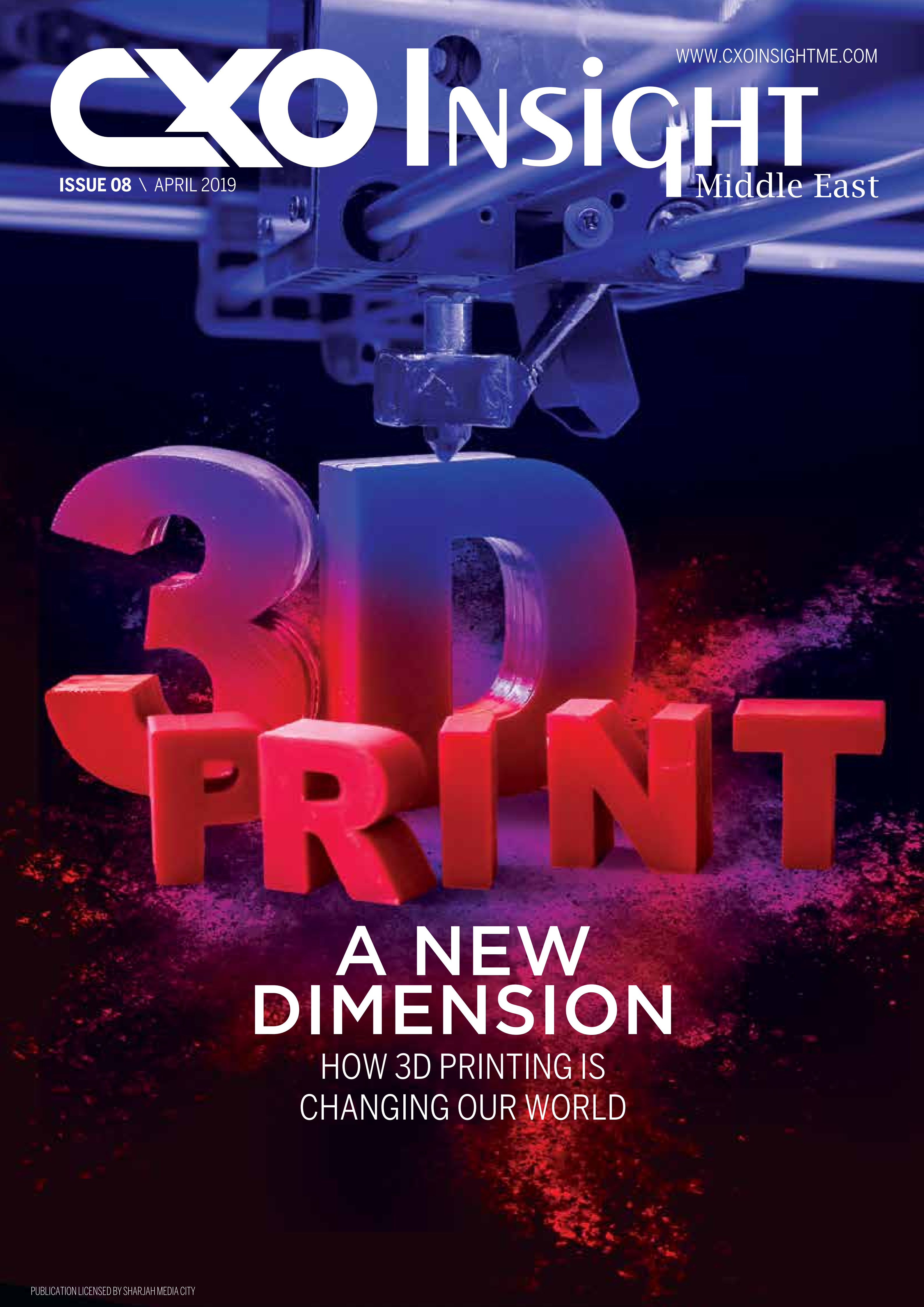
WWW.CXOINSIGHTME.COM

CXO Insight Middle East

ISSUE 08 \ APRIL 2019

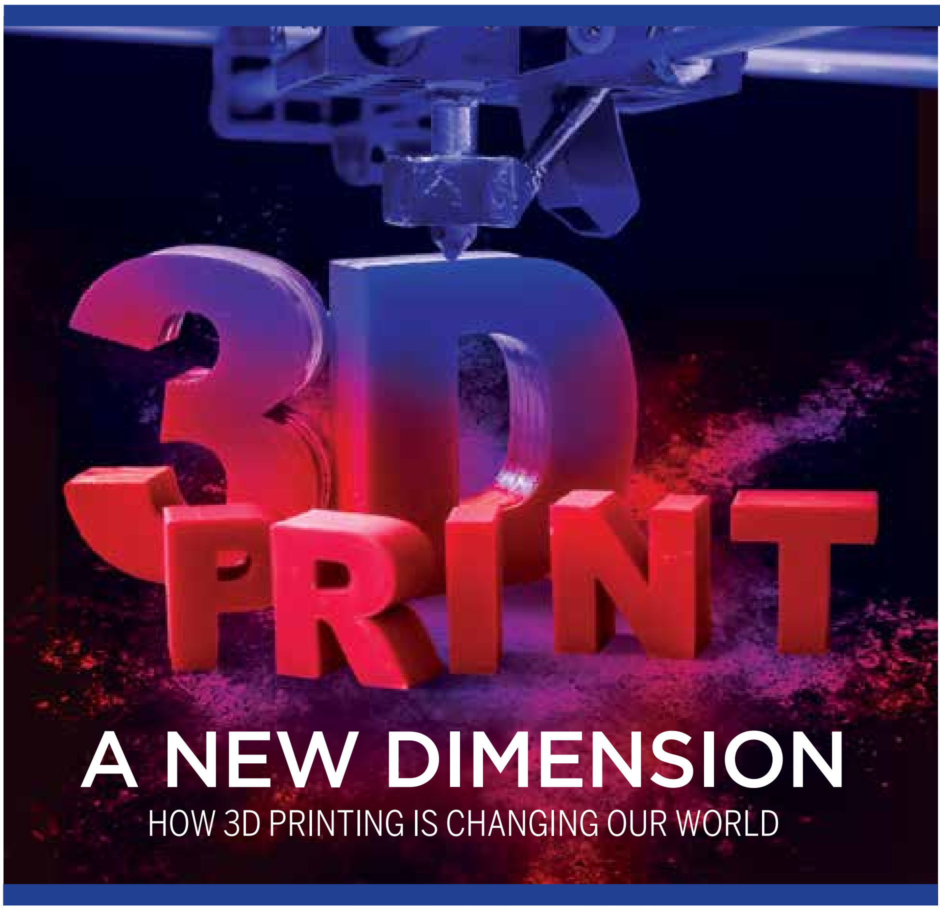


A NEW DIMENSION

HOW 3D PRINTING IS CHANGING OUR WORLD

PUBLICATION LICENSED BY SHARJAH MEDIA CITY

observe it
USER RISK DASHBOARD
INSIDER THREAT INTELLIGENCE
MANAGEMENT CONSOLE
USER ACTIVITY PROFILE
USER BEHAVIOR CHANGE
WEEKLY CHANGE
TOP RISK APPLICATIONS
TOP RISK ALERTS
5 RISKY USERS
0 NEW USERS AT RISK
RISKY USERS (5)
Alice Brenkov
85
Investigate
Brian Cameron
79
Investigate
John W Mac
53
Investigate



A NEW DIMENSION

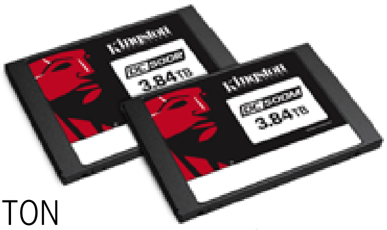
HOW 3D PRINTING IS CHANGING OUR WORLD

VIEWPOINT

INTERVIEW

REPORT

49 PRODUCTS



KINGSTON ENTERPRISE SSD

CANON ZOEMINI

XIAOMI MI9

6 NEWS

Epicor ERP Positioned as a Visionary in Gartner 2018 Magic Quadrant for Cloud ERP for Product-Centric Midsize Enterprises

Gartner

Licensed for Distribution

Magic Quadrant for Cloud ERP for Product-Centric Midsize Enterprises

Strategic Planning Assumptions

Market Definition/Description

EPICOR

TRUST ISSUES

We are gearing up for this year's edition of GISEC, where security vendors of various hues and colours will exhibit their wares. This year, the show boasts of some world-famous hackers such as Kevin Mitnick and Jamie Woodruff as speakers. And for the first time, GISEC also features an open forum to delve deep into the dark web and will host live hacks for visitors.

I have been a regular visitor to the show as it has always been a useful platform to find out more about the new trends in cybersecurity and meet some of the brilliant minds from the industry. Besides collecting good content, my mission this year is to talk to cybersecurity professionals and try to get to the bottom of the newest buzzword in the industry – Zero Trust. Over the years, we have witnessed various security models being advocated by vendors including 'defence in depth' and 'layered defence' as a panacea for breaches. So, what exactly is Zero Trust? The idea behind the concept is rather simple – don't trust anyone. The basic tenet of this model is that companies shouldn't allow automatic access to users or machines without proper authentication and authorisation, no matter whether they are inside or outside. It is touted as a new way of thinking about security but is something easier than done if you read the fine print. To achieve Zero Trust, organisations will have to leverage a myriad of technologies including encryption, multi-factor authentication, orchestration, IAM, to name a few. A piecemeal approach to security has been the bane for many organisations and the onus is now on vendors to make sure that their technologies integrate with others in the security stack. For many years, security vendors have been resorting to selling FUD, and it's time for them to listen more closely to CISOs and help them with meaningful metrics to gauge the efficacy of the security posture of their organisations.

Published by

INSIGHT
Media & Publishing LLC

Publication licensed by
Sharjah Media City
@Copyright 2019 Insight
Media and Publishing

Managing Editor
Jeevan Thankappan
jeevant@insightmediame.com
+97156 - 4156425

Sales Director
Merle Carrasco
merlec@insightmediame.com
+97155 - 1181730

Operations Director
Rajeesh Nair
rajeeshm@insightmediame.com
+97155 - 9383094

Production Head
James Tharian
jamest@insightmediame.com
+97156 - 4945966

Administration Manager
Fahida Afaf Bangod
fahidaa@insightmediame.com
+97156 - 5741456

While the publisher has made all efforts to ensure the accuracy of information in this magazine, they will not be held responsible for any errors

AVAYA TO SET UP CUSTOMER EXPERIENCE CENTRE IN DUBAI

Recognising Dubai as the epicenter for innovation in region, Avaya has announced that it will be building on its long-standing relationship with the Dubai World Trade Centre (DWTC) by opening a Customer Experience Center (CEC) at One Central, a new international Grade-A mixed-use development in the heart of the city.

Showcasing the latest advancements in artificial intelligence (AI), biometrics, and blockchain-enabled communications and collaboration solutions, the center will serve as a test-bed for Avaya's partners and customers, from across the globe, looking to develop world-class solutions to address the most pressing business needs and challenges.

