarded, more than 70% of respondents said it is difficult to find people with certifications.

Increasing Opportunities for Women, Veterans and Other Populations Can Help Solve the Skills Gap

While the report demonstrated that organisations are seeking ways to tap into new talent pools to fill cybersecurity roles, with 8 out of 10 organisations having diversity goals as part of their hiring practices, roughly 40% of organisations indicate they have difficulty finding qualified candidates who are women, military veterans, or from minority backgrounds.

- The report suggested that there was a decrease in veterans being hired compared to last year, with the number of organisations indicating they hired military veterans dropping from 53% in 2021 to 47% in 2022.
- At the same time, the report shows there was only a 1% increase year-over-year in organisations hiring women (88% in 2021 and 89% in 2022) and minorities (67% in 2021 and 68% in 2022).

MANAGED SERVICES SUMMIT EUROPE

13 JUNE 2023

NOVOTEL AMSTERDAM CITY
AMSTERDAM NETHERLANDS

The Managed Services Summit Europe is the leading managed services event for the European IT channel. The event features conference session presentations by specialists in the sector and leading independent industry speakers from the region, as well as a range of sessions exploring technical and operational issues. The panel discussions and keynotes are supported by extensive networking time for delegates to meet with potential business partners. This C-suite event will examine the latest trends and developments in managed services and how they have influenced customer requirements and the ability to create value through managed services for your organisation and customers.

THEMES, TOPICS AND TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero trust architecture (ZTA)
- Emerging advances in AI, automation and XaaS
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0)2476 718970

Leanne Collins
leanne.collins@angelbc.com
+44 (0)2476 718970

https://europe.managedservicessummit.com/

The top cybersecurity trends for 2023

Security and risk management (SRM) leaders must rethink their balance of investments across technology and human-centric elements when creating and implementing cybersecurity programs in line with nine top industry trends, according to **GARTNER, INC.**

"A HUMAN-CENTERED approach to cybersecurity is essential to reduce security failures," said Richard Addiscott, Sr Director Analyst at Gartner. "Focusing on people in control design and implementation, as well as through business communications and cybersecurity talent management, will help to improve business-risk decisions and cybersecurity staff retention."

To address cybersecurity risks and sustain an effective cybersecurity program, SRM leaders must be focused on three key domains: (i) the essential role of people for security program success and sustainability; (ii) technical security capabilities that provide greater visibility and responsiveness across the organization's digital ecosystem; and (iii) restructuring the way the security function operates to enable agility without compromising security.

The following nine trends will have a broad impact for SRM leaders across these three areas:

Trend 1: Human-Centric Security Design

Human-centric security design prioritizes the role of employee experience across the controls management life cycle. By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.

"Traditional security awareness programs have failed to reduce unsecure employee behavior," said Addiscott. "CISOs must review past cybersecurity incidents to identify major sources of cybersecurity induced-friction and determine where they can ease the burden for employees through more human-centric controls or retire controls that add friction without meaningfully reducing risk."

Trend 2: Enhancing People Management for Security Program Sustainability

Traditionally, cybersecurity leaders have focused on improving technology and processes that support their programs, with little focus on the people that create these changes. CISOs who take a human-centric talent management approach to attract and retain talent have seen improvements in their functional and technical maturity. By 2026, Gartner predicts that 60% of organizations will shift from external hiring to "quiet hiring" from internal talent markets to address systemic cybersecurity and recruitment challenges.

Trend 3: Transforming the Cybersecurity Operating Model to Support Value Creation

Technology is moving from central IT functions to lines of business, corporate functions, fusion teams and individual employees. A Gartner survey found that 41% of employees perform some kind of technology work, a trend that is expected to continue growing over the next five years.

"Business leaders now widely accept that cybersecurity risk is a top business risk to manage –

not a technology problem to solve," said Addiscott. "Supporting and accelerating business outcomes is a core cybersecurity priority, yet remains a top challenge."

CISOs must modify their cybersecurity's operating model to integrate how work gets done. Employees must know how to balance a number of risks including cybersecurity, financial, reputational, competitive and legal risks. Cybersecurity must also connect to business value by measuring and reporting success against business outcomes and priorities.

Trend 4: Threat Exposure Management

The attack surface of modern enterprises is complex and creates fatigue. CISOs must evolve their assessment practices to understand their exposure to threats by implementing continuous threat exposure management (CTEM) programs. Gartner predicts that by 2026, organizations prioritizing their security investments based on a CTEM program will suffer two-thirds fewer breaches.

"CISOs must continually refine their threat assessment practices to keep up with their organization's evolving work practices, using a CTEM approach to evaluate more than just technology vulnerabilities," said Addiscott.

Trend 5: Identity Fabric Immunity

Fragile identity infrastructure is caused by incomplete, misconfigured or vulnerable elements in the identity fabric. By 2027, identity fabric immunity principles will prevent 85% of new attacks and thereby reduce the financial impact of breaches by 80%.

"Identity fabric immunity not only protects the existing and new IAM components in the fabric with identity threat and detection response (ITDR), but it also fortifies it by completing and properly configuring it," said Addiscott.

Trend 6: Cybersecurity Validation

Cybersecurity validation brings together the techniques, processes and tools used to validate how potential attackers exploit an identified threat exposure. The tools required for cybersecurity validation are making significant progress to automate repeatable and predictable aspects of assessments, enabling regular benchmarks of attack techniques, security controls and processes. Through 2026, more than 40% of organizations, including two-thirds of midsize enterprises, will rely on consolidated platforms to run cybersecurity validation assessments.

Trend 7: Cybersecurity Platform Consolidation

As organizations look to simplify operations, vendors are consolidating platforms around one or more major cybersecurity domains. For example, identity security services may be offered through a common platform that combines governance, privileged access and access management features. SRM leaders need to continuously inventory security controls to understand where overlaps exist and reduce the redundancy through consolidated platforms.

CISOs must continually refine their threat assessment practices to keep up with their organization's evolving work practices, using a CTEM approach to evaluate more than just technology vulnerabilities

Trend 8: Composable Businesses Need Composable Security

Organizations must transition from relying on monolithic systems to building modular capabilities in their applications to respond to the accelerating pace of business change. Composable security is an approach where cybersecurity controls are integrated into architectural patterns and then applied at a modular level in composable technology implementations. By 2027, more than 50% of core business applications will be built using composable architecture, requiring a new approach to securing those applications.

"Composable security is designed to protect composable business," said Addiscott. "The creation of applications with composable components introduces undiscovered dependencies. For CISOs, this is a significant opportunity to embed privacy and security by design by creating component-based, reusable security control objects."

Trend 9: Boards Expand Their Competency in Cybersecurity Oversight

The board's increased focus on cybersecurity is being driven by the trend toward explicit-level accountability for cybersecurity to include enhanced responsibilities for board members in their governance activities. Cybersecurity leaders must provide boards with reporting that demonstrates the impact of cybersecurity programs on the organization's goals and objectives.

"SRMs leaders must encourage active board participation and engagement in cybersecurity decision making," said Addiscott. "Act as a strategic advisor, providing recommendations for actions to be taken by the board, including allocation of budgets and resources for security."

Worldwide IT spending to grow 5.5% in 2023

WORLDWIDE IT spending is projected to total $4.6 trillion in 2023, an increase of 5.5% from 2022, according to the latest forecast by Gartner, Inc.

DESPITE CONTINUED global economic turbulence, all regions worldwide are projected to have positive IT spending growth in 2023. “Macroeconomic headwinds are not slowing digital transformation,” said John-David Lovelock, Distinguished VP Analyst at Gartner. “IT spending will remain strong, even as many countries are projected to have near-flat gross domestic product (GDP) growth and high inflation in 2023. Prioritization will be critical as CIOs look to optimize spend while using digital technology to transform the company’s value proposition, revenue and client interactions.”

The software segment will see double-digit growth this year as enterprises prioritize spending to capture competitive advantages through increased productivity, automation and other software-driven transformation initiatives. Conversely, the devices segment will decline nearly 5% in 2023, as consumers defer device purchases due to declining purchasing power and a lack of incentive to buy (see Table 1). As enterprises navigate continued economic turbulence, the split of technologies being maintained versus those driving the business is apparent in their position relative to overall average IT spending growth.

“CIOs face a balancing act that is evident in the dichotomies in IT spending,” said Lovelock. “For example, there is sufficient spending within data center markets to maintain existing on-premises data centers, but new spending has shifted to cloud options, as reflected in the growth in IT services.” The IT services segment will continue its growth trajectory through 2024, largely driven by the infrastructure-as-a-service market, which is projected to reach over 30% growth this year. For the first time, price is a key driver of increased spend for cloud services segments, rather than just increased usage.

Exposure from bank failures remains contained, but Tech CEOs must prepare for disruption

The collapse of Silicon Valley Bank, Signature Bank and Credit Suisse created a shockwave within the banking and tech industries. While exposure remains relatively contained, tech startups are likely to face renewed questions and scrutiny from stakeholders, clients and prospects. “This is not just a tech problem, as these firms lent money to all forms of startups – not just IT,” said Lovelock. “Tech CEOs must urgently ensure they are moving their organization forward by conserving working capital, monitoring the impact on cash, securing access to credit and keeping a close eye on talent and culture. Once the organization is properly prepared, tech CEOs can then direct and engage employees to find, accelerate and execute on market opportunities.”

Tech shortages continue amidst layoffs

Even as layoffs continue to impact the tech industry at large, there is still a critical shortage of skilled IT labor. The demand for tech talent greatly outstrips the supply, which will continue until at least 2026 based on forecast IT spend. “Tech layoffs do not mean that the IT talent shortage is over,” said Lovelock.

	2022 Spending	2022 Growth(%)	2023 Spending	2023 Growth(%)	2024 Spending	2024 Growth (%)
Data Center Systems	216,095	13.7	224,123	3.7	237,790	6.1
Devices	717,048	-10.7	684,342	-4.6	759,331	11.0
Software	793,839	8.8	891,386	12.3	1,007,769	13.1
IT Services	1,250,224	3.5	1,364,106	9.1	1,502,759	10.2
Communications Services	1,424,603	-1.8	1,479,671	3.9	1,536,156	3.8
Overall IT	**4,401,809**	**0.5**	**4,643,628**	**5.5**	**5,043,805**	**8.6**

Source: Gartner (April 2023)

Table 1. Worldwide IT Spending Forecast (Millions of U.S. Dollars)

CELEBRATING 13 YEARS OF SUCCESS

The DCS Awards: 28 Categories across 4 Themes

THURSDAY 25 MAY

Leonardo Royal Hotel London St Pauls

DCS AWARDS 2023

Headline Sponsor

HUAWEI

Category Sponsors

BRIDGEWORKS simply making data flow

EnerSys

H2H COMMUNICATIONS

Schneider Electric

spa communications

BOOK YOUR TABLE PACKAGES NOW

Champagne Table - £3,395

Table of 10
4 bottles of champagne
3 bottles of house wine
3 course meal and coffee
Drinks reception
Evening Entertainment

Standard Table - £2,995

Table of 10
5 bottles of house wine
3 course meal and coffee
Drinks reception
Evening Entertainment

Half Standard Table - £1,795

Table of 5
3 bottles of house wine
3 course meal and coffee
Drinks reception
Evening Entertainment

SPONSORSHIP PACKAGES

The DCS Awards offer extensive branding and sponsorship opportunities through online advertising in our Datacentre Solutions & Digitalisation World publications, and of course at the awards ceremony itself.

For sponsorship opportunities and/or to book your awards table please contact: awards@dcsawards.com or call +44 (0)2476 718970

Supported by

dca The data centre trade association

Worldwide public cloud end-user spending to reach nearly $600 billion in 2023

Worldwide end-user spending on public cloud services is forecast to grow 21.7% to total $597.3 billion in 2023, up from $491 billion in 2022, according to the latest forecast from Gartner, Inc.

CLOUD COMPUTING is driving the next phase of digital business, as organizations pursue disruption through emerging technologies like generative artificial intelligence (AI), Web3 and the metaverse.

"Hyperscale cloud providers are driving the cloud agenda," said Sid Nag, Vice President Analyst at Gartner. "Organizations today view cloud as a highly strategic platform for digital transformation, which is requiring cloud providers to offer more sophisticated capabilities as the competition for digital services heats up."

"For example, generative AI is supported by large language models (LLMs), which require powerful and highly scalable computing capabilities to process data in real-time," added Nag. "Cloud offers the perfect solution and platform. It is no coincidence that the key players in the generative AI race are cloud hyperscalers."

	2022	2023	2024
Cloud Application Infrastructure Services (PaaS)	111,976	138,962	170,355
Cloud Application Services (SaaS)	167,342	197,288	232,296
Cloud Business Process Services (BPaaS)	59,861	65,240	71,063
Cloud Desktop-as-a-Service (DaaS)	2,525	3,122	3,535
Cloud Management and Security Services	34,487	42,401	51,871
Cloud System Infrastructure Services (IaaS)	114,786	150,310	195,446
Total Market	**490,977**	**597,325**	**724,566**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.
Source: Gartner (April 2023)

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

All segments of the cloud market are expected see growth in 2023. Infrastructure-as-a-service (IaaS) is forecast to experience the highest end-user spending growth in 2023 at 30.9%, followed by platform-as-a-service (PaaS) at 24.1% (see Table 1).

Gartner predicts that by 2026, 75% of organizations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform. "The next phase of IaaS growth will be driven by customer experience, digital and business outcomes and the virtual-first world," said Nag. "Emerging technologies that help businesses interact more closely and in real time with their customers, such as chatbots and digital twins, are reliant upon cloud infrastructure and platform services to meet growing demands for compute and storage power."

While cloud infrastructure and platform services are driving the highest spending growth, SaaS remains the largest segment of the cloud market by end-user spending. SaaS spending is projected to grow 17.9% to total $197 billion in 2023.

"The technology substrate of cloud computing is firmly dominated by the hyperscalers, but leadership of the business application layer is more fragmented," said Nag. "Providers are facing demands to redesign SaaS offerings for increased productivity, leveraging cloud-native capabilities, embedded AI and composability – particularly as budgets are increasingly driven and owned by business technologists. This change will ignite a wave of innovation and replacement in the cloud platform and application markets."

MANAGED SERVICES SUMMIT LONDON

13 SEPTEMBER 2023

155 BISHOPSGATE
LONDON, UK

The 13th Managed Services Summit London is the premier managed services event for the UK IT channel. 2023 will feature presentations by leading independent industry speakers, a range of sessions exploring technical, sales and business issues by specialists in the sector, and extensive networking time to meet with potential business partners. This is an executive-level event, exploring the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers.

THEMES, TOPICS AND TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero trust architecture (ZTA)
- Emerging advances in AI, automation and XaaS
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0)2476 718970

Leanne Collins
leanne.collins@angelbc.com
+44 (0)2476 718970

https://managedservicessummit.com/

IT market remains resilient

IT market performance remained patchy in April, with some vendors and resellers experiencing a sharp decline in growth while others continued to benefit from long-term enterprise commitment to cloud, digital transformation and security investments.

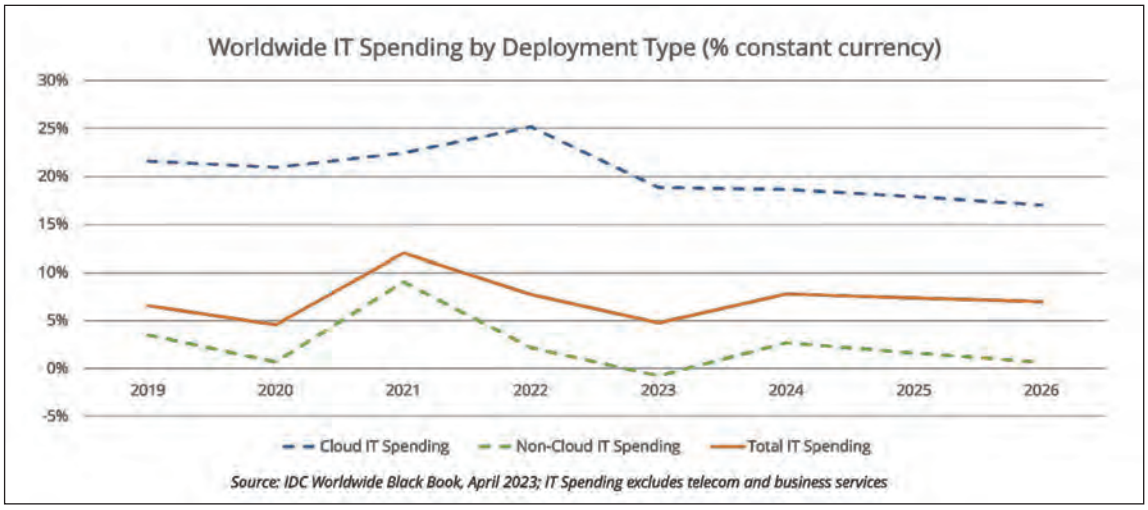
IN ITS LATEST monthly forecast for Worldwide IT Spending Growth, IDC forecasts overall growth this year in constant currency of 4.8% to $3.27 trillion, a slight improvement on last month's forecast which reflects resilient IT services market performance. IT services growth this year will be almost 6%, as large enterprises remain committed to long-term digital transformation investments despite short-term economic turbulence. Overall software spending growth will be almost 11%, driven mostly by cloud software revenues which will increase by 19%. This marks a slowdown compared to last year's cloud software growth of 25% and growth of public cloud IaaS will also slow compared to last year (from 33% in 2022, to 26% in 2023).

"Businesses are much more cost-conscious than a year ago, when inflation was adding to strong growth across much of the IT market," said Stephen Minton, Vice President in IDC's Data & Analytics research group. "Efforts to consolidate and control cloud budgets, along with economic uncertainty, mean that IT vendors are having to adjust to a slower pace of growth in the new post-COVID market. Nevertheless, continued double-digit growth in overall cloud spending is driving historic levels of resiliency for the tech industry."

While software and services spending continue to grow, this contrasts with a significant pullback in capital spending on hardware and equipment, as interest rates begin to have a direct impact on financing while recent turmoil in the banking sector has added to a general sense of economic uncertainty.

"Higher interest rates around the world are clearly a headwind for capital spending this year," said Minton. "Governments have reacted quickly to banking sector wild cards, but all of this just adds to expectations that a recession is still just around the corner."

PC spending will decline by 12% this year, while peripheral hardware spending will be down 3%. What little growth there is in hardware spending



in 2023 is increasingly concentrated in service provider and cloud-related budgets, but this growth will also be weaker than a year ago. Server/storage spending is forecast to increase by just 2% this year, down from 23% in 2022. While cloud infrastructure will continue to grow, non-cloud server/storage spending will decline by 7% this year.

"For IT vendors and resellers which are mostly providing on-premise and traditional hardware or software to their clients, this is shaping up to be a tough year," said Minton. "SMB and consumer markets are feeling the impact of higher interest rates and declining confidence. While large enterprise investments in cloud and digital transformation remain resilient, and service providers continue to invest in cloud infrastructure, other areas of the IT market are experiencing a slowdown as the post-COVID shakeout continues to disrupt inventories, supply chains and demand."

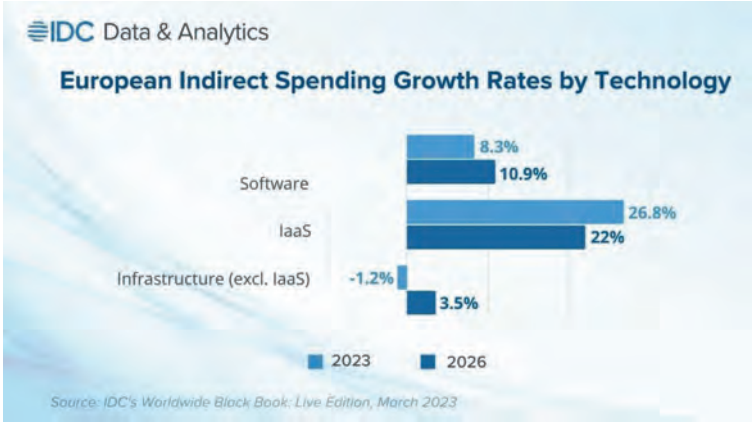
European ICT spending

To the Worldwide Black Book: Live Edition published by International Data Corporation (IDC), ICT spending in Europe is expected to grow by 2.8% year on year in 2023 in constant currency terms, reaching $1,184.5 billion.

DESPITE the challenging macroeconomic climate, software and services investments will continue to grow, exceeding the growth of overall ICT spending. Cloud migrations will accelerate, as many companies will try to mitigate the adverse effects of the impending recession and its accompanying disruptions. Platforms such as AI and business intelligence will continue to receive heightened attention as they enable organizations to attain a competitive edge. During turbulent geopolitical situations, companies typically increase investments in security solutions, due to intensified cyberattacks and emerging regulations.

However, continued inflation in many countries, weakening consumer confidence, and export disruptions has created uncertainty that is adversely affecting some hardware markets, mainly PCs, tablets, and monitors. The first signs of recession in some European countries and the subsequent slowing business activity will also negatively affect the server and storage infrastructure markets, which are projected to record a year-on-year decline in 2023.

Infrastructure spending (excluding infrastructure as a service) via indirect channels is expected to decline in Europe by 1.2% year on year in 2023. By 2026, almost half of server and storage spending will continue to be generated through the channel. "Partners will continue to help vendors in maintaining robust connections with customers, in order to address the ever-evolving customer needs for holistic solutions rather than delivering infrastructure components," says Lubomir Dimitrov, research manager with IDC Data & Analytics, Europe.



The increased emphasis on digital transformation has resulted in changes in customers' expectations, driving the demand for customized multi-vendor solutions that cater to specific customer segments and industries.

This resulted in increased spending flow from indirect sales through partners. Spending on software and services is expected to continue driving overall market growth. By the end of 2023, approximately 58% of software spending — i.e., applications, application development and deployment, and system infrastructure software – is forecast to go through the channel.

However, the increasing number of companies transitioning to cloud will continue to make the direct channel an important source of revenue generation to vendors.

Performance Intensive Computing as a Service market

International Data Corporation (IDC) has published its first-ever forecast for the performance intensive computing as a service (PICaaS) market. IDC projects that the total worldwide PICaaS market will grow from $22.3 billion in 2021 to $103.1 billion in 2027 with a compound annual growth rate (CAGR) or 27.9% over the 2022-2027 forecast period.

IDC recognizes the performance-intensive computing as a service market as a fast-developing category of the public cloud services offerings with end users leveraging the advantages of special cloud technology to run mathematically intensive computations. Mathematically intensive computations are typically found in artificial intelligence (AI), high-performance computing (HPC), Big Data and analytics (BDA), and engineering/technical use cases.

The percentage that the PICaaS market represents of the total $241.3 billion as-a-service market for 2022 is 12.5%. The PICaaS market encompasses revenue generated by cloud service providers for compute, storage, and software offerings within their infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) portfolio for AI, BDA, HPC, and engineering/technical workloads.

The BDA as a service market segment will remain the predominant contributor to the overall market throughout the forecast period, followed by AI as a service. The HPC-as-a-service market segment shows the highest growth rate, followed by AI, and then engineering/technical workloads.

Drivers for the market growth, according to IDC, are:

- Performance-intensive computing goes mainstream and is increasingly considered mission critical
- A growing number of enterprises identify themselves as digital businesses

But the market is also hampered by several inhibitors:

- Complexity in managing hybrid technologies and lack of HPC talent within enterprises
- Transferring of PIC workloads from the public cloud back into dedicated IT environments
- Disrupted IT spending plans (due to supply chain issues, labor shortages, economic slowdown, and geopolitical tensions)

IDC recommends that suppliers:

- Formulate an end-to-end bundled performance-intensive computing as a service product offering
- Demonstrate a secure and compliant cloud infrastructure
- Segment prospects by their level of enterprise intelligence and communicate on early vendor engagement opportunities and cost transparency
- Align teams with performance-intensive computing capabilities and demonstrate abilities to work with evolving roles such as chief data officer
- Be a trusted advisor of hybrid deployment models for performance-intensive computing workloads, offer multicloud support, and showcase a strong partner ecosystem

"IDC is projecting significant growth in the performance-intensive computing as a service market, which measures the revenue that providers generate from offering compute instances, storage, and software for Big Data and analytics, AI, HPC, and engineering/technical workloads," said Madhumitha Sathish, research manager, Performance Intensive Computing as a Service, at IDC. "These workloads all demand more advanced technologies, and cloud service providers are investing heavily to capture market share in a market that will grow to $103.1 billion by 2027."

APC

Just say where you want it...

We'll take care of the rest.

EcoStruxure™ Micro data centres from Schneider Electric™ bring together power, cooling, physical security, and management software and services into pre-packaged rack solutions that can be deployed globally in any environment.

- Allows for rapid IT deployment wherever and whenever it is needed in weeks, not months.
- Reduce service visits and downtime.
- Securely manage system from anywhere.

Explore EcoStruxure™ Micro Data Centre from Schneider Electric

apc.com/uk

Life Is On Schneider Electric

Why aren't businesses baselining their security?

Baselining security is a great way to implement a foundational set of controls that aligns with the sensitivity of your data.

BY DAVID ADAMS, SECURITY CONSULTANT AT PRISM INFOSEC

STANDARDS AND FRAMEWORKS such as the Cyber Essentials scheme, ISO 27002, NIS Cyber Security Framework, UK Government Minimum Cyber Security Standard and NIST 800-53B (Control Baselines for Information Systems and Organisations) apply best practice risk mitigation and this means they can be carried out without the need to conduct an initial risk assessment. Added to which, underwriter data suggests SMEs that are Cyber Essentials certified are 60 percent less likely to make a claim.

Yet, despite these advantages and the ubiquity of these standards, those choosing to adopt them remain in the minority. The Cyber Security Longitudinal Survey published earlier this year, found only 19 percent of businesses had adopted Cyber Essentials and only 15 percent were ISO 27001 compliant. Not baselining security can lead to the implementation of either too few or overly prescriptive controls which can result in negative impacts ranging from avoidable cyber-attacks to staff using workarounds which then introduce secondary risks. This means these businesses are much more exposed than they need be and the likelihood is that businesses will see their cybersecurity eroded still further due to shortages in the cybersecurity workforce.

Time for intervention

Recognising the importance of getting businesses onboard with these standards, the government has attempted to identify precisely why take-up has been so lacklustre. The Cyber Security Incentives and Regulations Call for Evidence and subsequent Review make for damning reading. It was found the current standards and frameworks were "unfit for purpose" because they were either too basic or too prescriptive while the "multiplicity of cyber risk management standards and frameworks results in confusion as to which is most appropriate for their particular organisational risk posture".

The conclusion drawn was that clarity was needed and the government would need to be more interventionalist as there had been insufficient drive in the market to create improvements in organisational cyber risk management.

Consequently, the National Cyber Security Centre (NCSC) overhauled the Cyber Essentials scheme this year, introducing five major changes. These ranged from the shared responsibility model for cloud security, to guidance on home working, multi-factor authentication, and what should be regarded as 'in scope' when implementing the standard (hint: all end user devices). Further clarity was also provided on BYOD, legacy software, and the security patching window.

These changes saw Cyber Essentials certifications rise 16 percent during the first half of the year. However, this still equates to only 100,000 accredited businesses out of the 1.4million companies with staff that are based in the UK. The prime reason for this is that reality is that most only implement such standards out of contractual obligations and its very much seen as a compliance task. This is a missed opportunity because such standards can be dovetailed to the data type, obligations, risk arena or risk appetite of the business to provide a recognised level of assurance to other parties that demonstrates the business is diligently managing its cyber risk.

Making risk relevant

So, what needs to happen for businesses to baseline their security effectively? It's not just a matter of whether businesses are aware of these standards (the Cyber Aware campaign for Cyber Essentials has already got the message out) and it's not that they're not being observed (the failure rate for Cyber Essentials is very low at just 3.5 percent month-on-month as of October 2022). Rather, it's a matter of making these standards relevant to the business with real gains.

The review claims there need to be more incentives to drive adoption. These include cost:benefit analysis to so that the impacts and costs of failing to mitigate risks can be gauged. Many underestimate the true costs of breaches and so under invest in cybersecurity or struggle to build the business case.

To counter this, we can expect more transparent reporting on breaches and impacts from the DCMS. Steps will also be taken to elevate the status and input of 'Market Risk Managers' such as insurers and procurement managers who have a limited role today but the potential to influence investment in risk management. There will also be more emphasis on accountability, with larger businesses likely to mandated to assess and address cyber risk.

Legislation, for now, will focus those deemed to offer critical digital services through the tightening of the Network and Information Systems Regulations. To further boost adoption, there's also a case for mandating Cyber Essentials through the use of tax rebates or providing incentives in the form of lower cyber risk insurance. So far the government has stopped short of taking this step but we could well see the cyber insurance sector offer lower premiums to certified companies.

The steps the government has taken in its intervention will see baselining become far more widespread, creating a minimum bar for security. But there's also the potential for businesses to use that baseline more constructively.

Better use of the baseline

To start with, effective cyber security should be applied in such a way that it mitigates or successfully manages security events as they occur so that they do not seriously impact the organisations drive towards its strategic goals. For this to happen, it is critical that the organisation communicates its business strategy clearly in order that its cyber security strategy can be aligned to support the strategic direction of the organisation. So there needs to be buy-in and steer from the top when implementing these standards.

When it comes to implementation, the organisation must maintain an understanding of the quantity, sensitivity and displacement of the information it uses as part of its day-to-day business. This information, regardless of whether it is in documentary, electronic or intrinsic form, will have risk appropriate controls applied and these should be assessed for effectiveness at regular intervals, either internally or through an external third party.

Data disposition and flows will need to be mapped and managed to ensure that information remains secure, intact and readily available to those with a proven need to know and is protected in all its forms whether at rest or in transit.

All organisations are subject to forces which can shape the way information is used. So, any changes affecting how data is collected, processed, stored, shared or disposed of must involve risk assessment to ensure that any new risks are mitigated and redundant risks retired. Here, the baseline controls can be adjusted to meet the demands of the change in risk climate or business operations.

Improving your security processes

Where to put your focus for real world results.

BY PAUL BAIRD, CHIEF TECHNICAL SECURITY OFFICER, QUALYS

YOU WOULD BE HARD PRESSED to find an organization that doesn't want to improve their security. Collectively, billions of dollars, pounds and Euros are spent globally on security in an effort to keep threat actors at bay - according to IDC, spending in Europe will grow 10.6 percent in 2023, with total spending estimated to reach $71 billion annually by 2026. But how can we ensure that this spending makes a difference?

Security teams must think holistically about attack paths, examine threat actor behaviours to understand what could wreak the most havoc, and quickly control threat activity when a breach occurs. They must adopt risk-based methodologies that allow cybersecurity technologies, processes, and people to converge and collaborate.