His Excellency Helal Saeed Almarri, Director General, Dubai World Trade Centre Authority (DWTCA) and Dubai Department of Tourism and Commerce Marketing (DTCM), said, "DWTC Authority is delighted to welcome Avaya to the One Central development. Avaya is a long-standing partner of DWTC and we have first-hand experience of their commitment to technological excellence. This innovative customer experience center is a solid new addition to the One Central ecosystem and reaffirms both, the development and Dubai's attractiveness as a dynamic urban destination of choice for businesses to accelerate their growth trajectory and expand their geographic reach."

Nidal Abou-Ltaif, President, Avaya International, said: "Today, it is our customers who are eager to leverage cutting-edge technologies and drive the evolution of communications and collaboration. We recognise this and as a customer-centric organization, we are facilitating this 'outside-in' approach to innovation that empowers our customers. This has meant not only placing our R&D centres closer to our customers than ever before, but actively involving them in the process of ideating and designing the solutions that will help shape the intelligent customer and experiences of tomorrow."

SAS TO INVEST $1 BILLION IN ARTIFICIAL INTELLIGENCE

SAS is investing $1 billion in AI over the next three years through software innovation, education, expert services and more. The commitment builds on SAS' already strong foundation in AI which includes advanced analytics, machine learning, deep learning, natural language processing (NLP) and computer vision. Educational programs and expert services will equip business leaders and data scientists for the future of AI, with the technology, skills and support they need to transform their organisations.

"At SAS, we remain dedicated to our customers and their success, and this investment is another example of that commitment," said SAS CEO Jim Goodnight. "With our innovative capabilities in AI, SAS helps businesses deter damaging fraud, fight deadly disease, better manage risk, provide exemplary service to customers and citizens, and much more."

The $1 billion investment in AI will focus on three main areas: Research and Development (R&D) innovation where SAS continues to build on the success of its global AI efforts; education initiatives addressing customer needs to better understand and benefit from AI; and expert services to optimise customer return on AI projects.

SAS is investing in R&D innovation in all core areas of AI, with a special focus on making it easy for users with different skill levels to benefit – from business experts to data engineers to data scientists. SAS is embedding AI capabilities into the SAS Platform and solutions for data management, customer intelligence, fraud & security intelligence and risk management, as well as applications for industries including financial services, government, health care, manufacturing and retail.

ANKABUT PICKS VMWARE FOR TRANSFORMING THE EDUCATION SECTOR

VMware has announced a digital transformation partnership with Ankabut, the United Arab Emirates' Advanced National Research and Education Network (NREN), to transform learning experiences for academic institutions in the UAE, regionally, and worldwide.

Ankabut's platform provides collaboration opportunities between UAE education, government, and industry sectors. Aligned with Abu Dhabi Vision 2030 and UAE Vision 2021 government transformation goals, Ankabut provides cloud connectivity, IT infrastructure and managed services for 80 UAE member institutions to drive innovative educational services such as digital student records, project collaboration and virtual reality field trips.

Ankabut also becomes a member of the VMware Cloud Provider Program, becoming the first dedicated education service provider in the UAE. Using VMware software-defined data center and VMware NSX network virtualization solutions, Ankabut can provide more secure data center and public cloud services that can quickly, easily, and affordable scale up as their student population grows.

"We needed to build a digital foundation to support our vision of becoming the region's leading education service provider, while allowing academic institutions to reduce capital and operating costs. To help accelerate digital transformation within the education sector, this required advanced automation, a standard for sharing services and the adoption of a cloud computing approach with virtualisation as its foundation. With VMware solutions, we are able to provide an innovative service to educational institutions that is flexible whilst reducing operational costs," said Fahem Nuaimi, CEO, Ankabut.

GOURMET GULF SELECTS FINESSE AND SALESFORCE

Gourmet Gulf, a renowned hospitality company in the region, selects Finesse, a global software system integrator and Salesforce to digitally transform, taking customer dining experience in the United Arab Emirates to new heights.

The UAE-based hospitality company's partnership with Finesse and Salesforce is set to equip its business with diverse and unique functioning that allows it to expand its guest base, brand portfolio, and cuisines while enhancing its customer loyalty.

Through Salesforce, Finesse supports Gourmet Gulf to drive higher customer engagement, world-class dining experience, and enhanced customer management. Salesforce's leading CRM and cloud computing services will enable Gourmet Gulf to usher in dynamic new customer engagement models in entirely new ways that will exceed its diners' expectations.

Sunil Paul, Co-Founder & COO, Finesse, said: "We are pleased to be chosen as a strategic partner by Gourmet Gulf. With our expertise and experience in digital solutions and services, we will support Gourmet Gulf to become the best-in-class when it comes to the Diner Success Platform, customer service and ensuring loyalty. We will always continue to invest our best in this association with them and navigate Gourmet Gulf in its digital transformation"

On the same lines, Joe Teixeira, CEO, Gourmet Gulf, said: "After an elaborate evaluation process, we have chosen Finesse & Salesforce to implement the proposed solution as it resonates with our vision and will help to leave a unique experience with our customers. By embracing the solution, we hope to revolutionize the restaurant industry with a technology that shall enable Gourmet Gulf to be the leader in providing a seamless dining experience."

ABU DHABI LAUNCHES 'HUB71' TO FOSTER DIGITAL TRANSFORMATION

Abu Dhabi has launched a new platform to support high tech startups. The $141-million 'Hub71' was launched by H.H. Sheikh Khalid bin Mohamed bin Zayed Al Nahyan, Member of the Abu Dhabi Executive Council, and Chairman of the Executive Committee.

His Highness also announced a new $145 million (AED535 million) fund, to invest in technology businesses established in Hub71, which raises the total government investment in the Abu Dhabi tech sector to more than AED1 billion, accord to a WAM report.

Hub71 was established by the government to further underpin the Emirate's status as a vibrant destination of digital transformation, innovative initiatives and high-tech entrepreneurs in collaboration with key global technology companies.

The new platform is a key initiative of Ghadan 21, the Government's economic accelerator programme announced last September by His Highness Sheikh Mohamed bin Zayed Al Nahyan, Crown Prince of Abu Dhabi and Deputy Supreme Commander of the UAE Armed Forces.

Commenting on the announcement, Jassim Mohammed Buatabh Al Zaabi, Chairman of the Abu Dhabi Executive Office, said, "Abu Dhabi has proven itself as a place where innovation can succeed and inspire. Through the Abu Dhabi Government's economic programs and plans, we're doubling down on our efforts to make Abu Dhabi a global beacon for technology and innovation."

As part of the initiative, the AED535 million fund will be administered by the Abu Dhabi Investment Office, to invest in startups and venture capitalists, VCs, at Hub71.

FAMED HACKER TO HEADLINE GISEC 2019

GISEC, held from April 1-3 at Dubai World Trade Centre, aims to unravel the complex web of technology, connectivity, data that makes up the modern cyber landscape. Co-located events IoTx and Future Blockchain Summit, which form part of the Future Technology Week, will demonstrate how robust encryption and always-on connectivity will be the backbone of the modern smart city.

Across three days and six in-depth conference tracks, the events will host over 300 lectures and workshops with candid discussions on the underbelly of cyberspace as well as the positive potential of cyber-enabled, connected cities. Across the exhibition halls, over 170 brands and technologists will unveil the latest innovations designed to protect companies and build future cities.

Speakers at GISEC 2019 include some of the most famous, and in some cases, infamous, names in cybersecurity. Keynote speaker Kevin Mitnick landed himself on the FBI's Most Wanted list after hacking more than 40 major corporations. Now a trusted security consultant to Fortune 500 companies and governments worldwide, his team of white-hat hackers use their talents to expose security flaws. Jamie Woodruff, Europe's top ethical hacker is widely known as the man who hacked Kim Kardashian. One of the world's leading authorities on hacking and cybersecurity, Woodruff will take GISEC's keynote stage to discuss his career as a hacker for good.

For the first time in Dubai, GISEC's Dark Stage will be a no holds barred open forum that will take a deep dive into the dark web. The stage will see live hacks, shocking tech-spy demonstrations and talks that will cover the most dangerous threats in cyberspace. Cybersecurity experts taking the Dark Stage include Furqan AL Hashmi, Vice President of Cyber Security, JP Morgan Chase, world renowned ethical hacker Shiba Prasad Manda, and James Hadley, CISO, Immersive Labs.

Elsewhere at GISEC, industry leaders from top cyber security brands will showcase demos, hacks and industry insights into the web's most damaging cyber threats. For those looking to stay on top of the latest trends, GISEC will provide a wealth of information at the CPD accredited (ISC)2 workshops. Returning again this year are the by invitation only GISEC Private Briefings, bringing lectures given by industry leaders for the benefit of industry leaders.

EMIRATES NBD TEAMS UP WITH DIFC TO VET FINTECH FIRMS

Emirates NBD, FinTech Hive, announced a new program where they are certifying fintechs that collaborate, co-create and innovate using Emirates NBD's API (Application Programming Interface) Sandbox.

Launched by Emirates NBD Future Lab in 2018, the API Sandbox is a first in the region, marking an important milestone in the bank's AED 1 billion digital transformation programme. The platform, which has been opened up to developers and FinTech firms, consists of over 200 APIs and 500 end points covering retail, corporate and SMEs. Developers also have access to over five million simulated customer transactions based on the BIAN (Banking Industry Architecture Network) model.

Commenting on the announcement, Evans Munyuki, Chief Digital Officer at Emirates NBD, said, “As a digital pioneer in the region's banking section, Emirates NBD is proud to foster collaboration and innovation in the fast-growing FinTech space.

“The API Sandbox equips fintechs and developers with the right tools to transform their ideas into working prototypes. Through this initiative, we hope to accelerate the development and market introduction of digital banking products and services, while recognising fintechs globally,” Munyuki added.

Emirates NBD's API Sandbox follows Open Banking Standards that ensure the utmost security and privacy for its users. The platform makes Emirates NBD more accessible to developers, creating increased for value for its customers and partners, while contributing to the economic growth of the region.

HYUNDAI TO INTRODUCE SMARTPHONE-BASED DIGITAL KEY

Hyundai has announced plans to introduce new ‘digital key’ technology on future models, allowing drivers to unlock and start their car via a smartphone. Selected new cars will start offering the technology during 2019. Users will download the digital key as an app, with each car allowing up to four authorized devices.

The system uses highly secure near field communication (NFC) technology, with antennas fitted in the front door handles and in a wireless charging pad inside the car. Users unlock the car by bringing an authorized smartphone close to the door, then start the car by placing it on the charging pad and pressing a start/ stop button.

The vehicle will also recognise each user's preferred settings, such as position of mirrors, seats and the steering wheel, as well as controls for the audio, video and navigation systems, and the head-up display.

“This is a practical application of Hyundai's connected vehicle technology to create new, genuinely useful functions,” said Mike Song, Hyundai's Head of Operations for the Middle East and Africa. “Not only will people be able to use their smartphone in place of a key, but they will also be able to authorise other drivers simply by sharing the app, without having to keep track of multiple sets of car keys.”

When sharing the car, a Hyundai owner will be able to limit the functions available for each digital key. This could include placing a time-limit for when the key will expire or setting an alert to warn the owner if the car is being driven too fast or is outside a designated area.