Today's tools often focus solely on generating more and more detections and alerts, which simply is not enough to help keep organisations secure. Now, more than ever, companies need insights that help prioritise their most severe vulnerabilities across their most critical assets, with a firmer grasp on how to resolve them before attackers can exploit them. The Qualys Threat Research Unit (TRU) looked at trillions of data points in 2022 to see where the biggest risks were for businesses, and where IT security teams can focus their efforts.

Deal with the patching gap

Patching has always been problematic for organisations of all sizes and industries. For small companies, it is difficult to manage as they often have limited staff. For large enterprises, the sheer number of devices, teams, business units and different teams responsible for the variety of IT and security processes involved increases the overall complexity. This slows down how quickly patches get deployed, leaving the gate open for threat attackers to exploit at their leisure.

According to our data, it took attackers 19.5 days on average to weaponise a new software vulnerability. However, it took security teams 30.6 days on average to patch those vulnerabilities. This means that attackers have 11.1 days to exploit that issue before patching is completed. Patching for those critical issues speeds up once an attack is successful and defenders know they have to concentrate on that particular attack vector, but there is still a gap that can lead to exploits.

The average time to patch is around 30 days, while the time to weaponise malware was nearer to 40 days. Ransomware takes even longer to weaponise, with an average of around 45 days. This means that these attacks take advantage of older issues that have not been patched. By prioritising patching for those vulnerabilities that could be weaponised, or that are specifically risky to your organisation, you can prevent problems as early as possible. This helps you avoid future emergency drills and overtime on responding to those issues.

Automate patching where you can

Understanding the best way to automate patching for your critical applications can drastically reduce the amount of time that it takes to protect applications against attack, as well as supporting the vast majority of users. For example, Chrome and Windows comprise one-third of the weaponised vulnerabilities data set, with 75 percent of these issues used by named threat actor groups. Because of the risk involved in these issues, organisations typically patch them first and most

thoroughly. According to our data, the mean time to remediate (MTTR) issues with these products globally is 17.4 days, or about 2 and a half weeks. Secondly, these two products have an effective patch rate of 82.9 percent. In essence, Windows and Chrome are patched twice as fast and twice as often as other applications in the business.

Automating the deployment process helps to speed up the delivery and successful deployment of patches. We can see this in our data - for patches that could be automatically deployed, they were put into place 45 percent more often and 36 percent faster than those that had to be deployed manually. Based on this, you can achieve better patching performance for your team if you take advantage of automated deployment where you can.

Understand who is targeting you

Aside from the new vulnerabilities that might be disclosed, there are a myriad of other attack vectors. A large issue in today's threat landscape are Initial access brokers (IABs), which look to create footholds within company networks and then sell them on to other groups. IABs look for issues around misconfigurations in perimeter devices or publicly-facing IT assets that they can exploit, or seek out opportunities based on phishing individuals. Their job is to get that foot in the door which they can then monetise, either by finding sensitive company data, deploying ransomware or selling that access to another threat actor. Because Windows and Chrome are patched so quickly, IABs tend to look at other software products for potential vulnerabilities. These other products tend to be lower priorities for security teams, but they still require patching over time. By understanding this 'long tail' of risk, you can manage it appropriately.

Malware is not the only attack approach

While a lot of the attention for security professionals will be spent on preventing malware attacks, misconfigurations are a huge area that must also be addressed. These issues fall into two groups - web applications and cloud infrastructure.

For web applications, misconfigurations can include a range of missed settings that would allow an attacker to get access, receive more data than they should, or build up more information on the rest of the company's infrastructure. Inadequate or missing encryption can expose data, while site injection attacks can lead to broken web applications or stolen data. Using the OWASP Top Ten list for web application security best practices can help, but the best approach is to look at how you can collaborate with your organisation's software and web developer teams to improve deployments ahead of time. By helping these teams to understand potential threats and prioritise risks, you can help them be more efficient in fixing problems that represent the most potential for attacks.

It is not enough to scan your web applications for potential security issues, as every application will display issues - based on our anonymised data from 370,000 web applications, there were 25 million flaws discovered. Instead, you have to help your developer colleagues to prioritise the risks that are the most pressing and potentially dangerous.

On the cloud infrastructure side, similar challenges exist. Cloud deployments can be complex, but there are also opportunities for simple misconfigurations to lead to data breaches. One of the top reasons for data leakage is because cloud storage buckets or databases were mistakenly left accessible without passwords or encryption. Checking for any instances of these misconfigurations in your cloud deployment should be automated, so you can automatically flag any problems for rapid response.

Using cloud security benchmarks can help you improve your security posture. For example, the Center for Internet Security provides benchmarks for the three major popular cloud security platforms - Amazon Web Services, Microsoft Azure and Google Cloud Platform. The CIS Benchmark for AWS provides several security controls to measure public access to data in S3 buckets, and it includes checks on status as well as preventative controls. Using these preventative measures can make it much harder to make mistakes or inadvertently expose data, but they are less likely to be used.

While a check for public exposure shows that only one percent of buckets are publicly exposed, there are two preventative controls that are implemented only 50 percent of the time. This means that there is a high potential for someone to inadvertently make an S3 bucket public. Although protecting the entire bucket is crucial, it is also essential to safeguard the files stored in the bucket from being publicly accessible. Unfortunately, only 40 percent of organisations are currently using those preventative controls to prevent files from being accessed publicly.

Looking at the whole picture around cloud and infrastructure, taking a proactive approach around security controls and mitigations can help you prevent potential problems more efficiently. Using the CIS Hardening Benchmarks is an effective starting point to address these potential threats, while individual controls associated with ransomware-specific techniques must be reviewed carefully too.

Overall, improving your security approach involves using automation, data and tools to support your team in being effective. However, the biggest opportunity comes from prioritising your own specific infrastructure gaps and risks. No one knows your infrastructure as well as you do, so use automation and data for how it can make you more efficient. At the same time, you can help your team to deliver better results.

SESIP's role in the IoT ecosystem

Armed with the SESIP methodology, certification bodies have a toolkit that comes complete with efficient and cost-effective security evaluations and accelerates the go-to-market of certified products for vendors.

BY GIL BERNABEU, TECHNICAL DIRECTOR, GLOBALPLATFORM

THE NUMBER of Internet of Things (IoT) devices available throughout the globe is forecast to be 29 billion by 2030. With technology adoption showing no signs of slowing down – as consumer spending on smarter technology continues to skyrocket – the need for greater efficiency, that is both cost-effective and secure, is clear.

However, while a smarter future is an exciting prospect throughout the globe, the introduction of even more connected devices brings about a brand-new set of challenges.

From interoperability obstacles to an increasing number of standards and regulations to swiftly address, product vendors must be equipped with not only the tools but also the knowledge to work efficiently and cost-effectively when evaluating the security of products.

The statistics evidence the need for additional layers of security too – with many devices still having little to no protection. According to research, only 4% of deployed IoT products have secure measures in place, leaving enterprises and consumers extremely vulnerable to cyberattacks.

While it is no secret that some industries are more susceptible to data breaches than others – for example, healthcare, finance, education and retail, to name a few – threats can apply to any product, of any value, if they do not have robust security in

place. And when protection is lacking, any level of cyberattack can create costly damages to not only revenue, but overall brand reputation.

The role of certification bodies in the IoT's quest for greater security

As technology continues to advance at a rapid rate, the number of attacks does the same – and they are getting more sophisticated by the day. With the variety of device types and limited cybersecurity expertise throughout the consumer landscape, this ultimately leaves a significant challenge to overcome for many. Cyber-crime is reportedly going to cost the global economy $10.5 trillion annually by 2025, so there has never been a more critical time to implement stronger security measures and more robust infrastructure to cope with the growing number of IoT devices.

To support their quest to keep cyberattacks at bay, IoT stakeholders must understand the positive impact that certifications can have on building trust when deploying a product. Certification bodies play a central role by maintaining the quality of security labels and raising the overall levels of security assurance across the ecosystem.

Security laboratories in particular have a never-ending task to maintain their cybersecurity skills so they can perform state of the art evaluation. But the IoT stakeholders are the ones that set requirements and overall schemes objectives that should adequately address product security for their market. In addition, they may select optimised and standardised evaluation methodologies or proprietary ones. The trusted role of the SESIP methodology

That is where the Security Evaluation Standard for IoT Platforms (SESIP) methodology comes to the fore. Ensuring that IoT device makers and certification bodies can adopt and establish their own IoT device security certification schemes, SESIP presents a flexible and efficient approach that both addresses unique challenges of IoT product development and drives consistency across markets.

Firstly, the SESIP methodology uses a simple and universal language to explain security requirements. Based on an ISO standard created by experts, there has been a conscious effort made to provide product vendors – that are not security experts – with a language that is consistent with their product features and ultimately supports their product improvement needs. Overall, this simple language allows IoT stakeholders to define a security profile that is understood by product vendors.
Secondly, as the demand to keep up with emerging cybersecurity legislation continues at pace, the SESIP methodology allows certification bodies to develop schemes that recognise and reuse the security capabilities of a product's components, regardless of device type. That means IoT stakeholders can adopt trusted components that have already been evaluated and combine to create a new product with greater efficiency, cost-savings, and security.

Reducing the complexity of certification and addressing interoperability challenges

It is no secret that the IoT market remains fragmented because different industries demand different security measures. Not only that, different countries or regions are defining security, privacy or resilience regulation that request specific security features to be evaluated.

However, the good news for IoT stakeholders is that SESIP addresses such challenges by aligning certification schemes to ensure there are comparable evaluations across the entire IoT ecosystem. By mapping to other standards – from bodies such as ETSI, ISO/IEC and NIST – the methodology provides a common and optimised approach for evaluating the security of connected products across a broad range of regulatory and security frameworks, as well as specific vertical regulations.

> Without SESIP, the IoT ecosystem will only become more fragmented because each industry, region – and sometimes country – will continue to define its own security needs using different languages and requirements

As an alternative solution that reduces the complexity of certification, SESIP helps to develop trust among consumers. It also encourages greater adoption of their products or services and addresses interoperability challenges with emerging technology. Without SESIP, the IoT ecosystem will only become more fragmented because each industry, region – and sometimes country – will continue to define its own security needs using different languages and requirements. And the result? Cybercrime vulnerabilities rise due to discrepancies in policy making and expertise.

Armed with the SESIP methodology, certification bodies have a toolkit that comes complete with efficient and cost-effective security evaluations and accelerates the go-to-market of certified products for vendors. And regardless of industry, collaboration will always be key, therefore if SESIP-certified laboratories, certification bodies and device makers can work together to ensure the methodology is accessible to all – and consistently applied throughout each sector – this can empower product vendors to future-proof their offering and further strengthen security assurances for consumers.

Cutting cybersecurity costs

Consolidating the technology stack during the recession.

BY TIM WALLEN, REGIONAL DIRECTOR, UKI & BENELUX, LOGPOINT

A KEY PRIORITY for firms in 2023 will be navigating the rising cost of doing business. Between energy price hikes, inflationary pressures, impending corporation tax increases, labour shortages and ongoing supply issues, companies are becoming more aware of their costs as they look to mitigate the worst effects of volatile economic conditions.

Security budgets are likely to be scrutinised with firms working to scale down their expenses and streamline operations more proactively, and CISOs will be required to justify spend more than ever. However, while this will undoubtedly create additional challenges for pressurised security teams, it is not all bad.

A looming recession could serve to accelerate strategic improvements thanks to faster board approvals, providing CISOs with the opportunity to carry out some much-needed spring cleaning as they consolidate the cybersecurity technology stack which typically ranges between ten and fifty point security solutions.

Cutting the security stack makes complete sense from an operational standpoint. The more tools you have in place, the greater the workloads of the security teams who must monitor and maintain them. Standalone point solutions often don't integrate easily and, as these tools generate numerous alerts, and it's difficult to measure how efficient they are and if they protect what needs to be protected. The stack also contributes to alert fatigue, increasing stress and burnout among team members.

It therefore stands to reason that 75% of CISOs are now pursuing a vendor consolidation strategy (up from 29% in 2020) in a bid to improve overall risk posture, gain efficiencies of scale and eliminate the need to integrate separate tools, according to Gartner's Top Trends in Cybersecurity 2022 — Vendor Consolidation report.

Doing so not only reduces pressure on the security team, but uncovers overlaps and security gaps

in the security posture, which enables CISOs to identify cost saving potential and justify spend. It can also help save costs associated with licensing, training and maintenance.

Avoid solution siloes

One of the most economic ways to cull the stack without experiencing performance losses is to combine multiple tools into one platform. Almost all security operations are centred around Security Information and Event Management (SIEM), which is the foundation of security data collection and analysis. But while a SIEM can alert you of any nefarious activity going on internally or externally, it doesn't typically house the tools required to respond effectively.

As a result, many businesses resort to using separate solutions like Security Orchestration, Automation and Response (SOAR) or User and Entity Behaviour Analytics (UEBA) to automate responses where possible and prioritise the investigation and response efforts. This is a logical approach, yet issues begin to arise where firms adopt fragmented solutions.

The security market can be a difficult one to navigate. Today, there are tons of seemingly necessary tools on the market touting how they're the next "ground-breaking" cybersecurity solution, encouraging organisations to jump on the bandwagon and invest.

Unfortunately, this can leave firms with a portfolio of siloed, conflicting systems that become extremely difficult to integrate within existing IT systems, leaving SOC teams overworked and overwhelmed. In addition, the CISO loses the ability to understand how the cybersecurity setup is performing, missing out on opportunities to make better decisions and interact with the board in a meaningful way.

A converged security operations setup

Instead, organisations should prioritise the big picture, working to develop a seamless converged security operations setup. Not only can this eliminate the complexities associated with managing and operating siloed security products, but it can also deliver several other benefits.

First, it can reduce the number of point solutions vendors and integrations that need to be maintained, reducing the burden on already overstretched security teams. By converging security technologies, organisations are empowered to unlock efficiencies of scale to help build defensive capabilities, giving users a transparent and comprehensive centralised overview that allows them to better manage cyber threats and reduce business risk.

Second, it improves security performance, helping to accelerate threat detection, investigation and response efforts. With a single platform, organisations can more easily surface high-value alerts, receive threat context to prioritised cases, and use data to optimise the efficacy of the broader security infrastructure.

It's a case of combining technologies to improve outcomes. A converged SIEM, for example, can deliver machine learning and AI behaviour-based analysis via UEBA and automated detection and response via SOAR. In essence, a converged security setup will automatically add threat intel, business context and entity risk to observations to transform weak alerts into meaningful investigations where analysts have orchestration and automation actions at their fingertips to respond faster than ever.

Thirdly, cost transparency will also be boosted with a converged solution. Costs can be controlled more easily, while insights into how often each solution is used can also be surfaced, providing indications of relevancy, importance, and total cost of ownership (TCO).

In this sense, by combining complementary tools into one platform, a much fuller picture is obtained. Indeed, organisations become empowered to accelerate threat detection, investigation and response efforts, all while achieving efficiencies of scale and consolidating the tech stack.

At the end of the day, your SIEM is more than just a place to aggregate security events. It's also the starting point for integrating threat intelligence into key insights and creating a highly effective incident response process for your security team.

Therefore, by integrating vital tools such as SIEM, UEBA and SOAR, you will be empowered to improve efficiency for your SOC teams and increase transparency for executives at all levels, providing tangible and actionable value to the companies and security teams implementing them.

Is being cyber insured worth the rising cost?

Insurance or no insurance, the threat landscape is evolving, and your security measures need to evolve with it.