EMPOWERING NETWORK OPERATIONS

LORI MACVITTIE, PRINCIPAL THREAT EVANGELIST, F5 NETWORKS, EXPLAINS WHY STANDARDISATION IS GOOD FOR NETOPS

Standardisation is sometimes viewed as an assault on innovation. Being forced to abandon a polyglot buffet and adopt a more limited menu will always sound stifling. That may be because standardisation is often associated with regulatory compliance standards that have official sounding names like ISO 8076.905E and are associated with checklists, auditors and oversight committees.

The reality is that there are very few standards – in fact none that I can think of – governing enterprises choice of languages, protocols and frameworks.

Enterprise standardisation is more driven by practical considerations such as talent availability, sustainability, and total cost of ownership over the (often considerable) lifetime of software and systems.

Studies have shown the average software lifespan over the past twenty years is around six to eight years. Interestingly, longevity tends to increase for larger programs, as measured by lines of code (LOC). Systems and software with over a million LOC appear to have lifespans over a decade, lasting 12 to 14 years. While you may dismiss this as irrelevant, it is important to realise that at the end of the day, network automation systems are software and systems. They need the same care and maintenance as software coming out of your development organisation. If you're going to treat your production pipeline as code, then you've got to accept that a significant percentage of that automated pipeline is going to be code.

Over the course of that software or system lifespan, it's a certain bet that multiple sets of operators and developers will be responsible for updating, maintaining, operating, and deploying changes to that software or system. And this is exactly what gets at the heart of the push for standardisation - especially for NetOps taking the plunge into developing and maintaining systems to automate and orchestrate network deployment and operation, as well as application service infrastructure.

Silos are for farms

If you or your team chooses Python while another chooses PowerShell, you are effectively building an operational silo that prevents skills sharing. This is a problem. The number one challenge facing NetOps, as reported in F5 and Red Hats' State of Network Automation 2018 report, was a lack of skills (49% of surveyed NetOps). Therefore, it would seem foolish to create additional friction

by introducing multiple languages and/or toolsets. It is similarly a bad idea to choose languages and toolsets for which there is no local source of talent. If other organisations and nearby universities are teaching Python and you choose to go with PowerShell, you're going to have a hard time finding staff with the skills required for that system.

It is rare that an organisation standardises on a single language. However, they do tend to standardise on just a few. NetOps should take their cues from development and DevOps standards as this will expand the talent pool even further.

Time to value is valuable

Many NetOps organisations already find themselves behind the curve when it comes to satisfying DevOps and business demands to get continuous. The unfortunate reality of NetOps and network automation is that it's a heterogeneous ecosystem with very little pre-packaged integration available. In the State of Network Automation survey, this "lack of integration" was the second most cited challenge to automation, with 47% of NetOps agreeing.

Standardising on toolsets, and on infrastructure where possible (like application services), provides an opportunity to reduce the burden of integration across the entire organisation. What one team develops, others can leverage to reduce the time to value of other automation projects. Reuse is a significant factor in improving time to value. We see reuse in developer proclivity toward open source and the fact that 80-90% of applications today are composed of third-party/open source components. This accelerates development and reduces time to value. The same principle can be applied to network automation by leveraging existing integrations. Establish a culture of sharing and reuse across operational domains to reap the benefits of standardisation.

> "IT IS RARE THAT AN ORGANISATION STANDARDISES ON A SINGLE LANGUAGE. HOWEVER, THEY DO TEND TO STANDARDISE ON JUST A FEW. NETOPS SHOULD TAKE THEIR CUES FROM DEVELOPMENT AND DEVOPS STANDARDS AS THIS WILL EXPAND THE TALENT POOL EVEN FURTHER."

Spurring innovation

Rather than impeding innovation, as some initially believe, standardisation can be a catalyst for innovation. By standardising and sharing software and systems across operational domains, you have a more robust set of minds and experiences able to collaborate on new requirements and systems. You're building a pool of talent within your organisation that can provide input, ideation, and implementation of new features and functionality – all without the sometimes-lengthy onboarding cycle.

Standardisation also speeds implementation. This is largely thanks to familiarity. The more you work with the same language and libraries and toolsets, the more capable you become. That means increased productivity that leads to more time considering how to differentiate and add value with new capabilities.

Standardisation is an opportunity

Standardisation can initially feel stifling, particularly if your pet language or toolset is cut from the team. Nevertheless, embracing standardisation as an opportunity to build out a strong foundation for automation systems and software can benefits the business. It also affords NetOps new opportunities to add value across the entire continuous deployment toolchain.

Even so, it is important not to standardise for the sake of it. Take into consideration existing skill sets and the availability of local talent. Survey universities and other businesses to understand the current state of automation and operations' skill sets and talent to make sure you aren't the only organisation adopting a given language or toolset.

For the best long-term results, don't treat standardisation like security and leave it until after you've already completed an implementation. Embrace standardisation early in your automation endeavours to avoid being hit with operational and architectural debt that will weigh you down and make it difficult to standardise later.

SUPPLY CHAIN RISK MITIGATION STRATEGIES

MARK STEVENS, SVP, GLOBAL SERVICES, DUGITAL GUARDIAN, ON HOW COMPANIES CAN MINIMISE THEIR SUPPLY CHAIN VULNERABILITIES

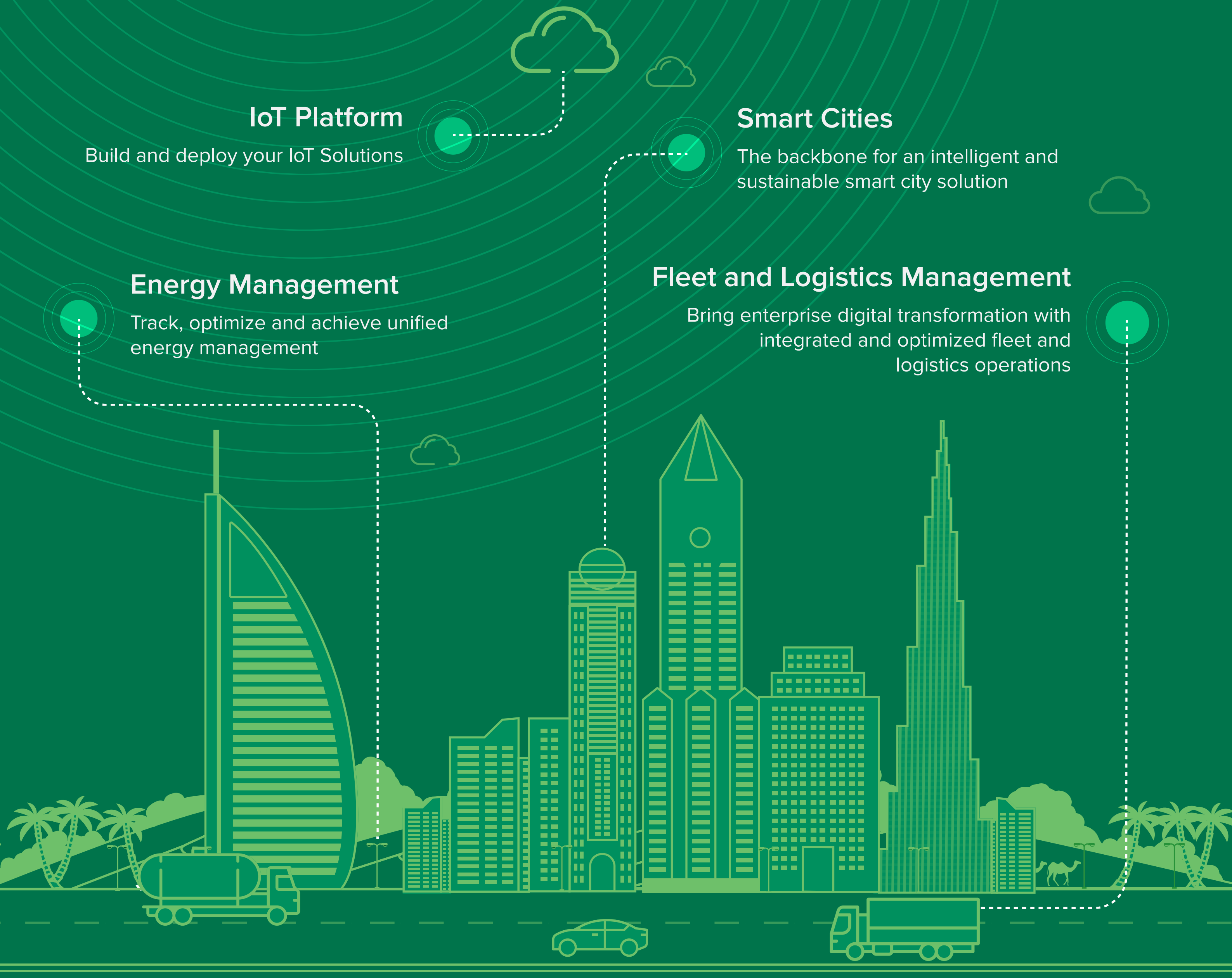
Companies today face the challenge of balancing strict data privacy rules, such as PCI-DSS and GDPR, with the growing need to leverage customer data. With yet more regulations looming on the horizon, especially in the wake of the 2017 Equifax breach, companies are under pressure to keep up with the latest legislation, guidelines and best practices to maintain compliance.

In addition to these pressing demands, finding better ways to mitigate supply chain risk is a further top priority. Everything from applying rigorous cyber security technologies, processes, and supply chain management strategies, to implementing a framework to assess and monitor supplier integrity.

WebNMS
IoT Division of ZOHO Corporation

ZOHO

WebNMS IoT Platform powering successful **Digital Transformation**



IoT Platform

Build and deploy your IoT Solutions

Smart Cities

The backbone for an intelligent and sustainable smart city solution

Energy Management

Track, optimize and achieve unified energy management

Fleet and Logistics Management

Bring enterprise digital transformation with integrated and optimized fleet and logistics operations

WebNMS is the IoT division of Zoho Corporation that offers powerful end-to-end IoT Platform and Solutions for SMBs and Enterprises.

www.webnms.com ✉ **iot-eval@webnms.com** **in @WebNMS** **@WebNMSIoT**

With supply chains becoming more complex, the consequential risk exposure for businesses is growing. And while the rise of third-party outsourcing has enabled corporations to innovate and boost efficiencies, with regulatory scrutiny tightening — and financial penalties in the face of compliance violations growing — taking steps to minimise risk, protect the smooth-running of operations, and assure customer confidence, is a vital yet tricky path to navigate.

Taking a holistic approach to data security is a must — and there are a number of steps organisations can take to mitigate their supply chain risk.

Know who you're doing business with

Better due diligence on third-party relationships will improve transparency within the supply chain. But for many corporations, conducting this due diligence efficiently and effectively is a challenge when dealing with thousands of third parties and vendors.

Deploying efficient and automated screening, using machine learning algorithms to speed up this process, can reduce the cost and time frame of conducting due diligence on suppliers. Similarly, ongoing monitoring programmes can automatically flag if a supplier is connected to criminal activity or Politically Exposed Persons (PEPs) who pose a greater risk of corruption and bribery.

Address IT and cyber risks

A belt and braces approach should incorporate a vulnerability assessment and ongoing monitoring of the network and all connected devices, alongside the organisation's websites, apps and firewall configurations.

Having remediated any gaps in IT security, the next step is to focus on updating processes to prevent these from reappearing, ensuring that the IT practices implemented are in line with industry standards to reduce the chance of unintentionally opening the enterprise to new risks.

Security awareness training for the workforce is the final vital step, ensuring that staff are able to identify and avoid cyber threats like phishing, malware and scams. Utilising security tools to scan emails, manage communications and quarantine any malicious threats that make it through the enterprise's security perimeter should also be in place.

Many organisations are eliminating the risks posed by the vulnerabilities of the traditional browser by disconnecting it from local IT and moving it to the cloud to create an additional layer of security.

Finally, when it comes to the transfer of personal or sensitive data between a supplier and vendor, compliance tools can help find data leaks before hackers do.

Understand supply chain dependencies

Modelling and analysing the supply chain — including identifying the operational impact of a critical supplier's facility being out of commission — will help uncover any hidden or overlooked areas of high risk. Revealing the dependencies and bottlenecks that will need to be addressed to minimise any potential disruption.

Automated risk assessment and advanced risk modelling can deliver the insights companies need to ensure they can quickly halt the use of unsafe suppliers or define operational risk management strategies.

This may lead to a further diversification of suppliers, or the signing-up of alternate suppliers who are poised to step in and replace parts of the supply chain in the event of a disruption.

Take an integrated approach to supply chain risk

Many organisations lack an integrated approach to managing the end-to-end delivery of products or services to customers that involves back office, middle office, risk management, business developers, finance and IT. As a result, they lack a clear picture of risk across the entire supply chain.

With each department working in silos and using their own methods and technologies to assess risk relating to their individual areas of work, it's easy to miss the bigger risk picture until something goes wrong. At which point the available mitigation options are limited and can be very costly to implement.

Instead, organisations should take a more integrated approach and consider the impact of a potential failure at any point along the supply chain – such as a data centre outage – as well as evaluating how different business units collaborate to deliver on broader organisational goals.

Conclusion

Today's technology solutions can help organisations minimise risk in their supply chains. Making it easier to automate workflows, compress the time needed for data mining and aggregation, and monitor large third-party data ecosystems. Similarly, utilising AI and integrated risk analytics can make it easier to identify and assess supplier related threats — including cybersecurity breaches, money laundering, insolvency, data mishandling and regulatory noncompliance — so that organisations can act promptly to manage or remove the risk source.

teksalah
BEYOND SOLUTIONS

Redefining ICT
With Innovation and Excellence

www.teksalah.com
solutions@teksalah.com

Dubai | Abu Dhabi
#Teksalah

REBOOTING RETAIL

MIRIAM BURT, MANAGING VICE PRESIDENT, GARTNER, ON THE TRENDS THAT ARE REVOLUTIONISING THE RETAIL INDUSTRY

In retail, is digital transformation all about automating existing business processes or creating new business models and revenue streams?
All of that, and that is why it is very difficult to pin down what people mean by digital transformation. The keyword that we need to remind ourselves of is digitalisation, which means anything that is running in your business on to which you can apply digital. It is not just about online marketing. For example, if you take a process that goes across the channels – you buy something online, and you pick it up in store. That is also a digitalised process. In the olden days, you'd go to a store, look for something and then pick it up off the shelf. Now, we have substituted that research part online. You need to think of digital business as digitalisation of business processes.

What are your thoughts on the so-called retail apocalypse?
I think it has been blown out of proportion by the media. While it's true that there have been some big-name closures and bankruptcies in retail, more stores are opening than closing globally. So, it is a fallacy and myth that online shopping is killing brick-and-mortar retail. What is actually getting reduced is the amount of space -a large retailer will close a big store and open up two small stores. Stores are growing, but retail space is becoming less.

Among the new crop of technologies, which one could change retail forever?
What we are seeing is that there is more adoption of AI because you can actually do something at both back-end and front-end with AI. For example, if you are a retailer with a call centre, you can use AI and chatbots to deal with customer complaints quickly, and on the front-end, if you are trying to improve customer experience, you can deploy chatbots there as well. It is not about any particular technology – you can't say it is going to be AI, blockchain or IoT that will be more transformational. Furthermore, these technologies work together, and it's meaningless to talk about them in isolation. If you look at AI and machine learning, you need data - some of the data will come from databases, some of it will be unstructured data such as podcasts, videos, blogs and also from things that ping, which are sensors. That is IoT, and already you have a connection between AI and IoT.

Most of the retailers seem to be focused on transforming the front-end. Wouldn't they need a corresponding digital back-end to make a difference?
Actually, they are focusing on the back-end, and you may not see it. One of the biggest discussions we have at the moment is the automation of labour – replacing people with machines. For the most part, the back-end discussion tends to be about cost optimisation while on the front-end it is all about revenue generation and enhancing value for customers.

Bridging the gap between physical and virtual worlds is a daunting challenge for many retailers. How can they go about it?
What we have found from our research is that retailers who have been successful in gaining traction know how to bring the two together. It's about very simple things- you need to have the same pricing across channels, and the same thing applies to returns policies and promotions, which will lead to channels syncing up with each other even in the very basic things. But, then you start to offer buy online, pick up in-store services. So, whatever processes you have online should be extended to offline. If you have customers who purchase online and want to pick it up in store, the integration between the two in terms of customer, product and order data should be a smooth process.

What is your advice to retail CIOs?
Whatever technologies retailers are using, they really have to make sure they do three or four things: make people's lives easier, better, safer and simpler. When retailers start to talk about AI or some other new technology, our simple question is this: does it make your customers' experience simpler and easier? If it does not, then why are you doing it? By that I mean not just the front-end but the back-end as well.

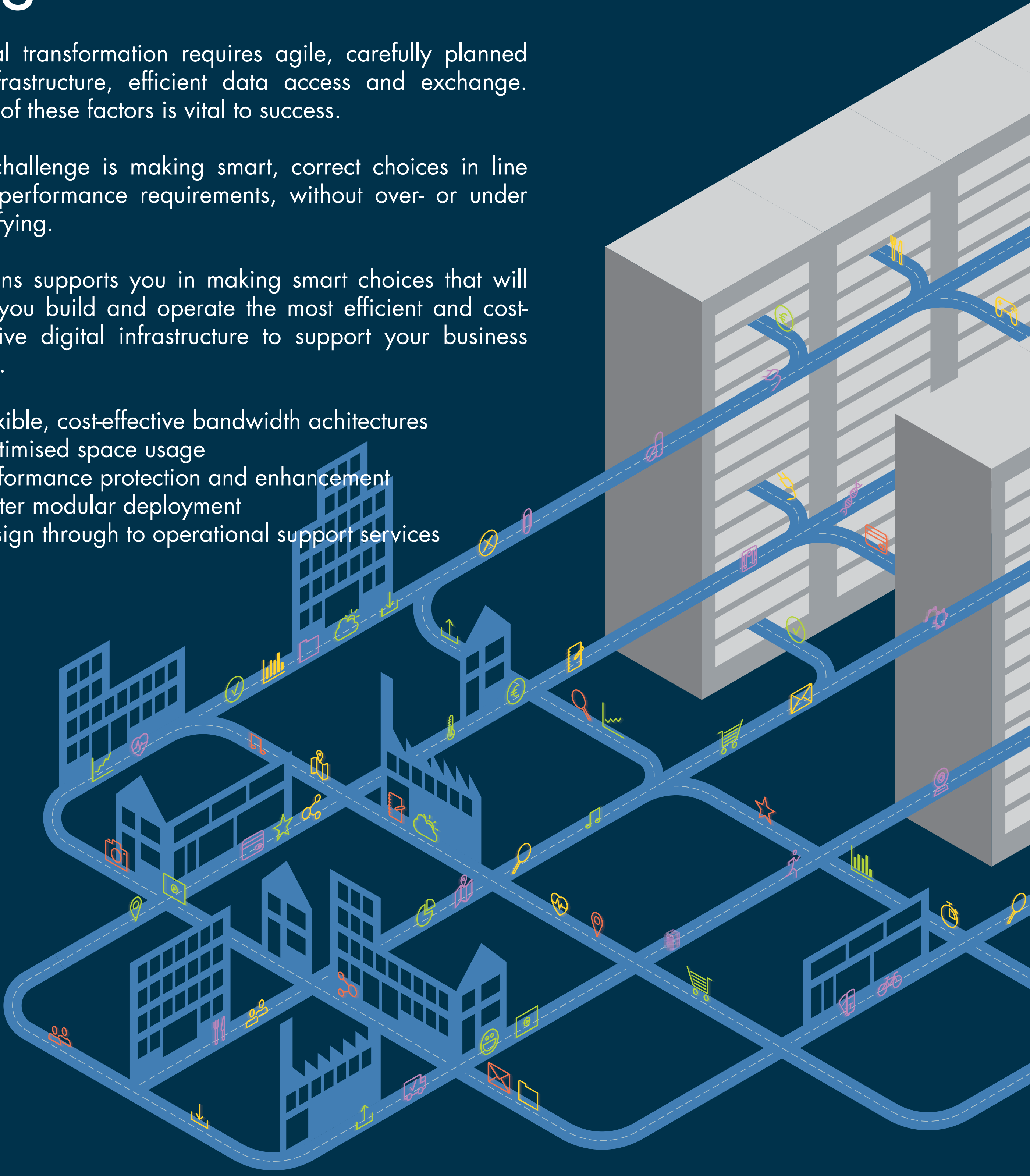
Smart Choices for Digital Infrastructure

Digital transformation requires agile, carefully planned IT infrastructure, efficient data access and exchange. Each of these factors is vital to success.

The challenge is making smart, correct choices in line with performance requirements, without over- or under specifying.