BY JOHN WAREING, ACCOUNT DIRECTOR, RED HELIX

WITH MAJOR hacking scandals making global news, it's no secret that cybercrime is on the rise. Owing to the rapid digitalisation and major advances in network technology, we have become more reliant on our devices. This, in turn, has created an array of new endpoints for criminals to target, leading to hacking offences more than doubling in the year ending March 2022, compared with the year ending March 2020.

Not only have the number of crimes increased, but the impact of these breaches has also become more severe. Criminals are gaining access to huge amounts of personal data from enterprises, including bank details and ID documents, as seen in the recent attack on Arnold Clark. Companies integral to the UK's national infrastructure are also being crippled by cyber attacks, such as Royal Mail, who has seen severe disruption to its overseas delivery capabilities following a breach.

Owing to the higher severity of breaches, the average cost of a single attack in the UK has reached a seven-year high at £4.56 million which has, in turn, had a major impact on both the rates and the requirements for cyber insurance. As the frequency and value of pay outs has gone up, so has the price of cyber insurance – rising by 66% in the third quarter of 2022, following a peak increase of 102% in the first quarter.

And, while policies will of course differ between insurers, there is an ever-growing checklist of requirements that organisations need to adhere to in order to be accepted. It is no longer an expectation that companies show they've taken appropriate action to protect themselves against cyber crime, it is a requirement. And those that can't prove they have provided sufficient technical solutions and training to secure their network will be denied insurance or refused payment when making a claim.

This comes alongside an increased number of exemptions from Insurers as to what they will, and will not, cover. One of those most notable of these recently was Lloyd's of London's decision to no longer protecting against 'state-sponsored attacks', meaning that any attacks an Insurance company could claim were linked to a nation-state would no longer be covered. For businesses, this has led to a few questions. Firstly, what are the requirements to qualify for cyber insurance and what will be covered? And secondly, given the robust level of security your organisation will achieve through ticking off the checklist of requirements – is the cost of insurance actually worth it?

Am I eligible for cyber insurance?

Across the board insurance is becoming increasingly challenging to get hold of. Not only are costs soaring, but underwriting requirements are higher and a greater scrutiny is being placed on risk mitigation and security program maturity. Therefore, for businesses to be eligible for cyber insurance, they need to show that they already have robust security in place. While the specific requirements for cyber insurance will vary – based on the industry, insurer, the size of the business and the type of coverage required – there are some universal security measures that every business looking for insurance needs to have in place: Endpoint Detection and Response (EDR) – As the number of endpoints (including laptops, mobile phones, tablets etc) continues to rise, so does the number of entry points for criminals. EDR is designed to monitor, discover, investigate and respond to threats across a network of endpoint

devices and is becoming a must-have for those seeking insurance.

Multi-Factor Authentication (MFA) – This one almost goes without saying, as it has become a common part of day-to-day business operations, but having MFA in place for business networks, emails and applications is another requirement Insurers are looking out for.

Separate backups

As attacks become more advanced, having a single data backup is no longer enough, as this can potentially be compromised. Having multiple backups, in different locations, is another requirement for cyber insurance.

Cyber awareness training

Even the strongest cyber security measures can be brought down by a hole in the human firewall. Therefore, Insurers will need businesses to provide regular training, and assessment, to their employees to mitigate the risk of breaches through social engineering attacks.

Penetration and stress testing

As with assessments to show staff are trained against cyber threats, Insurers also need to see that cyber security tools can withstand the threats in the environment. Showing the results of penetration and stress tests can help alleviate concerns around a business' level of protection.

Zero Trust Network Access (ZTNA)

Whilst ZTNA may not yet be a universal security measure, it is growing in popularity, and has become a widely accepted choice for providing secure network access - replacing outdated VPNs. It may not be something all Insurers are looking for now, but will likely become so down the line due to the increased security it provides.

Having these measures in place can help towards eligibility for cyber insurance, however actual requirements will vary on a case-by-case basis. Additionally, while implementing the above can help organisations to secure insurance and start better protecting themselves, certain industries will have their own regulations that need to be met – such as the Telecommunications (Security) Act (TSA) for Network Operators – and it is unlikely that Insurance companies will accept those that don't comply with Government legislations.

Is cyber insurance worth it?

Ultimately, there is no 'yes or no' answer to whether cyber insurance is worth the cost. It comes down to the details of the individual policy, and will require in-depth investigation into exactly what will be covered, any stipulations and limits included in the contract, and the price of the premium.

One of the many elements that should be considered is that in the event of a breach some Insurers will insist on choosing the company who investigates the attack themselves. And while that may not seem like a big deal initially, it becomes more of an issue when combined with the recent exemptions around state-sponsored attacks, giving the Insurance company the power to determine if there is a link to a nation-state or not – and ultimately if that affects the eligibility of the claim.

Organisations therefore need to ask themselves whether they are comfortable with this and whether they are happy to trust the results of the Insurer's investigation, particularly if they have their own means to investigate a breach – be it their own technology, or an existing relationship with an attack remediation company – as an insurance company may reject findings that differ from its own.

This may draw the level of worth provided by cyber insurance further into question. What is, however, without a doubt 'worth it' is ensuring your cyber security continues to be at a level where its eligibility for insurance couldn't be brought into question. As the threat landscape continues to grow, businesses need to remain aware of the evolving threats, and increase their security measures alongside them, so they can continue to protect themselves, their business partners and their customers from attack. And while cyber insurance requirements themselves shouldn't be used as a base level for an organisation's security, the higher bar being set does indicate the need to reassess levels of protection.

Furthermore, as additional security compliances are imposed on some sectors, such as the aforementioned TSA and the EU's DORA (as well as a likely UK equivalent) for Financial Services, reviewing and upgrading security measures isn't just important for protecting your business – it is becoming a more important part of the criteria for companies assessing their 3rd party suppliers.

The bottom line

Ultimately, the choice to take out cyber insurance will come down to the cost of the policy, the level of cover you're able to receive and any stipulations or exemptions. Nevertheless, whether you are insured or not, paying attention to the requirements for cyber security – both from insurance companies and Government regulations – is of upmost importance. Adhering to security guidelines, such as cyber essentials and cyber essentials plus, can help to strengthen your security environment, while regular testing of cyber defences can determine any areas of your security that need to be upgraded. This will not only help your organisation qualify for cyber insurance should you want it, as well as likely reducing your premium, but it will also majorly reduce the chance of a successful breach.

Insurance or no insurance, the threat landscape is evolving, and your security measures need to evolve with it.

The evolution of ransomware recovery

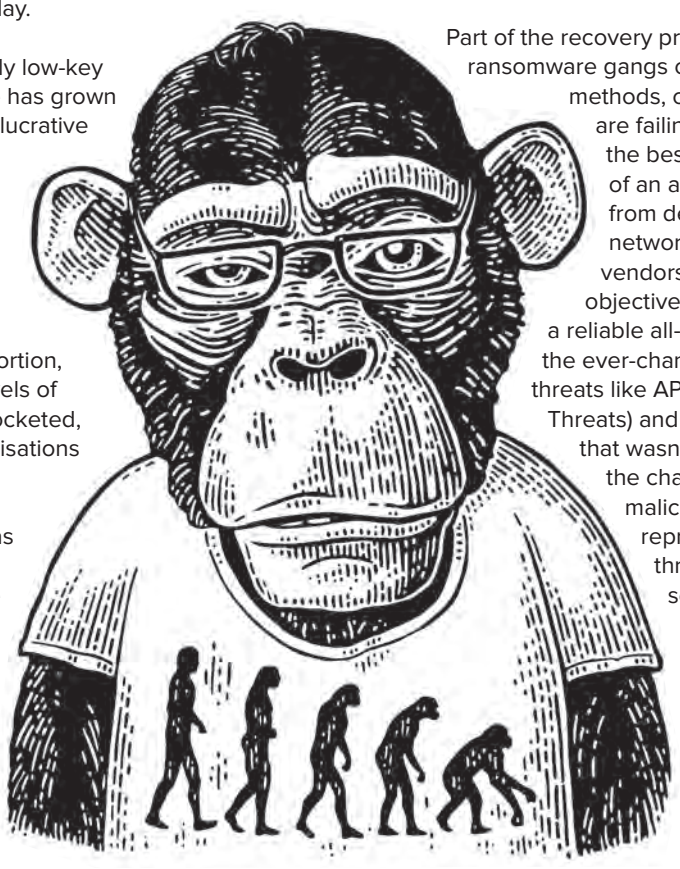
IT organisations are dealing with an ever-increasing complexity in providing data security and disaster recovery due to the pervasive danger of ransomware and the deployment of new apps at the core, in the cloud and at the edge.

BY CHRISTOPHER ROGERS, TECHNOLOGY EVANGELIST AT ZERTO
A HEWLETT PACKARD ENTERPRISE COMPANY

BACK IN 1989 when the first ransomware attacks occured, they were relatively unsophisticated – at least by today's standards. Distributed via floppy disks, their encryption methods could be easily reversed, and the ransom payments being demanded were a tiny fraction of the eye watering amounts seen today.

Since this relatively low-key start, ransomware has grown into an incredibly lucrative international cybercrime industry with the ability to bring organisations large or small to their knees.

As the cost of extortion, downtime and levels of disruption have rocketed, data-driven organisations are becoming more focused on recovery as well as prevention. Yet, most ransomware victims still regularly suffer extended outages and are unable to recover all their data. In fact, a recent study found that only 1 in 7 companies recover all their data after an attack. Worse still, paying the ransom offers no guarantee of a return to business as usual with only 14% of businesses who paid a ransom to their attackers in the past 12 months subsequently getting 100% of their data back.



Part of the recovery problem is that as ransomware gangs continue to evolve their methods, current backup vendors are failing to keep pace. Clearly, the best outcome for the target of an attack is to prevent it from deploying malware on the network at all. While security vendors are focused on this objective, in general they still lack a reliable all-round defence against the ever-changing nature of security threats like APTs (Advanced Persistent Threats) and Zero Day exploits. And if that wasn't enough, there remains the challenges presented by malicious insiders, who still represent one of the biggest threats to organisational security.

The result? Being on the receiving end of a ransomware attack is no longer a question of 'if' or even 'when' – today, it's about 'how often?'. In 2020, for instance, more than 60% of businesses

were hit by ransomware attacks, fuelled by trends such as the growth of 'ransomware as a service' and nation-state activity.

From backups to data protection

To prepare for this unfortunate reality, many organisations rely on backups as a tried and tested technology used across a multitude of data loss and recovery use cases. Indeed, backup vendors are among the most vocal in the ransomware prevention and recovery ecosystem, aggressively marketing their solution when compared to other manufacturers of data protection software and storage systems that are designed to protect against the impact of ransomware.

These older generations of data protection software and storage systems, however, are simply unable to stop data loss or downtime because the majority of future apps will reside in the cloud or at the edge. As a result, most businesses lack confidence in their backup and disaster recovery (DR) options with an IDC poll suggesting only 28% of participants had complete trust in the capabilities of their backup solution to restore all data.

In addition, many organisations employ a variety of technologies, including disaster recovery solutions to assure data recovery in the event of any loss, such as a ransomware attack, alongside backup and recovery software, snapshots, mirrors and replicas. This brings with it an ever-increasing level of complexity in delivering cost-effective and high performance data protection and disaster recovery strategies.

Instead, IT organisations are searching for solutions that can reduce Service-Level Agreements like RTO and data loss SLAs (RPO) to almost zero. To meet this need, Continuous Data Protection (CDP) is becoming more important because it can dramatically reduce the risk of data loss, regardless of the reason, while also speeding up and simplifying the recovery process. Since CDP records data changes as they are made, the effective RPO is lowered to seconds and the "backup gap," which can be a significant factor in data loss, is essentially eliminated.

IT organisations are dealing with an ever-increasing complexity in providing data security and disaster recovery due to the pervasive danger of ransomware and the deployment of new apps at the core, in the cloud and at the edge. But by using CDP, recovery operations can be completed rapidly and with little data loss, going back to a point that was just seconds or minutes before an attack or any disruption, including those caused by ransomware. This is especially true when combined with recovery orchestration and automation, and as a result, organisations should make CDP, the most important recent development in recovery technology, a top priority if they want to adopt an effective strategy that tackles the threat posed by ransomware head-on.

Turning the tables on tomorrow's threat agent

The more customers can address alert fatigue whist upgrading their security posture, the better.

BY NICK EDWARDS, VP PRODUCT, MENLO SECURITY

LONG GONE are the days of every worker being a nine-to-five commuter. While some employees retain a preference of working in the office all the time, many are embracing the willingness of employers to offer flexible alternatives such as remote and hybrid models.

Research shows that UK staff went to the office 3.8 days per week on average pre-pandemic, this having dropped to 1.4 days per week in 2022.

While the new normal is undoubtedly improving workplace cultures and driving forward a new frontier that centres around enhancing the employee experience, in the case of security, it has had dramatic implications.

No longer are staff members all accessing the internet behind a security perimeter – where applications were all controlled, and VPNs could be used on a remote basis where necessary to replicate safe sessions.

Today, employees can readily use the internet to access corporate networks housing sensitive and personal data within key applications and SaaS platforms from a range of devices in a variety of locations. And as a result, the web browser has now become the biggest attack surface and target for threat actors, many of whom are leveraging and exploiting it successfully.

These changes in working patterns have undermined the methods that security practitioners traditionally relied upon to secure their organisations. Indeed, firms have been forced to re-evaluate their business needs and develop entirely new strategic roadmaps, leaving CISOs scrambling to find ways in which to bake in security best practices.

Understanding of modern security requirements is improving

During the past three years, the picture has thankfully become somewhat clearer. Today, organisations typically require a consistent set of security policies for all users – be it an employee in the office, or an engineer commuting and using a cellular network. Regardless of the device they are using and app they need to use, there needs to be a clear security framework that guides universal best practice across the board.

Unfortunately, firewalls and VPNs simply aren't designed to deliver that. Instead, organisations are now tapping into cloud services that can effectively manage comprehensive security permissions and deliver key insights, detailing exactly who each user

is, and what they can respectively access on the corporate network.

This has become a highly intelligent process. More advanced security setups can manage privileges and assess the security posture on an ongoing basis, adapting permissions based on the type of user, location of that user, what systems they're trying to access, and when they're trying to access them.

It is critical that companies adapt in this way. Not only has security become a more complex undertaking with many different moving parts, but the threat landscape has also changed dramatically. According to Statista's Cybersecurity Outlook, the global cost of cybercrime was estimated to be $8.44 trillion in 2022 – over seven times the $1.16 trillion reported in 2019.

Resultantly, security has fundamentally become a boardroom issue. It cannot be an afterthought. Instead, the CISO now needs to be a major part of business decision making. CISOs are there to add value, applying security as an integral part of the technology stack. To achieve this effectively, they must have an ongoing understanding of each new product, how customers will consume them, and the inner workings of the architecture underpinning each solution.

Responsibility isn't solely on the CISO, however. A culture in which security becomes a leading priority needs to be instilled throughout the organisation – every enterprise will have different models and workforce structures, and there are many roles that need to be thinking about security more actively.

Interestingly, a Gartner study found that 88% of boards regard cybersecurity as a business risk rather than solely an IT problem. The threat of ransomware and nation-state-backed threat outfits has changed cyber perceptions, with those at the top table becoming increasingly aware of the challenges.

Bolstering defences in the face of evasive and complex threats

This growing appreciation provides CISOs with the opportunity to bridge the gap between technical professionals and the broader C-suite. They are now enjoying greater influence over boardroom discussion to ensure best practices are instilled more readily. However, given the continual advance of new threats, this is the bare minimum that is required.