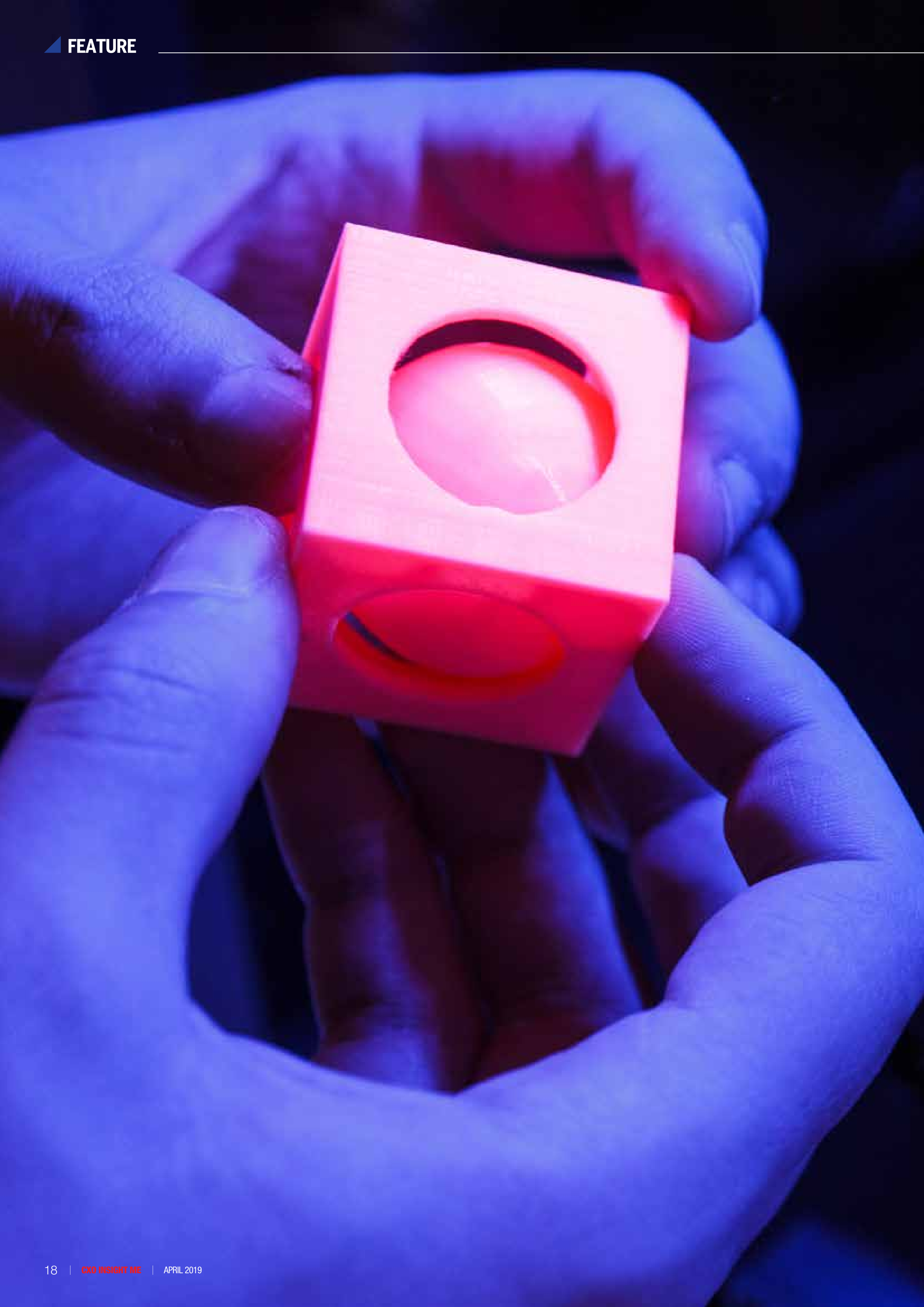
Nexans supports you in making smart choices that will help you build and operate the most efficient and cost-effective digital infrastructure to support your business goals.

- Flexible, cost-effective bandwidth achitectures
- Optimised space usage
- Performance protection and enhancement
- Faster modular deployment
- Design through to operational support services



www.nexans.com/LANsystems

Nexans
BRINGS ENERGY TO LIFE



A NEW DIMENSION

IS 3D PRINTING A NEW REVOLUTION OR A TECHNOLOGY FAD?

In 2016, Dubai announced the world's first 3D-printed office, dubbed office of the future. Last year, Saudi Arabia showcased the country's first house built with 3D printing. Why is 3D printing getting so popular in the Middle East? It is being touted as a revolutionary new technology that will change every aspect of our lives with its ability to print or replicate everything from human body parts to multi-story houses. Though 3D printing has been around for more than 30 years, used mainly for product prototypes, the latest advances in the technology have made it popular outside of its traditional base of automotive manufacturing and healthcare. Today, 3D printing applications are being used in many other industries including fashion, jewellery, and even in the food industry.

According to IDC, the global spending on 3D printing including hardware, material, software, and services is slated to grow to $23 billion in 2022, and worldwide spending is predicted to exceed $14 billion in 2019.

The analyst firm says 3D printers and materials will account for roughly two-thirds of the global spending, reaching $7.8 billion and $8 billion respectively in 2022, while services will account for $4.8 billion, led by on-demand parts services and system integration services.

Though many countries have started to grab the opportunities presented by the technological advancements in 3D printing or additive manufacturing as some call it, the Middle East region is witnessing the most notable growth in adoption.

Ashish Panjabi, chief operating officer at Jacky's Business Solutions, explains why: "3D printing has benefited from the fact that we are in a fairly advanced region when it comes to adoption of new technologies and there is an ability to invest in innovation. The largest market for 3D printers in the Gulf countries has been education. Governments, as well as private educational institutions, have been investing in technologies such as 3D printing, robotics, and VR as more use cases find their way into the educational curriculum. The emphasis on STEM (science, technology, engineering, and math) in schools has helped increase the adoption of 3D printing in schools across the region.

"In addition to that, the growth in innovation centres, especially those that are government-backed has meant there are more workspaces where people have access to 3D printers. This, in turn, creates a secondary market for 3D printers."

Julian Callanan, founder and MD of Sinterex, which specialises in 3D printed healthcare products, says government strategy and market demand are combining to grow the 3D printing market in the Middle East. "Specifically, the Government of Dubai has outlined a strategic plan to position Dubai as a world hub of 3D printing by 2030. This has driven government departments, such as DHA, to be very open to collaborating with companies developing 3D printing business concepts. Outside of the public sector, in the private sector, we are seeing growing demand for 3D printed products in the fields of education, healthcare, and consumer products."

What are some of the leading use cases for 3D printing today? A massive drop in prices of 3D printers and printing material has spawned a wide variety of use cases in sectors such as aerospace, architecture, healthcare, electronics, and consumer products. In fact, some industry experts envision a future with 3D printers in every home, churning out everything from pizzas, pasta to shoes and clothing.

"Apart from education, we have seen 3D printing's role increase in industries where 3D imaging is readily available, such as dental and medical fields. However, what has been most interesting is to see more makers in the region adopt 3D printing. These makers could be designing, developing or prototyping products such as fashion accessories, finished goods or even aircraft parts," says Panjabi.

In most countries, traditionally the largest market for 3D printers has been manufacturing, but since we don't have a large manufacturing base here, education is still the largest market. The hope is that this market will continue to grow as the products of the education system will probably expect to see and use 3D printers in their workplace in years to come, he adds.

Callanan from Sinterex says 3D printing is making inroads into several different industries and cites the example of the large construction market in the UAE. "3D printing is helping architects and project developers to create miniature models of their future planned projects. Similarly, we have a heavy industrial base including oil and gas, and shipbuilding and repair. 3D printing is allowing engineers to create prototype parts for analysis, short-run specialty product parts for

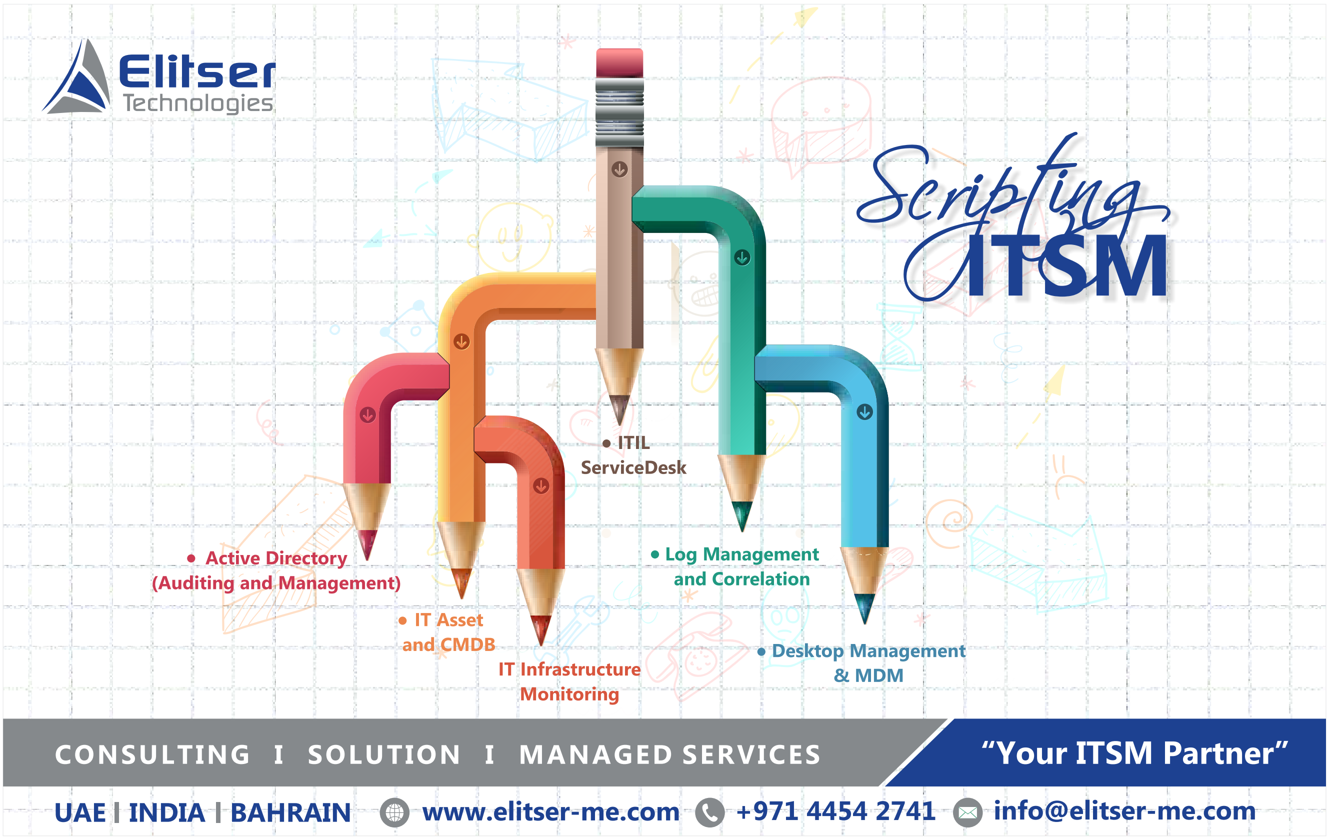
Ashish Panjabi, chief operating officer at Jacky's Business Solutions

high-end applications and to replace damaged parts at short notice."

In the healthcare sector, where Sinterex is focused, 3D printing is used to product study models which allow doctors to physically inspect complex medical issues. "Also, we see 3D printing being used for the production of customised patient-specific medical devices. These are printed in materials such as titanium and allow doctors to pre-fabricate the solutions to address complex medical cases," adds Callanan.

Julian Callanan, founder and MD of Sinterex

Now, the question is whether 3D printing will become a mainstream technology within this decade as printer speeds keep doubling and becoming more affordable. Panjabi from Jacky's says the price has never been an issue. "They have always been available at a wide range of prices for several years now. The main limiting factors have been speed (the time it takes to print something in 3D) and materials that can be printed in 3D. 3D printing will continue to get quicker and more materials will keep being developed. However, there is no one 3D printer that can print all the different materials. Many can print on a variety of materials, so most 3D printing facilities need a variety of 3D printers or combine them with traditional technologies like CNC or milling machines if they want to have a complete solution."