Today, the browser is the new office. Where previously you'd have had to have gone into a conference room to have a meeting, employees are now typically spending 75% of their working days on a web browser or using web conferencing applications.

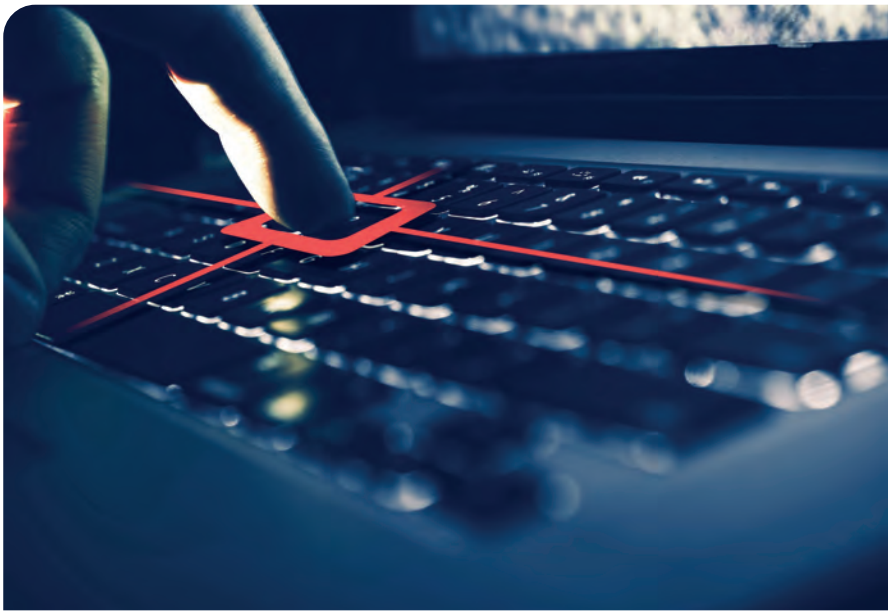
Unfortunately, as we have mentioned, threat actors are aware of this and the opportunities it presents, adapting their techniques accordingly. There has been a significant uptick in the use of evasive attack methods leveraged by nefarious actors, enabling them to bypass traditional security tools such as secure web gateways (SWGs), firewalls, phishing detection tools and malware analysis engines.

Known as highly evasive adaptive threats (HEAT), these attacks are actively exploiting the web browser as the attack vector, rendering a decade or so of security investments focused on network perimeter protection almost obsolete.

It's a frustrating reality that has left many security departments having to completely rebuild their defences from scratch. Yet the dangers of HEAT simply cannot be ignored. Research conducted by the Menlo Labs team revealed that there had been a 224% increase in HEAT attacks in H2 2021 – a trajectory that only seems to have continued through 2022.

Menlo Security also surveyed 505 IT decision makers at firms with at least 1,000 employees across the US and UK last year found more than half (55%) of organisations encountered advanced web threats at least once a month, with one in five facing them on a weekly basis.

There are several increasingly concerning signs. Hackers now looking to overcome two factor authentication through social engineering campaigns to access corporate assets, for example. And it is clear that browser-based attacks are not just becoming more common, but more successful. Indeed, almost two thirds of the respondents (62%) to our survey had seen a device compromised by a browser-based attack in the previous 12 months alone. Further, it is also clear that some of these



Threat intelligence teams are already looking at massive amounts of data. They don't want to have to sift through even more to find one needle in a haystack. The more customers can address alert fatigue whist upgrading their security posture, the better

attacks could have been avoidable. Indeed, the survey shows that less than three in 10 organisations have advanced threat protection solutions in place on all endpoint devices used to access corporate applications and resources, while almost half (45%) had not added any new capabilities to their network security stack in the previous year.

Embracing a security-first culture

For many, there continues to be an issue around prioritisation.

Given the threat landscape, security now more than ever before needs to be a forethought. Yet approaching things in such a manner is easier said than done in the case of organisations that have always made operational changes first before implementing security adaptations on top.

It's about embracing a security-first culture – a shift that can be accelerated via a few simple strategies.

Specifically, CISOs should focus on building a greater consciousness of security within the workforce, enabling every worker to be more adept at spotting suspicious activities such as social engineering attempts. The good news is that a growing number of roles are coming to the realisation that they have a responsibility to practice good security hygiene. CISOs may operationalise this mentality, but it is becoming everybody's responsibility to embrace it.

Further, organisations should ensure security parameters extend to all endpoints capable of accessing the corporate network. This can go a long way in enabling firms to thwart any kind of threat.

Perhaps the most important realisation is that there is no quick fix when it comes to the cyber security of an organisation. Good management principles must apply, centred around hiring well, training well and executing toward a roadmap that is forward looking whilst prioritising security.

Of course, everyone is looking for the next shiny new widget or silver bullet technology capable of keeping everyone safe, but the reality is that the strongest teams are the ones that are consistently deliberate with their intentions, taking longer to steer the ship whilst doing so in a way that's secure and safe and executed according to the needs of the business.

Isolating the end point

In the case of browser threats, a good starting point for mitigation is removing user interaction and traffic from the browsers themselves as much as possible. This might sound like an impossibility given the criticality of the browser to modern day working models, but it's easily achieved with the right supportive solutions.

Isolation technology can be used to isolate the end point from the internet browser, re-writing it and then delivering it as a clean stream.

This prevents any malicious code from ever reaching user endpoints by moving the point of execution to a disposable, cloud-based container that acts as digital air gap between the browser and corporate networks. It also reduces the number of alerts reaching the security operations centre (SOC) which can exacerbate alert fatigue – a major issue facing security professionals as they attempt to navigate the demands of the new normal.

Addressing security alert fatigue

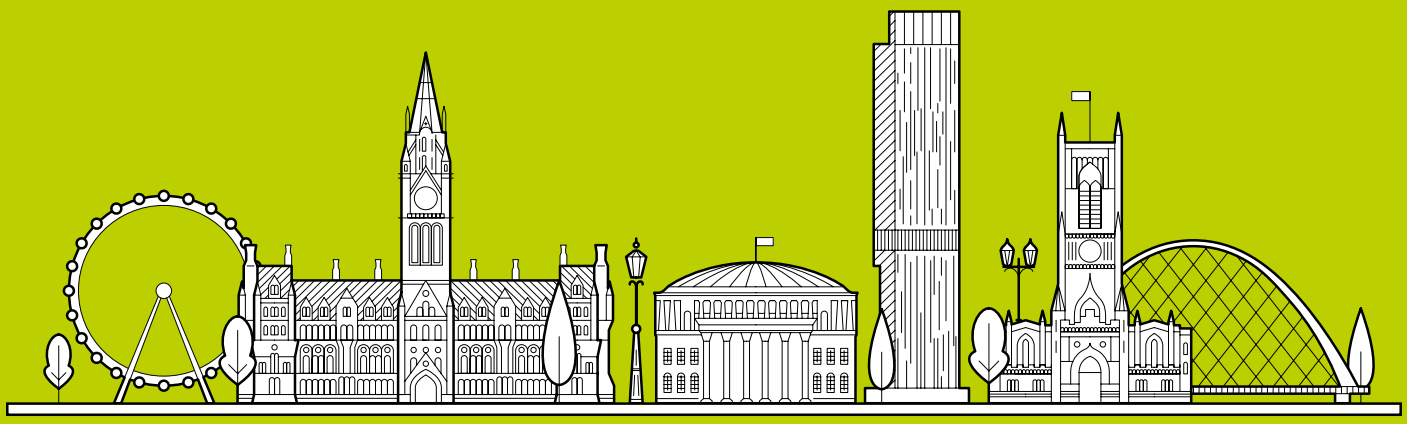
We're confident that this approach will soon become the mainstream model for internet security. It's not necessarily about eliminating proactive detection and identification. Instead, it's about creating clean working environments while dramatically reducing the burdens on the SOC from alerts and false positives.

Threat intelligence teams are already looking at massive amounts of data. They don't want to have to sift through even more to find one needle in a haystack. The more customers can address alert fatigue whist upgrading their security posture, the better.

MANAGED SERVICES SUMMIT NORTH

21 NOVEMBER 2023

MANCHESTER CENTRAL,
PETERSFIELD, MANCHESTER



Managed Services Summit North (sister events in London and Amsterdam) are the leading managed services events for the UK and European IT channel. Featuring conference session presentations by major industry speakers, the Summit provides opportune networking breaks for delegates to meet with potential business partners. The unique mix of high-level presentations plus the ability to explore and debate the most pressing business issues with sponsors and peers across the industry makes this a must-attend event for any senior decision maker in the IT channel.

THEMES, TOPICS AND TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero trust architecture (ZTA)
- Emerging advances in AI, automation and XaaS
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0)2476 718970

Leanne Collins
leanne.collins@angelbc.com
+44 (0)2476 718970

https://north.managedservicessummit.com/

The ‘Golden Pipeline’ principles for securing the supply chain

As a cloud native security vendor, we know the stakes are high when it comes to supply chain vulnerabilities.

BY NURIT BIELORAI, GO-TO-MARKET MANAGER, SUPPLY CHAIN SECURITY AT AQUA SECURITY

ON THE ONE HAND we work at the frontline with hundreds of customers, helping them tackle the most critical security challenges associated with their digital transformation.

On the other, we need to ensure our software development life cycle is second to none and excels when it comes to delivering the security, agility and speed of deployment organisations need to stay on the front foot where innovation is concerned.

Having implemented security on thousands of software supply chains, we’re able to provide a behind-the-scenes look at what it takes to build immutability and security into today’s software development pipelines. And how the resulting ‘golden pipeline’ will prove reliable time and time again.

Incorporating security by default

Under growing pressure to deliver software faster,

developers are increasingly reliant on open source code and other third-party components that enable them to build products and services more rapidly. The problem is this introduces potential vulnerabilities into development pipelines that will likely expose organisations to supply chain attacks. As a result, building security into the development process has become a top priority for organisations looking to avoid the risk of a supply chain compromise. This is no easy task when security teams are wrangling multiple tools to try and connect the dots, and need to avoid compromising development flows at all costs.

This is why we recommend that organisations incorporate comprehensive security testing and validation from the get-go and across the entire end-to-end application development and deployment process.

The golden pipeline principles – start clean, stay clean, and store approvals

By embedding and automating security and enforcement practices across the supply chain, organisations can create a 'golden pipeline' that ensures an application is validated at every stage of development. So, by the time it reaches production, it's as clean as possible – and all known supply chain risks have been eliminated.

When it comes to building a golden pipeline, organisations should first aim to start 'clean' by integrating auto-triggered periodic scans into their source code management (SCM) system. Designed around a defined policy that triggers specific actions and responses, this will help assure the quality and integrity of existing components, keeping them up to date with a real-time updated vulnerability and risk database.

Next, to ensure their pipelines 'stay clean' and are secure-by-default, every new pull request by a developer should activate an automated scan that generates a pass/warn/fail outcome. These results are then notified to developers via the SCM, together with any fix suggestions.

At the build stage a definitive automated scan provides the final audit and seal of approval. If compliant, the component gets the green light and goes into production – accompanied by a detailed software bill of materials (SBOM) and security manifest that provides full visibility into all software components and dependencies. If yes, this is stored in a manageable pane with all other SBOMs, for easy and clear investigation whenever needed. If not, teams gain insights into next actions to take.

By incorporating robust policy-driven controls into the development pipeline, organisations are able to get instant feedback on supply chain risks. This means vulnerabilities can be caught and fixed the moment they are introduced, and before they reach runtime, a stage in the application's lifecycle where stakes (and costs) are much higher.

Long term gains and ROI

Many of the companies we work with have committed to this golden pipeline reporting approach, they've achieved some significant returns on investment. Alongside protecting revenue streams from the risks arising from application breaches or compliance issues, they've benefited in a number of other key ways:

- Automating previously manual processes to streamline their programme orchestration and cut the time and cost associated with patching and remediation.
- Giving back valuable time and bandwidth to their security and development teams that can be used more productively on other projects.
- Consolidating and reducing the number of security tools they need to procure and use – generating further sizeable cost savings that go straight to the bottom line.

In addition to elevating the supply chain defence posture of the enterprise itself, implementing a golden pipeline enables organisations to develop and deploy applications faster. Generating efficiencies along the way will make a lasting contribution to the long-term sustainability of the business.

The Internet of Things (IoT) cybersecurity crisis

IoT security should be a consideration for any organization's overall cybersecurity strategy.

BY ZEKI TUREDI, EMEA CTO, CROWDSTRIKE

OVER THE PAST DECADE, the Internet of Things (IoT) has become one of the most critical and valuable technologies. The IoT is a system of connected devices embedded with sensors and software that allows them to transfer data over a network. This can include anything from a pacemaker in a human's chest or a network-accessible screen, to a car with sensors that gather information on engine temperature or fluid levels. IoT has provided a vast number of benefits for businesses as it allows companies to actively observe their systems and collect data, insights and performance metrics without the need for human intervention.

But there are some issues. Protecting, monitoring and remediating threats related to this vast network of connected devices and technologies constantly gathering, storing and sharing data via the internet has made IoT security challenging. So much so that even the FBI recently issued an industry-wide warning around cyber criminals increasingly targeting internet-connected devices for the purpose of exploiting their vulnerabilities. So what's the solution?

IoT is the future, but is it safe? It's safe to say that IoT isn't slowing down. IoT research shows that IoT connections, such as smart home devices, connected cars and networked industrial equipment, exceeded traditional connected devices, such as computers and laptops, for the first time in 2020, representing 54% of the 21.7 billion active connected devices. It is estimated that by 2025, there will be more than 30 billion IoT connections, which equates to about four IoT devices per human on the planet. But, as with any successful technology, there are always problems. IoT hacks have been growing over time. The most significant attack was the Mirai Botnet hack in 2016, which targeted DNS service provider Dyn using a botnet of IoT devices. The Mirai malware successfully managed to infiltrate networks, where it automatically searched for more vulnerable devices and, using stolen credentials, gained access and repeated the process to gain control. This attack dismantled servers and significantly affected major media platforms such as Netflix, Reddit and Twitter. But IoT hacks don't only affect tech giants. Cybercriminals are also targeting

hospitals' medical devices and placing many patients at risk. St. Jude Medical, an American global medical device company, in 2017 experienced hackers gaining access to its patients' pacemakers. This gave the adversaries access to alter the pacemaker's functions and even adjust settings that could potentially prove fatal to patients.

IoT security has become an even more pressing concern for organizations, given the recent shift to remote work due to COVID-19. With people now relying on both their home network and personal devices to conduct business activities, many digital adversaries are taking advantage of lax security measures to carry out attacks.

Understanding what you're up against

Despite this heightened risk and broader threat surface, IoT cybersecurity is often still overlooked or minimal. Inadequate IoT security policies pose a grave risk for organizations, since any device can serve as a gateway to the wider network. Once adversaries gain access through a device, they can move laterally throughout the organization, accessing high-value assets or conducting malicious activity, such as stealing data, IP or sensitive information.