Smart Business Solutions

- IT Consultancy
- Core Business
- Digital Transformation
- Cyber Security
- Data Centers

Banking & Financial Services

- Payment Systems
- Reporting Systems
- Mobile Payments & Blockchain
- Financial Peripherals

“TOGETHER ON YOUR DIGITAL TRANSFORMATION JOURNEY”

Technical Staffing Services

- IT Professionals Outsourcing
- IT Managed Services (Onsite & off-shore)

رقميات
Raqmiyat

Dubai - UAE
P.O.Box 8547
Tel: +971 4 295 9606
Fax: +971 4 295 9515

Abu Dhabi - UAE
P.O.Box 44195
Tel: +971 2 627 0576
Fax: +971 2 627 4867

Riyadh - KSA
P.O.Box 301503
Tel: +966 1 293 7344
Fax: +966 1 293 7388

Chennai – India
#236, OMR, CH-97
Tel: +91 44 3041 3600
Fax: +91 44 3041 3611

www.raqmiyat.com

THE FUTURE OF WORK

ABHIJEET SANYAL, AVP OF TECHNOLOGY STAFFING SOLUTIONS AT RAQMIYAT, EXPLAINS WHY ON-DEMAND STAFFING, WHICH ALLOWS COMPANIES TO HIRE SKILLED AND VETTED WORKFORCE WHEN THEY NEED IT, IS THE BEST CHOICE.

How is Raqmiyat helping to fill the skills gap?
Our IT staffing business dates back to 2004. We started offering this as a value-added service predominantly for the banking industry, where Raqmiyat has a strong foothold with our own products such as cheque clearing systems and payment gateways. Later, we moved into the government sector. Currently, our IT staffing portfolio has more than 400 resources deployed with 50 active customers across the UAE, Bahrain, and KSA. We are a technology company, and we can provide an entry-level help desk resource all the way up to a highly specialised AI expert. We cover the whole technology stack.

Is it more challenging to staff IT projects today than say five years ago?
As technology keeps advancing, the cost of acquiring skills has increased. This is a highly competitive market but unregulated. We have seen many small-time staffing companies mushrooming across the country, offering their services cheap and this has led to severe margin erosion. We are addressing this challenge by going up the value chain of IT skills.

There was a time when finding the right skill was also an issue. But, this has changed with the onset of rapid technological evolution, and candidates have had to ramp up their efforts with training and certifications to hone their skills to keep pace. This has an impact on our training costs while managing a workforce.

What kind of skill sets are in high demand now?
Right now, the most sought-after skills are in the cybersecurity space, and we are also driving that as a focus area because Raqmiyat has a fully-fledged cybersecurity practice. Apart from security, there is also a robust demand for ERP experts. We are an Oracle shop, and we have always been known for our quality Oracle specialists. However, in the last one year, there has also been an increasing demand for SAP consultants, especially in the manufacturing sector.

Do you see a demand for skills in new areas such as data scientists and analytics?
We are seeing a demand for data scientists in industries such as aviation and media, and also for Hadoop developers.

How do you make sure your workers are a good match for the job?
Raqmiyat has mastered the art of match-making. We have a two-pronged approach with the presales team going the extra mile to understand what the client needs beyond a job description, identifying the hidden nuances of the department requisitioning the particular skill or a group of skills, while the recruitment team tests and screens candidates who can deliver on the requirements for the job with the right skills.

What are the benefits of workforce-as-a-service (WaaS) model for customers?
We are in the business of selling careers. It is a common knowledge that a content employee is more often a productive one when their career is mapped out by the organisation with a growth path both in terms of earning and learning. What we guarantee to our clients is a productive and quality workforce.

The biggest benefit of the WaaS model is that it completely eradicates direct HR overheads and the cost of support functions, which enables our customers to focus on their core business. Another benefit is you can hire a 'plug-and-play' resource because you don't have to train them, and they can be on the job from day one. This is ideal for companies who don't want to hire or train new employees and it saves them huge upfront investments as well.

Additionally, the WaaS recruiters stay abreast with the ever-changing work environments and labour laws. They know how to recruit of out the box. At Raqmiyat, we make our recruitment team go through regular technology enablement sessions and labour law training. The team is also trained to hire quality resources using social media effectively, not just job boards.

Hewlett Packard Enterprise | AMD

HPE and AMD deliver Around-the-Clock performance, security & savings

HPE and AMD:
A future of innovation

Dual-socket power in
a single socket server.

Up to 32 cores
per socket

Delivers outstanding
performance

33% more
memory capacity

2TB
RAM per socket

More memory per core means more VMs and workloads per server

8 memory
channels per CPU

Reduces latency

Exceed customer expectations and service-level agreements

Silicon root of trust:
protection from power on

Fast data security from
hardware encryption

Rated the
most energy-efficient

Around the clock space
and power savings

Real-time user and
data monitoring

Up to 128 PCIe Gen 3 lanes

delivers agile software-defined
storage solutions

25% better
processor-performance value

Increased agility helps you
deliver increased value

Footnotes:

[1] Based on a comparison of the SPECvirt_sc2013 results for the HPE ProLiant DL325 Gen10 with 1 AMD EPYC 7551P. SPEC and the benchmark name SPECvirt_2013 are registered trademarks of the Standard Performance Evaluation Corporation (SPEC). The stated results are published as of 06-05-18; see spec.org

[2] The stated leadership results are published as of 8-15-2018 to SPEC; see spec.org/power_ssj2008/results/res2018q2/power_ssj2008-20180410-00808.html

A KING'S RANSOM

BRIAN PINNOCK, CYBERSECURITY SPECIALIST AT MIMECAST, ON HOW TO AVOID THE HIGH COST OF POOR CYBER RESILIENCE

Question: Does your business have over US$ 1 million stashed away to recover from a ransomware attack? Unless you have a solid cyber resilience strategy in place, I hope you answered 'yes'. If not, you might want to consider one – a cyber resilience strategy, that is, not a 'rainy day fund'.

Ransomware attacks are increasing, both in frequency and cost to businesses. They are expected to impact one business every 14 seconds by the end of 2019, up from every 40 seconds this year. This makes it hard to know how much an attack will cost businesses in downtime, lost revenue and ransom. But, $1 million is the average for Middle East organisations.

Globally, damages from ransomware attacks are expected to reach $11.5 billion in 2019. That's up from $5 billion in 2017 and $325 million in 2015. These are massive increases every two years – and the trend is likely to continue. My point is that US $1 million might be a conservative estimate in a few months' time. Plus, the golden rule of cybersecurity is not to wonder if, but when you will be attacked. Honestly, assume you're already a target.

In the case of a ransomware attack, your organisation needs to be able to recover quickly so employees can carry on with their day 'business as usual'. This will help avoid losing valuable productivity, revenue, brand reputation – and, potentially, customers. And the best way to do that is by having a comprehensive cyber resilience for email plan in place.

A 2018 study by Vanson Bourne and Mimecast found that 52% of organisations had seen an increase in ransomware over the previous year. And, the longer an attack goes undetected, the bigger the financial and reputational damage, and the harder it is to recover. An alarming 71% of organisations that experienced a ransomware attack over the past year reported that downtime lasted for one day or longer, with three days of downtime being the average. Could your business survive if it came to a screaming halt for that long?

Keys to the kingdom

Ransomware is just one type of attack that businesses should be concerned about. Another way cyber criminals can access valuable information or money is through impersonation fraud. So, not only do criminals kidnap your king and demand money for his safe return; they sometimes also pretend to be your king – and it's hard to spot the imposter.

Impersonation fraud is one of the most common attack vectors used by cybercriminals to gain access to company information, with global businesses seeing a 40% increase in this type of fraud. Typically, hackers masquerade as a high-ranking individual in the company. They send an email to someone, asking them to wire money or send them sensitive information. Because this person carries a lot of authority within the business, few people will object to the request.

If you received an email from your head of compliance, asking for personal data about your customers, you'd probably give them the information. You might not notice that the email was fake until it was too late because hackers use sophisticated techniques such as URL spoofing and domain similarities, which most office workers are not trained to spot.

When sensitive information gets into the wrong hands, it creates all sorts of problems for the business. Reputational and financial damage is one thing. Running into compliance issues is a whole other ballgame. The European Union's General Data Protection Regulation, which came into effect in May last year, can impose fines of up to €20 million on companies that fail to protect European citizens' personal information.

Batten down the hatches

Only 11% of global organisations conduct near-continuous training to help employees spot cyberattacks. Twenty-four percent of respondents have monthly training sessions and 34% have quarterly sessions. But monthly or quarterly training is not enough and the information being shared usually isn't absorbed properly. This is because training sessions are seen as inconvenient by staff and are often boring. For the best results, businesses should conduct security awareness training continuously. More importantly, training should be engaging and interesting.

Security awareness training is a crucial aspect of a cyber resilience strategy and needs to be entrenched in the culture of an organisation – especially since 23% of global businesses are not confident that their employees can spot and defend against impersonation fraud.

> “THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION, WHICH CAME INTO EFFECT IN MAY LAST YEAR, CAN IMPOSE FINES OF UP TO €20 MILLION ON COMPANIES THAT FAIL TO PROTECT EUROPEAN CITIZENS' PERSONAL INFORMATION.”

But training alone will not deter cybercriminals from trying to 'kidnap your king' – your critical data, systems and, of course, your money. And because email breaches account for 96% of security incidents, addressing this exposure should form the core of your cyber resilience strategy.

If you think your business is protected because you use Microsoft Office 365, I have bad news. In our latest Email Security Risk Assessment (ESRA) report, we found that incumbent email security systems are missing more than 25 percent of emails containing dangerous attachments in comparison to last quarter's findings. The report also found that 17,403 malware attachments and 42,350 impersonation attacks were missed and delivered to users' mailboxes.

Traditional, defence-only security approaches that rely on disparate technologies are no longer enough and will leave you chasing your tail. The only way to get ahead of cybercriminals is through cyber resilience for email, which will help you secure, preserve and continue the flow of information via email, even during an attack.

A key component of any cyber resilience strategy is email and data archiving, which allows you to immediately recover all your data in the event of an attack. This ensures your data is always protected and accessible to users. It also prevents a data hostage situation and means you never have to pay a ransom to get your data back.

Having a solid cyber resilience for email strategy prepares you for every stage of attack: it puts the right security in place before an attack happens, provides you with the durability to continue with business as usual during an attack, and helps you recover your data after an attack.

A robust email security inspection system should be able to score emails for potential impersonation attacks and either block, quarantine or flag them as suspicious before they reach the recipient's inbox.

Essentially, they give you time to move the king to safety before the kidnappers arrive at your door. Who knows what arsenal they're carrying and if you can fight fire with fire? If you only act after they've arrived, it's probably already too late to save the king.

THE RISE OF DIGITAL IDENTITY

BY ALEJANDRO GOMEZ DE CUENCA, VICE PRESIDENT, GEMALTO GOVERNMENTS BUSINESS UNIT

The field of digital identity management is fast expanding, with the adoption of the Internet of Things (IoT) forecast to connect over 200 billion devices by 2020, irruption of new technologies such blockchain and DLT and use of digital technologies across the world at an all-time high.