Many companies focus entirely on endpoint cybersecurity. But, the same levels of diligence needs to be applied to IoT devices. If IoT devices are not equipped with the same level of protection, the organization as a whole is at risk of a cyberattack. Research shows that 33% of companies that have adopted IoT consider cybersecurity issues related to the lack of skilled personnel to be the most critical concern for their IoT ecosystem. This lack of skill and knowledge results in multiple common cybersecurity malpractices, such as using default credentials for matters of convenience and not staying up to date with the latest software or firmware updates on their device, which are necessary to prevent software vulnerabilities and manage bugs. Cybercriminals are always adapting their methods of intrusion. A common pathway of attack for criminals is known as 'on-path attacks'. These rely on the nature of IoT devices, which frequently don't encrypt their data by default. The attacker then has the ability to relocate between two devices that trust each other and exfiltrate any data being passed between them. Another common vulnerability is stealing or deciphering simple credentials. Cybercriminals are experts at identifying weak or generic passwords and using them to slowly gain access and even admin control. Denial of Service (DoS) attacks are also a common technique. Here, cybercriminals will gain control of an IoT device and begin flooding the website with fake traffic, which overwhelms servers with web traffic and denies legitimate users from carrying out their everyday activities.

Securing IoT can secure a company's future

IoT security should be a consideration for any organization's overall cybersecurity strategy. This includes carrying out IoT security best practices such as updating and patching devices, using strong passwords and multi-factor authentication, taking inventory of all connected devices, and ensuring the correct access is enabled for each one. No single security tool can provide uniform and complete protection across all IoT devices. But, the best cyber security partners provide a blend of security measures across all endpoints and the cloud, allowing companies to be as secure as possible. Organizations need to develop a comprehensive cybersecurity strategy that protects against a wide range of cyberattacks across all devices at both the endpoint and network levels. The IoT security market has already grown significantly from £13.28 billion in 2021 to £15.63 billion in 2022 and this is only going to increase. Companies that stay vigilant with their IoT security are more likely to stay afloat in the upcoming years.

Hybrid cloud environments require a new security playbook – here's why

There's a huge range of security considerations for businesses to bear in mind as they implement a hybrid cloud infrastructure.

BY MASSIMO BANDINELLI, MARKETING MANAGER AT ARUBA ENTERPRISE

THE POPULARITY of hybrid cloud is exploding, with the global market for this technology set to rise to $145 billion by 2026. For businesses, hybrid cloud environments bring numerous benefits in terms of agility and scalability, as well as driving cost efficiencies. But when it comes to security, hybrid cloud requires a specific approach to keep on top of possible vulnerabilities, due to the flow of data from both public and private environments.

Not all IT decision-makers realise that protecting a hybrid cloud environment demands a different set of considerations than say, securing their public cloud solution. For instance, businesses going down the hybrid cloud route should pay special attention to protecting data in flight, ensuring supply chain security and even preventing physical security breaches.

Let's take a closer look at why addressing these security risks is particularly crucial in hybrid cloud environments.

Protecting data when it's in motion

Data is at its most vulnerable when in motion (being transported either within or between systems). It's at this point when businesses are most likely to suffer 'man-in-the-middle' attacks, ransomware and data theft.

If they're not configured correctly, hybrid cloud environments are particularly vulnerable to these threats. That's simply because data moves between different systems and environments more frequently in a hybrid set-up.

The answer? Encryption. Converting data into an unreadable format before it's either transferred or stored in the cloud is a no-brainer – especially for businesses handling sensitive personal or financial information. This way, even if bad actors manage to successfully access the data, it remains unintelligible.
It's also widely accepted that simply having encryption in place can make businesses a less attractive target for cyber criminals – as criminals know that they won't be able to use stolen data, even if they do manage to exploit a vulnerability.

Supply chain security

Hybrid cloud environments often include software applications from multiple vendors, working together in a complex, integrated ecosystem. This has created a lucrative opportunity for cybercriminals, who are targeting SaaS/IaaS/PaaS vendors with the aim of accessing their customers' networks. This is known as a 'supply chain attack'.

Think about it this way. Why would a criminal spend time trying to steal hotel keys from individual guests, when they could steal the cleaner's master key and gain access to hundreds of rooms? The same logic applies here. One successful vendor breach can offer a 'master key' to thousands of end-users.

Businesses implementing hybrid cloud infrastructure should be aware of supply chain attacks. In general, the best way to prevent these is to adopt a zero trust architecture – which works on a 'never trust, always verify' model. And to give all users the bare minimum level of system access required to do their job. As well as this, businesses can make use of strong authentication to better protect their systems from attacks and exploits.

Physical security

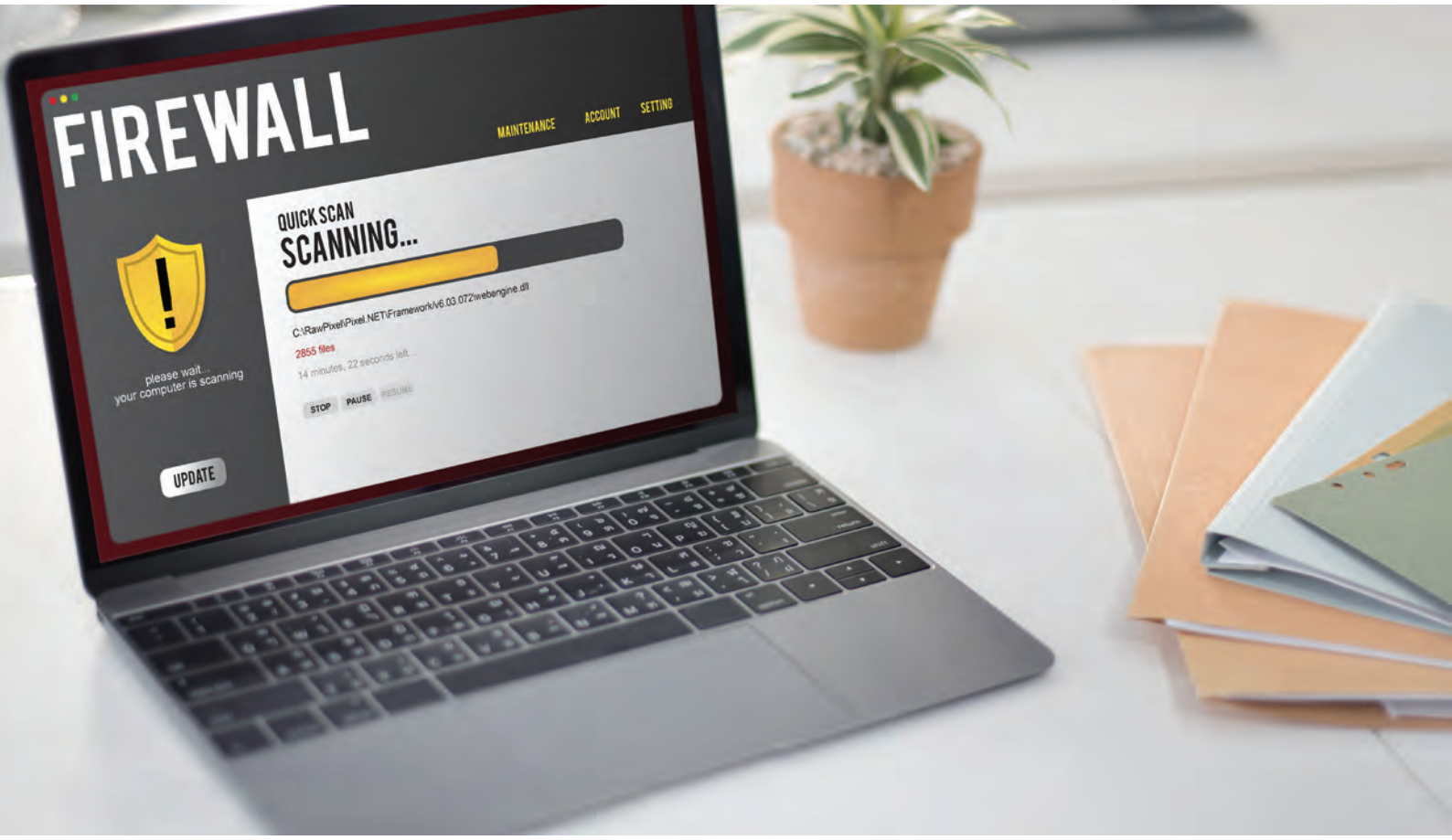
Hybrid clouds are made up of a patchwork of the following environments – public clouds, private clouds, on-premises data centres and edge locations. Businesses shouldn't forget that all these environments need to be physically, as well as virtually secured. The fact is that data breaches do occur outside of the digital sphere. The physical insertion of ransomware, which can lay can remain unnoticed until activated at a later stage, is a prime example of this.

Data centre providers tend to have robust security measures in place at their facilities – such as biometric authentication, CCTV, anti-intrusion sensors, and bollards. But this level of diligence doesn't extend to many on-premises facilities, which tend to be more vulnerable.

And so much more...

Of course, there's a huge range of security considerations for businesses to bear in mind as they implement a hybrid cloud infrastructure. Fundamentally though, with the right strategy in place - such as network segmentation, regularly run VAPT, and usage of EDR software - businesses should be aiming for a higher level of security than with their existing on-premises or public cloud infrastructure.

Looking forwards, we can expect to see the emergence of more managed service providers that specialise in helping businesses secure their hybrid cloud infrastructure. As a cloud provider, we're already seeing growing demand for this among our enterprise customers.



Choosing a firewall – top tips for businesses

All organisations are looking for ever more agile approaches to their security as they look to match it with the desired levels of agility they want from their business.

BY SIMON CROCKER, SENIOR DIRECTOR, SYSTEMS ENGINEERING, PALO ALTO NETWORKS

DIGITAL TRANSFORMATION, hybrid working, and market forces are all putting pressure on businesses and organisations to change and adapt. Next-generation firewalls (NGFW) are critical components for any network data security strategy, and a desire for greater agility here is no different. In achieving this, it is important to note that not all next-generation firewalls are created equal.

There are two high-level considerations to be made when deciding on a firewall strategy. Firstly, what is the determination that the solution can keep pace with the evolution of today's advanced attacks?

And secondly, how does the solution ensure business growth, agility and innovation are delivered? An essential balancing act needs to take place; here are the critical steps that need to be taken before you choose which next-generation firewall to go with.

Always Test Before You Buy and Size Correctly

Buying a next-generation firewall without doing your own research should never happen. The firewall needs to mould perfectly into your networking environment and the company's individual security requirements. When testing, ensure that the firewall is well equipped to face real traffic patterns and assess the end user application experience, whether this is on-premises or a SaaS application. Layering all tests is critical as this will mirror real-world requirements and challenges.

One common pitfall to look out for here is that in a lot of testing, testers review one feature at a time, which could result in choosing the wrong firewall; you need to look at everything running together to guarantee the right choice. Knowing this, do not rely only on datasheets and other "performance on paper" analyses, as there are substantial differences between firewall vendors. Some might consolidate threat prevention features (e.g. intrusion prevention systems [IPS], antivirus, command and control, URL filtering) in factors of performance impact. At the same time, another might showcase performance impact based solely on best-in-class IPS capabilities in isolated criteria.

It is critical that you make sure you are making the perfect match. In that case, you need to understand the capabilities of your company's environments' real-world requirements like IPS, application control, IPSec Decryption and advanced malware detection with your traffic analysis. Capacity planning is vital for sizing; therefore, time must be taken to properly test your requirements for the most intense issues that might arise.

Pay attention to the past whilst thinking about future business requirements

Usually, a firewall vendor collaborates directly with the networking team to gauge the requirements of the project. However, with the importance placed on an organisation's security efficacy, automation, agility and user application experience, it would be a mistake to just consider the needs of the networking team.

When assessing which firewall to choose, stakeholders should always be considered and involved across all business units. This includes application end users. You should also involve stakeholders in the beginning stages of the process for their differing views of the level of security and prevention needed. For example, data centre teams need automated features and capabilities, segmentation/microsegmentation of hybrid cloud environments, scalability to meet evolving needs, and single-pane management. By contrast, the application teams want simple, quick, and secure application development and deployment, whether the application is SaaS or in the data centre.

Accounting for Integration and Scalability

A new firewall should drive your IT Infrastructure performance without complex integration. There should be a simple process of pairing it with your current environment without making you replace systems. Assessing API integration, automation capabilities and cloud management should be the main focuses of the evaluation since these are vital for an organisation's approach.

Avoiding historically common mistakes, like vendor lock-in, will be beneficial. Choose a firewall vendor with a valuable community of technology partners to drive seamless integration with your environment from a security and networking stance. Remember, if you consolidate with one vendor, management issues and complexities can continue between security devices and individual networking, so making the right choice is crucial. Also, make it the vendor's responsibility to manage the integration efforts of a new security platform – you should not have to implement this yourself.

As your company changes and evolves, scalability must be front of mind. A vendor that utilises cloud architecture for design and innovation can scale more efficiently without the need to consistently update hardware on the network edge. This will benefit the organisation when understanding the journey to SASE or hybrid SaaS – boosting your protection in the long term.

When everything is in place for these tips to work, an organisation must trial a new firewall in a real-life environment. Proof of Concepts (PoCs) are priceless in avoiding the mistakes that occur when understanding a firewall offering. A PoC implements a forensic test of next-generation firewall performance in your real-world ecosystem. It also helps you assess how successfully a firewall can sustain performance and security to promote scale and agility for digital transformation.

Overall, the necessary steps to ensure a company implements the right firewall are clear. Shopping for protection takes time and care. The necessary testing is vital, plus understanding your vendor's history and prioritising scalability will take you closer to your perfect firewall strategy.

When assessing which firewall to choose, stakeholders should always be considered and involved across all business units. This includes application end users. You should also involve stakeholders in the beginning stages of the process for their differing views of the level of security and prevention needed

How education and technology can stop hackers stealing corporate credentials

Spending on corporate cybersecurity measures is on the rise as cyber-attacks wreak havoc on businesses. In the UK alone, cybercrime is costing the economy nearly £27 billion per year, while 83% have reported phishing attempts.

BY DAVE PREZZANO, UK & IRELAND MANAGING DIRECTOR AT HP INC.

WHY ARE ATTACKERS having success? An unholy trinity of static passwords, user error and phishing attacks continues to undermine efforts to secure data. Easy access to credentials gives threat actors a huge advantage. And user training alone cannot reset the balance – user education, and a robust approach to credential management is needed, with layers of protection to ensure credentials don't fall into the wrong hands.

Challenges with passwords

Nearly half of all reported breaches during the first half of this year involved stolen credentials. Once obtained, threat actors can exploit them to deploy malware, spread ransomware or move laterally through corporate networks by impersonating genuine users. Extortion, data theft, intelligence collection, and business email compromise (BEC) are some activities that attackers could facilitate, with potentially severe financial and reputational ramifications.

It's perhaps unsurprising to hear that the cybercrime underground is awash with stolen credentials. In fact, research reveals that 24 billion were in circulation in 2021, which is a 65% increase on 2020. So why is this? One reason is poor password management. If a password can't be guessed or cracked, logins can be phished individually from users, or stolen. The common practice of password reuse means these credential hauls can be fed into automated software to unlock additional accounts across the web, in credential stuffing attacks. Once in the hands of the hackers, they're quickly put to work. According to one study, cybercriminals accessed nearly a quarter (23%) of accounts immediately post-compromise—most likely via automated tools designed to rapidly validate the legitimacy of the stolen credential.

User education is not a solution

Phishing is becoming increasingly sophisticated and poses a severe threat to businesses. Some attempts look so genuine that even a seasoned practitioner would have problems detecting them, unlike the error-filled spam of the past. Corporate typefaces and logos are faithfully reproduced.

Domains may utilise typo-squatting to appear at first glance identical to the legitimate ones. They might even use internationalised domain names (IDNs) to mimic legitimate domains by substituting letters from the Roman alphabet with lookalikes from non-Latin alphabets. This allows scammers to register phishing domains that appear identical to the original.