The global shift towards digital identification systems provides organisations and governments with the opportunity to act as main accelerators of this trend. The world is demanding a rapid change towards new technologies and consumers are expecting to transact digitally in real-time. On the other side regulations related to data privacy such the GDPR in EU and similar regulations across the globe, individuals demand a more secure mechanism to store Identity information where self-sovereign identity is slowly taking traction in some implementations and pilots world-wide.

Digital identity is the technological link between a real entity, such as a person, and its digital equivalent entities. It encompasses a collection of electronically captured and stored identity attributes, including biographic and biometric data, stored in something the person has—like a smartphone (used as an IoT device)—that can uniquely describe them within a given context. We all possess a digital Identity such the one we use in social networks or the one we use when interacting with several online services.

Trusted digital IDs are created when the information provided has been verified or checked for authenticity. A trusted digital ID consists of a set of verified attributes (like verified ID documents or biometrics), thus providing a certifiable link between an individual and their digital identity. These attributes may also include verification with third parties, such as government databases, social identity, credit card information, mobile records and so on.

Technology is at the heart of enabling trusted digital IDs, helping governments, service providers and other players in the ecosystem to create trusted digital security.

The key question here is to determine which digital identity can be trusted. Self and remote registrations processes are more and more the way to go for service facilitation which brings several challenges and threats to trust, such counterfeit identity documents, spoofing attacks to facial recognition technologies and others. Under these conditions, governments play a major role in issuing a 'trusted' digital identity to its citizens and residents assuming the entire chain of identity proof from birth registration to identity card issuing is secured.

In cases of important interactions conducted online, such as governmental and banking transactions, it's critical that you are who you claim to be. The same applies to our mobile phones – as an essential extension of ourselves that holds our most security-sensitive information, it's crucial that the identity connected to that phone is real and verifiable, which is where trusted digital IDs come into play.

With that in mind, the GCC market shows several initiatives and can be considered as an early adopter of the concept of digital identity.

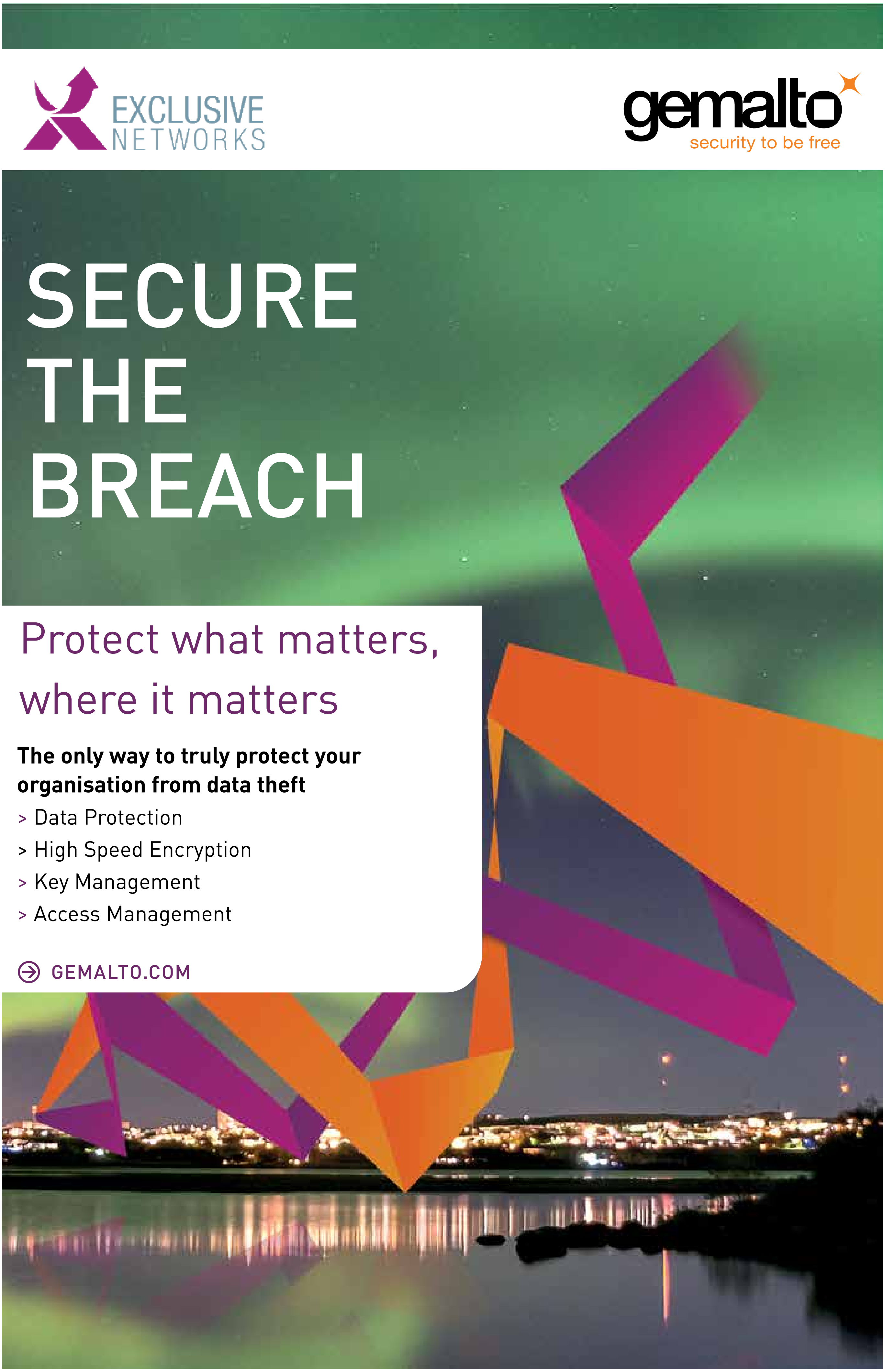
The UAE has also made significant strides in the field of digital IDs, as different possibilities continue to be deployed, especially in the government sector, showing us the rapid pace that this technology is developing. For example, the UAE recently introduced the UAEPASS, which not only streamlines transactions but also ensures that digital data is protected by enabling all UAE residents to have a digital national identity that can be used to access government services and make transactions online.

There are five key trends driving the trusted digital identity, which we will explore below.

1 THE TECHNOLOGY

New technologies are constantly emerging to support and shape the shift towards digital identities. There are many notable examples of digital transformation initiatives in the UAE and the GCC countries, where trusted digital IDs are in the heart of the service.

Dubai already has Smart Gates, which use a system integrated with the Emirates Identity Authority in order to enable Emirates ID card holders to pass through



Dubai Airport seamlessly and securely. The government of Dubai also aims to develop digital passports for seamless entry at Dubai Airport, combining biometric verification and blockchain technology, allowing people to walk straight through to baggage collection without stopping at passport control.

2 MORE MOBILITY AND CONVENIENCE

Today's customers are able to access online services remotely without having to go to physical branches, which is especially true for transactions related to banking. In order to provide a seamless omni-channel experience that is convenient and also secure, implementing trusted digital IDs is a must.

In fact, according to recent Gemalto research, 70% of users would like to have trusted digital IDs, and 66% of them would use them to perform more transactions.

3 GREATER DEMAND FOR SECURITY AND TRUST

According to Gemalto's latest Breach Level Index, of the 1,765 data breach incidents in 2017, identity theft represented the leading type of data breach, accounting for 69% of all data breaches. Additionally, following the significant cyberattacks we witnessed in the last few years, 43% of users claim they fear fraud, phishing, hacking and getting their personal information stolen. Here in the UAE, a recent Norton Cyber Security report showed that more than half (52%) of respondents experienced any sort of cybercrime in the country.

It's clear that consumer awareness of security and privacy is increasing, making regulators, MNOs, manufacturers and service providers more concerned about providing the right protection for connected devices, and the data they collect, share and store.

This means that the demand for security and trust is greater than ever before. So, robust security measures will be the obvious response to new demands for trust in all exchanges between users and service providers.

> “OTHER STAKEHOLDERS SUCH AS SMARTPHONE MANUFACTURERS, MNOs, GOVERNMENTS AND FINANCIAL INSTITUTIONS ARE ALSO SHIFTING TOWARDS DIGITAL IDENTIFICATION SYSTEMS TO PROVIDE TRUST AND CONVENIENCE FOR CITIZENS USING THEIR SERVICES.”

4 NEW REGULATIONS

As new regulatory environments take shape, close collaboration between the financial world, central and local public authorities and digital communications operators will support effective solutions and implementation of best practices.

For example, organisations offering financial services need to comply with anti-money laundering (AML) legislation leading them to follow a client identification procedure of Customer Due Diligence (CDD) or Know Your Customer (KYC). The Abu Dhabi Global Markets recently launched an electronic-Know-Your-Customer (eKYC) project in collaboration with a number of financial institutions in the UAE to use regulatory technology or 'RegTech' solutions to address industry challenges.

Increasingly, banks and financial institutions are seeking more ways to meet KYC and AML requirements and standards. The focus will be on the adoption of the new structures and regulations that are needed to govern the associated services, transactions and reducing the current cost of the KYC process.

5 SHIFT TOWARDS DIGITAL IDENTIFICATION SYSTEMS

The importance of user acceptance and trust was revealed in a recent survey, where users expressed concerns with pairing social media credentials with something as important as their bank account. However, it looks like some social media players have taken this into consideration and are also looking at more secure digital IDs. For instance, Facebook recently acquired a startup for ID verification that allows other companies to verify a user's government-issued identification card.

The UAE Federal Authority for Identity and Citizenship (ICA) also announced the introduction of digital ID software this year. The technology would enable ICA to issue a digital ID for its individual customers by installing software on their smartphones or tablets, facilitating the verification of identities depending on biometric data (fingerprints) and allow them to sign their transactions online.

Other stakeholders such as smartphone manufacturers, MNOs, governments and financial institutions are also shifting towards digital identification systems to provide trust and convenience for citizens using their services.

Without a doubt the more robust trusted digital identity initiatives should involve government, private sector and citizen collaboration to avoid identity data silos, protect and securely store citizens information, allowing them to decide when, who and what information can be shared with the outside world (self-sovereign) and how the private sector can validate such data efficiently, at low or zero cost. Here applications such Identity wallets stored in mobile phones, blockchain and DLT technologies and latest advances in biometrics including spoofing detection will play a major role in the digital identity arena today and in the next coming years.

VISIONTECH
SYSTEMS INTERNATIONAL LLC

Building strong bridges between the islands of Business & IT

Intelligent Managed Services from Visiontech Systems International LLC.

- Data-Driven approach to customize operations & day-to-day support
- Focused to deliver Performance, Security and Business Continuity
- End-to-end Process deployment
- Intelligent Optimization & Technology Transformation
- People experise

Managed Services | IT Infrastructure | Networking | Unified Communication | ELV & Automation

ELV & Automation | Cloud Solutions | Software & Apps | Consultancy and Audit

☎ +9714 3869 786 ✉ sales@visiontechme.com www.visiontechme.com

THE FIRST LINE OF DEFENSE

JESPER ANDERSEN, CEO OF INFOBLOX, EXPLAINS WHY DNS IS THE MOST EXPLOITED NETWORK PROTOCOL AND WHAT COMPANIES SHOULD DO TO MITIGATE THE THREATS.