The same is true for the phishing websites that fraudsters lead workers to. These pages are intended to come across as credible. The URLs frequently use the same strategies as those described above, like substituting letters. They also copy fonts and logos. These tactics mean phishing pages appear to be the “real deal”.

To deceive users, some login sites even display phoney URL bars that display a legitimate website address. This is why you can’t expect employees to know which sites are real, and which are trying to trick you into submitting corporate credentials.

As a result, user awareness programmes must be updated to account for evolving phishing tactics and those risks associated with hybrid working. A culture where reporting attempted scams is encouraged is crucial, as are brief, bite-sized training sessions with practical simulation exercises too.

Users should be urged not to click on links to pages from unknown or untrusted sources. They should instead log in directly to trusted websites. Additionally, employees should be taught to always check the URL bar to ensure they are on the site they think they should be on. Another key skill will be showing employees how to inspect URL links and interpret them, allowing them to potentially distinguish between a legitimate login page, and something posing as the real deal. This won’t work in all cases but could help in most.

The importance of real-time protection

But remember, there is no silver bullet and user education alone isn’t reliable to stop credential theft. Bad actors only need to get lucky once. Additionally, there are several ways for them to reach their victims including email, text, social media, and messaging apps. It’s unrealistic to expect every single user to recognise and report phishing attempts. Education must work with technology and robust processes.

Organisations should take a layered approach to credential management. The aim is to reduce the number of sites users have to put passwords into. Businesses should endeavour to implement

single sign-on (SSO) for all reputable necessary work applications and websites. If there are logins that require different credentials, then a password manager would be helpful in the interim. This also provides a way for employees to know if a login page they are on can be trusted or not as the password manager won’t offer credentials up for a site it does not recognise.

Organisations should also enable multi-factor authentication to secure logins. FIDO2 is also gaining adoption and will provide a more robust solution than traditional authenticator apps, which are still themselves better than codes sent via text messages.

But not all of this is fool proof, and phoney login pages could slip through the net. A last resort is needed to flag potentially risky login pages to employees. To deliver this, organisations can analyse threat intelligence in real-time, including metrics such as web page similarities, domain age and how users got there.

This provides a real-time analysis for a login page. This could be used to block high-risk login pages or provide warnings to users to check again for less-risky login pages. Crucially this technology, part of the HP Sure Click Secure Browser, only intervenes at the last minute, so security appears transparent and doesn’t result in them feeling watched.

When combined with an architectural approach to security, a layered approach to credential management can not only reduce the attack surface but mitigate risk from an entire class of phishing threats.

Should Browser Isolation be part of a Zero Trust solution?

Endpoints present a significant security risk that leave organisations vulnerable to cyber attacks. User devices therefore need to be front-and-centre of any Zero Trust architecture development and maintenance.

BY HENRY HARRISON, CO-FOUNDER AND CHIEF SCIENTIST AT GARRISON

THE MOVE to a Zero Trust model of cyber security is gaining momentum. Enterprises across sectors are recognising the shortcomings of existing security approaches, and are looking to Zero Trust as a way to create peace of mind against a backdrop of increasingly sophisticated and dangerous cyber attacks.

So what is Zero Trust? Essentially, this is a security approach that does away with the assumption that everything within an organisation's networks is trustworthy, and instead takes a 'never trust, always verify' standpoint. In short, the Zero Trust model trusts nothing and no one.

Cyber attacks increased by over a third (38%) in 2022 compared to the previous year, and the cost of cybercrime is expected to rocket from $8.44 trillion in 2022 to $23.84 trillion by 2027. If these numbers tell us anything, it's that the security tools relied on by private and public sector organisations alike simply aren't working.

The limitations of perimeter security

Traditional IT security has typically focused on defending an organisation's perimeters. This model tries to prevent bad actors from gaining access from outside of the corporate network, and then assumes that everyone inside the perimeter should be trusted by default.

These methods are not failsafe, and the rise in successful cyber attacks is proof. One reason is that these security tools are powerless to stop attacks

that use social engineering – for example, as with ransomware attacks, which manipulate employees to get past security measures and give malware a foothold in the organisation. In short – detection-focused security tools can be circumvented, and this leaves enterprises vulnerable to attack. What's more, most security strategies don't recognise this vulnerability, and therefore mistakenly allow bad actors full access to company data and systems once they are inside the organisational network

Zero Trust is different because it distrusts everything inside an organisation's network, as well as everything outside – meaning that if a threat actor is able to penetrate external security, they will not automatically be given access to sensitive data and documents.

Identity management alone is not enough

When talking about a Zero Trust architecture, it is important to understand that it is not made up of one solution; rather, as the name suggests, this is a holistic, all encompassing security environment. But when some companies think about Zero Trust, they may focus exclusively on one area – identity management. This is how users are authenticated before being given access. However, while this might seem to solve the security risk posed by threat actors breaching an organisation's perimeter, in reality, these only offer a partial solution.

Looking at online banking as an example, the shortcomings of identity verification tools such as biometrics and multi-factor authentication (MFA) are clear. Despite online banking users being both authorised and authenticated, it is still common for them to be the victim of a cyber attack. If user verification on its own was sufficient, this surely wouldn't be the case.

The vulnerability that's being exploited here is the user's device. This is crucial because if the endpoint is compromised – for example through an MFA bypass or a man-in-the-browser attack – the financial data is not only accessible to the verified user, but also the threat actors behind the attack. In a business setting, this has the potential to open up sensitive data, critical documents and core networks, and put them all in the hands of cyber criminals. Breaches of this nature not only put an organisation's ability to operate at risk, but can also irreparably damage its reputation.

The complexity of endpoint security

When considering endpoint security, it is important to recognise that context is key. In other words, it is the task in hand that determines whether or not an endpoint has adequate security in place – the same device may be considered to have adequate security to access one resource, but not to access another, more sensitive, resource.

The challenge of endpoint security is complicated by the growth of hybrid work, which has in turn led to the rise of the bring your own device (BYOD) trend – where employees use their personal computers and devices to access company networks. The security status of these personal devices means that IT teams are unable to implement universal security measures for those endpoints accessing company networks.

The problem of endpoint security is amplified further by the continued move of business applications and data storage into the cloud. Many cloud providers focus exclusively on user identity verification and do not offer endpoint security support, which as we've already seen, does not adequately address the security gap.

The cloud providers that do consider the issue of endpoint security tackle the problem by making access conditional on the source IP address. But this simply doesn't work for companies whose workers have adopted hybrid working patterns.

Browser Isolation – the move to Zero Trust

Growing numbers of enterprises are turning to Browser Isolation as a Zero Trust solution that enables uniform endpoint security, regardless of where an employee is located, or the security status of the device they are using. What's more, it does this without having to resort to limiting users' access to the internet.

So how does it work? Browser Isolation creates a barrier between the endpoint and the internet, meaning that the employee's machine – be it a personal device or company property – never comes into contact with the internet. This therefore removes the risk of users coming into contact with web-based malware. It does this through a process known as 'Pixel Pushing' – which converts the browsed web content into a video representation of the web. While the online experience remains the same for the user, in reality, they are seeing an interactive video rather than the web page itself.

This important difference completely removes the possibility of all web-based malware attacks Zero Trust is the core principle underpinning Browser Isolation – the technique assumes that all internet content is untrustworthy, and in doing so provides strong endpoint security.

A holistic approach to Zero Trust

There is no silver bullet when it comes to Zero Trust. Instead, companies need to take a holistic approach that is led by the need to protect and secure critical data and networks, while also giving employees the freedom and mobility they require.

Endpoints present a significant security risk that leave organisations vulnerable to cyber attacks. User devices therefore need to be front-and-centre of any Zero Trust architecture development and maintenance.

Learning and Development:
What employees want versus what employers need

With the skills crisis - particularly in tech - stubbornly refusing to go away, the smartest companies are looking to plug the gaps by upskilling or reskilling their existing people, or growing their own talent.

BY ANDREW BARDSLEY, HEAD OF LEARNING & DEVELOPMENT AT XDESIGN

AT THE SAME TIME, employees are increasingly looking for much more than just a job; they want exciting work and the chance to grow and improve their skills and career.

A recent survey by Docebo found more than 8 in 10 people (83%) saw learning and development (L&D) as a vital factor in their choice of employer.

Certainly, whenever I am involved in interviews, arguably the most frequently asked question I hear from candidates is 'what opportunities are there to develop myself at your company?'

And while Millennials and Gen Z undoubtedly view work a little differently from older generations, I am noticing staff of all ages taking greater interest in their own professional development. It's a marked shift in attitude, rather than a genuine generational difference. Addressing L&D from both a skills gap and staff development point of view requires businesses to invest in solid planning. But huge care

needs to be taken to balance what your business needs its employees to know with what your people want to learn.

Balancing wants and needs

A top priority must be getting your senior management team on board and engaged with your L&D plan, so behaviour is modelled from the very top. If you succeed with this, a genuine thirst for learning will filter down through the organisation, creating an engaged workforce who want to develop their careers.

The topics people want to learn about can be hugely varied - but I am seeing a growing trend of employees wanting much more from their learning than just tuning into a webinar or sitting in a classroom watching someone present a PowerPoint.

It's time to think wider than these traditional ways of learning. So ask yourself three overarching questions – is formal training what we really need?; what changes do we want to see?; and are there other ways to achieve all that?

Everyone has different preferences and styles when it comes to how they learn. Peer-to-peer learning, either through mentoring or shadowing a colleague, remains a favourite, but I am seeing more requests than ever for advice on how best to give and receive feedback, especially from managers.

So much more training is done online these days, allowing people to learn at their own pace, from wherever they happen to be.

This has its place - but there's still great value in getting people into the same room for a brainstorm, working on a group project together, or attending a conference in person to hear from industry experts. The key is to provide a variety of different opportunities.

'Mandatory training' that employers need their people to complete for compliance reasons - such as security awareness – has often tended to strike fear into employees.

We always recommend L&D teams look at this through the eyes of their learners and make this type of training a more engaging experience. If mandatory training is uninspiring and boring, you risk tarnishing the reputation of all the L&D on offer, and turning your people off learning altogether.

So, ditch that dull e-learning module. If you can keep the 'need to learn' experience enjoyable and positive, it will encourage more people to sign up for non-mandatory learning.

Sometimes there is also the need for 'regular training' - management development, for example – to ensure consistency in knowledge across a group of staff. This can feel repetitive for those people who have already completed it, so finding a good balance here is key too.

We build a lot of our own L&D content internally, which allows us control over it; but we also offer everyone their own dedicated personal learning budgets, to spend how they choose with external training providers

We build a lot of our own L&D content internally, which allows us control over it; but we also offer everyone their own dedicated personal learning budgets, to spend how they choose with external training providers. This flexibility is very popular.

Growing your own talent to plug the gap

Growing your own talent, through graduate programmes or internships, also has significant business advantages. When you bring someone into your company at entry level, and you then find a position that is right for them once they complete their programme, the chances are they are already fully engaged with your business and culture, and committed and motivated to continue learning.

You can always train good people on the specific skills they need for their role, but a desire to learn is something you can't teach.

It might not be realistic to fill every single vacancy this way, but I firmly believe it should be an important part of every corporate toolkit.

Nearly half of our own 'emerging careers' intake has come to us through a 'boot camp' or other fast-track training programme, which have become some of the most popular routes into the tech sector, especially for career-changers.

I can't praise these programmes enough. These young people might not be coming to us with all the technical skills they need, but their attitude to learning means they pick them up in no time.

L&D comes in many forms. But only by listening to and understanding your people, can something be built that really works both for them and your business.

And above all, resist the temptation to do what you've always done before.

By approaching everything with a high-quality learning experience in mind, you'll soon have an L&D plan that gets your people and your senior management equally enthused.

Can AIOps plug the storage skills gap?

Ultimately, AI is facilitating a new, 'set-it-and-forget-it' era for enterprise storage management, reducing complexity, standardising processes across applications and service levels and reducing the burden of resourcing with skills that are in very short supply.

BY ERIC HERZOG, CMO, INFINIDAT

REGARDLESS of economic uncertainty, businesses everywhere are pushing forwards with plans for Industry 4.0 and key technology investments. They can't afford to do otherwise if they want to remain competitive. Yet, the potential to deliver on promises of advanced connectivity, AI, automation, machine learning and real-time data availability, is at risk - because of the ongoing shortage of IT professionals. It's a feature common to every sector within enterprise IT, including storage.

80% of IT leaders report that skills gaps pose a 'high or medium risk to their team's ability to meet key objectives', according to the Skillsoft 2022 IT Skills & Salary Report. Where the requisite skills are available, workers are commanding premium rates and salary inflation is running at an all-time high. Some companies admit paying up to 40% more for the right candidates.

Against this macro backdrop IT budgets are being squeezed due to inflation, the threat of cyber-attacks and international compliance requirements. This makes infrastructure provision, like enterprise storage, ever more challenging to resource. Now a possible solution exists, thanks to ready availability of advanced AIOps capabilities at the storage layer in sectors where the right skills cannot easily be found, AI provides a route to 'getting things done' and solving the problem of talent scarcity, without compromises. Rather than removing jobs, AIOps technology brings continuity for enterprises who cannot recruit into key roles. It's a win-win, delivering many other advantages to enterprises and the start of a new 'set-it-and-forget-it' era for enterprise storage. Given all the economic uncertainty, its timing couldn't be better.

AIOps at the storage layer simplifies management
Modern data centre environments are now highly complex, featuring multiple architectures and technology stacks, often with siloed applications. The storage layer lies at the heart of addressing many of the challenges created by this complexity. By using an artificially intelligent solution at the storage layer, organisations can exploit built-in infrastructure intelligence, facilitate easier service level delivery, and improve the efficiency of data centre operations, without worrying about how the technology itself operates.

Used at the storage layer, artificial intelligence (AI) can also optimise performance by optimising the cache, creating a better understanding of workloads and behaviours, and delivering memory-speed access to data. Deep machine learning capabilities

deliver enhanced cache utilisation, with the ability to accurately predict which workloads will be required so that they can be brought into the cache more quickly. These performance improvements are possible because the algorithms learn to prefetch any data likely to be required based on previous transactions and then retain it in memory on request. This machine-based learning also means the speeds of reading and writing, sequentialisation of inputs and outputs (I/Os) based on behaviour and understanding block sizes in relation to each other and to applications, are all enhanced.

In addition to higher performance, using AIOps at the storage layer also supports greater consolidation of applications based on data utilisation, with multiple nodes that deliver enhanced redundancy. The system effectively keeps on learning and its capabilities continuously improve as the algorithm continues to be used.

AIOps benefits extend beyond storage layer
AI offers many benefits outside of the main storage layer too, through cloud-based applications to deliver a multi-system, detailed and granular view of and across workloads, platforms and data centres. This is particularly useful where resourcing challenges make it difficult to recruit the right calibre storage professionals. AI based support means management workloads are halved because a singular, consolidated dashboard can be created to cover the entire storage architecture. Other benefits include early issue detection and prevention, alerting and system management.

Delivered through an open, cloud-based architecture, these solutions can be customised to fit various workflows, while predictive analytics can deliver trend analysis and reporting, anomaly detection and enhanced resource planning. This enables automated, actionable insights on areas such as performance and capacity, which can ultimately lead to better business decisions through integration with ServiceNow, VMware vCenter Ops and other pan-data centre/cloud AIOps packages.

Combining storage insights with DevOps capabilities
An intelligent storage solution delivers a lot more than high performance, improved storage utilisation and actionable insights to an enterprise. It is also possible to integrate development operations capabilities and at the same time, ensure that storage layers are in tune with the needs of system administrators. This gives direct access to broad and deep capabilities through proven solutions including cyber resilience, seamless migration, automatic file system extension, infrastructure as code and Storage-as-a-Service (STaaS) automation. In turn, solution deployment can be expedited while eliminating solution development risks, as well as improving integration capability with other third-party functionality, such as Ansible and other pan-data centre/cloud DevOps packages.

Intelligent storage underpins performance transformation

At a time when storage resources are so challenged – both in terms of talent availability and high salary costs, implementing an intelligent storage architecture can help organisations minimise the consequences, without compromising performance. Integrating AIOps into the storage layer means the infrastructure can become self-managing and self-optimised, with 100% uptime. Direct access to DevOps capabilities ensures that functionality can be extended with simplified solution implementation, expedited solution delivery and reduced solution risk.

'Set-it-and-forget-it' era for enterprise storage
Ultimately, AI is facilitating a new, 'set-it-and-forget-it' era for enterprise storage management, reducing complexity, standardising processes across applications and service levels and reducing the burden of resourcing with skills that are in very short supply. Instead, with an AI powered storage infrastructure, less time and fewer people are needed to manage an increasingly advanced and powerful architecture, one that supports consolidation, breaks down siloes, supports diverse workloads and delivers an all-round improved return on assets employed.

The Rising Star Programme

By Steve Hone DCA CEO

THE RISING STAR PROGRAMME is an initiative to support those in their early careers within the data centre industry. When recently polled, 85% of data centre professionals commented that their workplace would be the perfect environment for young, fresh talent, but that there were a number of barriers to entry including employer brand, attraction strategies and retention of trained talent.

Things are changing, these issues can be addressed - The Rising Star Programme help can help to do this!
The programme has been devised by Adelle Desouza of HireHigher and as the Data Centre Trade Association The DCA is proud to offer its support.

As the founder of The Rising Star Programme, Adelle has already hosted a number of panels at industry events, initially focusing on the need for an industry initiative of this kind and she has been gaining much support for the idea. The Rising Star Programme was launched a year ago and it is now building momentum. The Global Strategies: People Environment and Innovation Theatre at Data Centre World 2023 enabled Adelle to host a specialist Rising Star panel which allowed the audience to hear the opinions of several young and talented people who now work in our sector. Adelle also masterminded a ground-breaking event in West London for over 60 year 12 students from two local schools on International Data Centre Day. The students were encouraged to recognise what they as individuals could bring to a work environment, they heard from a group of Rising Stars – on their route into the data centre sector and they also had a tour of a 'real live' data centre!

> "The Rising Star programme is an opportunity for young people to not only connect with other like minded individuals at a similar stage in their career but to form a force to be reckoned with as we propel our industry forward."
>
> Steve Hone, CEO, Datacentre Alliance

These activities have been very well received and the programme is gaining traction – I believe the industry is ready to step up and The DCA will continue to support and encourage this venture.

Find out more about The Rising Star Programme here.
The Rising Star Programme – #StartTheRevolution

Time is not on our side, but we have made progress - are you a walker or a talker?

By Adelle Desouza, Founder of HireHigher and Advisory Board Member, DCA

A year ago, in a previous update article I shared the findings of two interactive workshops at The DCA's annual Data Centre Transformation Conference (DCT 2022). The findings focused on the barriers to entry for new and diverse talent to the Data Centre Sector. In last year's article I concluded that change was coming and in a big way, and so I return to share the progress we have made and what we are yet to overcome...

It is safe to say the talent topic has exploded - primarily on our social media feeds. Whilst the threat is far from neutralised progress has been made. As of October 2022, The DCA formally partnered with HireHigher to present The Rising Star Programme. A dedicated project designed to work a number of initiatives, closely aligned to the very barriers raised at DCT 2022 to future proof our industry.

The Rising Star Programme functions purely as a result of the industry pledging support to the cause. To date, a mere four months at the time of writing, we have enabled a nationwide PR campaign to begin to address the negative brand image of our industry that is perpetuated by the media.

We have created a dedicated community of Rising Stars – these are individuals in their early career. By creating a centralised group on LinkedIN, they are enabled to connect and network. We provide opportunities to build their professional and personal brands, through speaking and writing engagements both to the industry and to students. The programme has also curated the industry's first award category devoted to those in their early career with our industry. This will showcase the value and impact the next generation is already offering the industry.

Finally, we have begun to bridge the gap between our experienced experts, rising stars and current students through the #RisingStarsInSchools

campaign on International Datacentre Day. This event was no small feat. It all came together thanks to working with organisations who 'talk the talk' and 'walk the walk'. Over sixty 6th form students attended a morning of workshops designed to highlight their natural tendencies and personalities and allowed them to understand how best to take these into the workplace. The students also heard from current Rising Stars and heard how they had discovered the Data Centre Sector and secured apprenticeships or jobs after graduation. The day culminated in all students being able to visit a local data centre.

The feedback has been immensely positive, the energy on the day second-to-none and on top of all of that we were able to inspire students to consider a career in our industry. There is no denying the issue the industry faces is one of our own making, and whilst many comment and 'like' the premise of change, bureaucratic inertia still plagues many. From insights from successful early careers programmes from within the IT industry to sharing the stage with current Rising Stars who addressed the barriers to entry within our recruitment processes there is something preventing seismic change in our industry. I can and have commented over the years on why I believe this may still exist, however ultimately we must remain focused and energised by those organisations who have pledged their support to The Rising Star Programme they have clearly identified themselves as walkers and not just talkers.
In just a few weeks, we will again take to the stage at Datacentre Transformation, hosted by The Data Centre Alliance, but this time the rising stars will take the spotlight. Following a successful panel at Data Centre World which looked to address the barriers to entry from the perspective of those new to our industry we intend to hold an interactive session surrounding retention.

A topic that was raised by experienced experts last year as a concern for them to introduce new and diverse talent. So, what better than to hear from the target audience themselves. We hope to discover and share views on the relevance of the great resignation, the impact of hybrid working and the role of benefit packages - in a candid and open way.

The Data Centre Transformation Conference will once again drive change and action in our industry, and we look forward to seeing what the day brings - and no doubt will share with the readers of Digitalisation World. To find out more about the programme and how you can join the revolution I'd love to connect.

Developing a sustainable workforce for the digital infrastructure industry

The need for a sustainable workforce for the digital infrastructure industry has never been greater. Predictions for the future, such as an anticipated 75 billion connected devices by 2025, are so astronomical they're beyond rational understanding. What is widely understood, however, is the immediate need to recruit, train and retain talent in order to meet this huge demand.

A SKILLS SHORTAGE of this scale requires equally ambitious solutions that may only be achieved by collaborative and positive actions. By joining forces, there is the capacity to implement meaningful and effective solutions at every potential opportunity; the good news is there are plenty of opportunities to exploit.

Growing the opportunities for young people to develop their skills and improving access to a quality education are paramount in addressing the skills gap throughout the digital infrastructure industry from the ground up. In order to effect the best improvements, it's vital we create more chances at the beginning of a young person's career pipeline so they can learn about and develop an interest in the industry.

Now is the ideal time to shout about the opportunities that the data centre sector provides while graduates experienced in STEM subjects are in such high demand. Collaboration as an industry is required to make sure that we are shouting loud enough to be heard. Alongside this, general awareness that the industry actually exists is a good starting point, as well as its extensive career opportunities – both of which need to be elevated so that people in positions of influence, such as parents, teachers and career advisers, are initiating discussions about it with young people who are at the point of choosing a career path. Clearly laid out routes through education, that equip young people with the skills and qualifications they need to forge a successful and satisfying career in the industry, need to be established to ensure that talent is able to confidently flow in our direction.

The introduction of T Levels (Technical Levels) in September 2020 positioned them as the main technical education qualification option at age 16, alongside A Levels and Apprenticeships. Widely supported by employers, T Levels are starting to gain good traction and are a definite step in the right direction towards providing more opportunities for young people to choose technical subjects.

Initiatives such as University Technical College (UTC) Heathrow and Partners and the Digital Futures Programme, where students undertake a level 3 engineering curriculum alongside projects and workshops led by industry partners, are forging essential inroads into creating these opportunities. Such initiatives provide young people with the vital skills required to secure a career in the industry along with helping them to make connections with real-life employers, who are actively looking to recruit new talent.

Another key aspect of the UTC initiative is tailoring the opportunities to local employer demand. There are hotspots throughout the UK where STEM jobs are crucial to the local economy and therefore targeted solutions presented at a local level, such as a UTC, can prove individually more effective than

broad national schemes. The good news is that more industry focused UTCs are planned to open in the near future.

Apprenticeship schemes are also proving to be an effective way of nurturing new talent across the board and they're particularly well-suited to the digital infrastructure industry due to their hands-on nature and practical learning opportunities. According to Department for Education apprenticeship data, engineering-related apprenticeship starts increased by 25.8% in 2020/21, a greater rate than all sector subject areas which in comparison showed an 8.6% increase.

The tide seems to be turning, where companies who previously shied away from longer-term apprenticeship schemes in favour of employing ready-skilled employees, have now recognised that there are no quick fixes, and time needs to be invested in order to progress. The first Government funded Apprenticeship for Network Cable Installation is now available; the Network Cable Installer (NCI®) Apprenticeship is a 12-15 month program Level 3 program that is creating the next generation of competent, confident, and qualified network cable installation professionals.

When a skills shortage exists in any industry, the demand for talented, experienced individuals rises and so too do the corresponding salaries, benefits and temptations to jump ship – to another company or sometimes even another sector. Individually, organisations can make some really positive steps towards retaining the talent that already exists within their ranks. Investing in training and ongoing professional development is essential to ensure each and every employee possesses the right skills to succeed.

A company that considers each person's skill set and puts a plan in place to help progress it will engage employees far more successfully, increasing staff morale, improving job satisfaction, all of which ultimately help to mitigate mission critical risk. Companies that are also able to establish productive educational partnerships and promote them to existing and prospective employees can yield higher team retention results, not to mention the increased competitive advantage essential in a competitive marketplace.

Alongside this focus on upskilling, other measures can be employed at a company level. When putting together a job advert, there is a temptation to specify a degree level of education, that may not actually be a necessity. When we home in on the actual required skills, knowledge and behaviours of the type of person we are looking for - and then team this with an individual professional development plan - we can open up an entire pool of people who previously may not have made the cut.

Allowing for flexibility in your workforce also helps keep experienced employees engaged. People's attitudes to work have changed, largely due to the pandemic which provided the opportunity for people to review their priorities and rethink what they want from a job. Relaxing the attitude that employees must be full-time to be effective ensures that those who can provide vital industry skills and experience on a part-time basis remain valued.

Crafting a culture that encourages people to join and remain within a company is a company-wide responsibility, however crafting a culture that encourages people to join and remain within the industry lies on the shoulder of us all. Our ability to sustain our industry to meet the world's increasing demand for digital services relies on our capability as an industry to pull together, not just at company or even country level but in an industry-wide, international effort.

I would like to see more collaborations of industry partners, working together towards the combined goal of identifying and trialling new initiatives to help close the skills gap. Initiatives such as UTC Heathrow and Partners, that provides proof of concept of the industry working together with the common goal of spreading awareness of the industry, educating and nurturing potential young talent, leading to new entrants to our industry are a must. Plus, these proven initiatives can often be duplicated in numerous locations creating scale and multiplying the efforts to really tackle the talent shortage.

These types of collaborations are the key to unlocking the future talent pipeline that the digital infrastructure industry requires in order to develop a sustainable workforce and provide the skills to meet demand, now and for the future.

Iulian Trifan - Hybrid Cloud Engineer (DTS) Apprentice at JP Morgan

I DECIDED that an apprenticeship was right for me when I found out what it is - studying while working and putting your study into practice to solve real-world problems - this motivated me to keep applying until I received an offer.

Applying to apprenticeships isn't an easy task, I started off by searching mainly on the government apprenticeships website, general Google searches and LinkedIn. What stood out to me is the importance of communication and transparency from employers during the application process given that I didn't receive a response from about 30% of applications I made. From the responses I did receive, I found it most useful when I was given a rough timeline of when the next steps are happening and when to expect further communications. Staying on top of communications with candidates I think is one of the best improvements an employer can make to their application process.

The myth I'd like to bust is that "Apprentices don't do 'real' jobs ". This is certainly not the case; I consistently have the opportunity to contribute to any piece of work my team is set out to do. I am treated exactly like any other employee, not as the coffee maker of the team. This makes for a great experience as I feel valued and listened to by the people I work with every day.

Two things I would tell my younger self, if I could, would be to apply to level 5 as well as level 6 apprenticeships and to seek more opportunities to talk to current apprentices. Apprenticeships are getting very competitive, so applying to more would've given me a higher chance of securing an offer to even keep it as a backup. If you've decided apprenticeships are for you, this will help you because once you're in the company, it's very likely that you'll be offered a place afterwards. I also wish that I'd spoken with more apprentices while I was applying, to get a better idea of what it is like. It would've helped motivate me in applying to more, but it would've also helped me understand what to expect once I did start. Another improvement employers can make, is to include apprentices in their recruitment process, to give candidates a chance to ask them questions as well as the hiring managers.

In retrospect, getting an apprenticeship was the biggest and best decision I made to start my professional career, and this is why I'm getting involved in helping the next generation. I'm hoping that by sharing what being an apprentice means students make a more informed decision regarding their future. Also, by sharing the best tips I learned while applying myself, I hope students feel better prepared in submitting their next application.

Laura Allwood – Junior Project Manager, Arcadis

Q. *Share one reality that working and studying for your degree apprenticeship you think would surprise others in our industry?*

A. As a degree apprentice you are able to take on responsibility within the projects you work on as you learn so fast. There shouldn't be a stigma around apprenticeships and business are really beginning to understand the benefits of apprentices. You can quite quickly become a very valuable asset on large scale data centre projects even if you don't have a lot of experience. This responsibility gained through work combined with studying for your degree can be stressful at times especially when university assignments are due and work deadlines are approaching. Although once completed it can be a very rewarding feeling.

Q. *Name one thing you have noticed in the industry that has surprised you?*

A. The one thing that has surprised me about the industry is the lack of awareness for the industry. For something that is used by so many people so regularly it shocks me how many people don't know it exists. I am guilty of this myself, until I was allocated to work on a data centre construction project I had no idea what one was. Working on these projects allowed me to realise the importance of the industry.

Q. *Fast forward a few years, you are now senior management within the datacentre industry, what is one thing you want future Laura to hold on from current Laura when it comes to new/diverse talent?*

A. I want future Laura to make the industry welcoming and encourage new talent to attend conferences and events. Also, to ensure that they have time to participate in more technical training. New talent can hold a lot of value if you give them the time to learn and develop. I want to be able to continue with this mindset in mind to help inspire that new generation. Another point is to remember how I was treated when I first joined and understand that it might take a while for someone new to learn but that is ok, but once integrated into this new talent will be able to provide us with new ideas.

APC

Just say where you want it...

We'll take care of the rest.

EcoStruxure™ Micro data centres from Schneider Electric™ bring together power, cooling, physical security, and management software and services into pre-packaged rack solutions that can be deployed globally in any environment.

- Allows for rapid IT deployment wherever and whenever it is needed in weeks, not months.
- Reduce service visits and downtime.
- Securely manage system from anywhere.

Explore EcoStruxure™ Micro Data Centre from Schneider Electric

apc.com/uk

Life Is On Schneider Electric