What exactly is 'actionable network intelligence' that Infoblox is pitching to customers?

Typically, the idea of network intelligence is information you would find from log files. In our case, it is IP addresses and DND queries, which are essential to understanding what is going on in the network, mainly who had what IP address at what point in time, and what applications were they trying to access.

Network intelligence is essentially the history of everything that is going on in the network. And what we have worked hard at is finding ways to make that actionable. In today's world where the network has become a critical business enabler, dumping log files into some kind of analytics system is just not cutting it, especially when it comes to cybersecurity.

I meet with many CISOs, and they tell me, especially in large banks, that they get millions of events in a day and are trying to correlate that information to find out what is most critical. We can help them with the data that we have. For

> ANOTHER DRIVER OF DNS SECURITY IS THE EXTENSION INTO THE CLOUD. IF YOU ARE PUTTING MORE AND MORE APPLICATIONS ON THE CLOUD, YOU NEED AN INFRASTRUCTURE FOR DNS AND DHCP THAT ALLOWS YOU TO EXTEND YOUR NETWORK TO THE CLOUD. ONCE YOU HAVE THAT AUTOMATION AND ENTERPRISE-GRADE INFRASTRUCTURE IN PLACE, YOU NEED TO SECURE IT AND MAKE SURE THAT SOMEONE CAN'T HIJACK THOSE SERVERS.

example, if we see an IP address that is making a query to a domain name that we know is on the blacklist, we could block that and notify the vulnerability scanners in our customers' networks. That is what we mean by actionable network intelligence.

Isn't that similar to sharing threat intelligence?

We have a threat intelligence platform called ActiveTrust, which is used by large organisations across the world to correlate and manage all the threat intelligence they have.

We were the first to launch what is known in the industry today as a DNS firewall. The idea of a DNS firewall is that you look at every domain name you are querying and if it is a bad one, you block it. Initially, we partnered for that threat intel but three years ago, we bought a company called IID, which has now become our ActiveTrust platform. The list of bad domain names changes many times every single day, and you have to manage it actively.

DNS might be the number one threat vector today but isn't DNS security getting a lot better?

There is a lot more attention paid to it now. The issue with old technologies is that there are more ways to protect it, so how do you make it a priority and what can vendors really do? Many things have been written about Cisco Umbrella, Zscaler and Palo Alto Networks in the DNS security space. All of these vendors can do a decent job when you are looking at the public Internet, but they don't know the context of what really went on in the network. When you think of how DNS works in a corporate network, there are all these recursive resolvers all over the world depending on how big is the company. They all recurse up to what is called an internal authoritative DNS server, which is a box that forwards traffic to the public Internet. So the only thing the Cisco Umbrellas of the world sees is the IP address of that box – they don't know which IP address on the network made that query because that is lost in the recursion. We are the only vendor who has that context.

Why should enterprises pay serious attention to DNS security?

With digital transformation initiatives, it has become very apparent to companies that if DNS is down, or DHCP for that matter, nothing works. It is literally like electricity and running water these days - it is a tier 1 network service. Another driver of DNS security is the extension into the cloud. If you are putting more and more applications on the cloud, you need an infrastructure for DNS and DHCP that allows you to extend your network to the cloud. Once you have that automation and enterprise-grade infrastructure in place, you need to secure it and make sure that someone can't hijack those servers.

You may have heard of DNS-based DDoS attacks, but there are more harmful attacks as well. If someone takes over your DNS server, they can redirect traffic to an application server in their control, which means all your customers and partners are logging into the wrong site where their information is compromised. What we did was to create hardened instances for the DNS and control access by other protocols such as FTP and TCP/IP. The next thing we did was to protect DNS infrastructure by calling out bad applications with DNS firewall.

Is DNS in the cloud a good idea?

If you look at how companies are using the cloud today, they are extending their data centres to the cloud. They are moving more applications to the cloud, and they are leveraging cloud-based applications such as Office 365, Salesforce, Workday and others. That means, by definition, they are extending their network as well. Since DNS needs access to all these applications and because latency really matters, your DNS server needs to be near where your applications and users are. It is why you should extend your DNS into the cloud.

THE FUTURE OF DELIVERY

KUSHAL NAHATA, CEO & CO-FOUNDER, FAREYE, ON THE KEY CHALLENGES BRANDS MUST OVERCOME IN LAST MINUTE DELIVERIES

You have a meeting at 3PM and you ordered your food at 1:45PM hoping it would arrive in the next 20 minutes. For some reason, your calculation went wrong and your food arrived at 2:45PM, which doesn't give you as much time as you'd have liked to enjoy a hearty meal. It is our first instinct to go out and tweet about the lousy experience, (not to mention the terrible food). It is a double-edged sword for the brand because if the food also turned out to be bad, it would mean double trouble - what was delivered plus how it was delivered.

If the food was good, it was still trouble because you'd planned it with such robotic precision and the delivery goof-up led you to gobble it up in an orifice-sized time window before your meeting. Let us flip the story a bit and what caused your delay.

Let us face it! Your delivery guy does not take any special efforts to get your package delivered late. In fact, his deliverable is to deliver on time and there are repercussions for delays. However, what are the challenges when it comes to meet delivery timelines? Why is last mile delivery such a challenge for most brands while some brands ace it and set benchmarks for not just competing brands but change the expectations for entire humanity that all industries need to take notice and deliver similar if not better experience to their customers.

Last mile delivery has become quite mainstream yet, the challenges still remain. A seamless last mile delivery experience is still easier said than done and there are some serious challenges that brands encounter time and again. While there are a lot of technology advancements in the logistics space, last mile challenges seem to evolve at a pace which is a tad bit faster compared to the way solutions evolve.

7 key challenges in the context of last mile deliveries

1 Cost - who bears the cost of free deliveries

While 86% customers are currently ready to pay for expedited deliveries, this trend will see a decline as same-day delivery is increasingly becoming the new normal. Same-day/expedited deliveries or normal deliveries, there are two parts to the problem. Expedited deliveries will soon become a basic expectation and brands need to figure out a cost-effective

“SO, IT IS ESSENTIAL THAT YOU HAVE NECESSARY CHECKS AND BALANCES IN PLACE TO ENSURE SEAMLESS COLLABORATION AND COMMUNICATION CHANNELS BETWEEN YOUR AGENTS AND CUSTOMERS.”

way to make this possibility a reality. The problem is with normal deliveries. Usually, normal deliveries do not attract a delivery fee and the customer does not bear the cost of shipping. This means that the brand needs to bear the cost and it can't take too long to deliver these shipments as storing them would shoot up inventory storage/management costs. In either case, there is a cost involved and it is either borne by the vendor or the customer. To balance cost and not compromise on service quality is a challenge in itself.

2 Allocation & Address Issues

In many cases, destination grouping/ management is a serious issue. Many brands allocate jobs manually and that leaves ample scope for human error. Invariably, shipments get mis-allotted or missed out in a particular route.

In addition, there is also the challenge of bad address quality, incorrect addresses, lack of proper signage. These are enough reasons to let the delivery professional go on a never-ending, tediously long and a complex maze.

3 Changing routes dynamically

When it comes to last-mile delivery, there is always a possibility of route changing based on conditions that prevail on that particular day on the ground. This could further complicate the scope of last mile delivery and timeline adherence for order fulfillment. Auto-routing technology has considerably evolved to help delivery companies solve this challenge and achieve efficiency thereby significantly save costs on fuel. However, the ones that are yet to adopt auto-routing solutions are still staring at this major operational issue.

4 Managing delivery density

There is capacity on one side and then there is capability on the other side. To achieve a fine balance between managing the number of deliveries in a day within a particular area is a common challenge you would find in the last mile delivery scenario. This boils down to the following four use cases.

- Low-Density Short Distances
- Low-Density Long Distances
- High-Density Short Distances
- High-Density Long Distances

This is not taking into account the size of shipments, which adds another variable to the mix as to what is the mode of delivery in each of these cases. Thus, the delivery density problem quadruples in magnitude with these permutations and combinations and variables in the picture.

5 Unpredictability in transit

Whether it is an act of God or act of man, if there is one thing you should predict, it is unpredictability. Especially when there is a shipment transit or a delivery in progress, the proverbial Murphy's Law will point and laugh at you, merely seeking acknowledgement. This is beyond control and invariably happens 2/10 times. The least brands can do is to have a communications plan in place so that the delays are communicated to the respective stakeholders in a proactive manner.

6 Availability of customer

Let us say that after crossing the seven mountains and seven seas, the delivery agent reaches the place of delivery. The last thing he wants to greet is a locked door or a guard who wouldn't accept the package and get into all kinds of trouble. Customers are demanding and they generally feel entitled. After all your efforts, if the delivery timeline is missed due to unavailability of a customer, it would still lead to a less-than-delightful experience for the customer and thus mitigate the effect of all your effort in this direction. So, it is essential that you have necessary checks and balances in place to ensure seamless collaboration and communication channels between your agents and customers.

7 Meeting fulfillment timeline

The biggest battle that brands face is adherence to timelines. If the timeline is missed, it could then prove very expensive for brands in both the short and long term. In the case of food deliveries, some companies cannot charge customers for the delivery if the guaranteed timeline is missed. Not just that, it also causes damage in terms of reputation for the brand. Hence, the process of delivery needs to be as robust as possible to help them fulfill orders in a timely manner. This calls for a lot of flexibility and agility in the context of delivery management as a process. There are platforms that can help in this direction solving this specific challenge which essentially manifests itself in several other forms as mentioned in this post.

The Bottomline

These challenges need to be solved at the earliest because the delivery landscape is changing rapidly with advancements such as drone deliveries, delivery robots and driverless vehicles in the picture. These would become part of the mainstream in the blink of an eye and pose an entirely new set of challenges that will be several times more complex than the current ones. It is now the right time to look for technologically feasible, affordable solutions to the current challenges before this game becomes a game of catch-up as these are core challenges affecting both operational efficiency and profitability.

WHY DATA AND ANALYTICS ARE KEY TO DIGITAL TRANSFORMATION

DOUGLAS LANEY, DISTINGUISHED VP ANALYST AT GARTNER, URGES ORGANISATIONS TO BUILD DATA AND ANALYTICS COMPETENCY FOR DIGITAL TRANSFORMATION SUCCESS.

Information as an asset is still in the "early adoption" phase, which makes it a competitive differentiator for leading organisations as they focus on digital transformation. In turn, data and analytics become strategic priorities.

Data and analytics are the key accelerant of an organization's digitization and transformation efforts. Yet today, fewer than 50% of documented corporate strategies mention data and analytics as fundamental components for delivering enterprise value.

Gartner predicts that this will change quickly. By 2022, 90% of corporate strategies will explicitly mention information as a critical enterprise asset and analytics as an essential competency.

A company's ability to compete in the emerging digital economy will require faster-paced, forward-looking decisions. Data and analytics leaders need to assert themselves into corporate strategic planning to ensure that data and analytics competencies are incorporated within the highest-level public-facing enterprise plans."

Amplify the data and analytics discussion

Make data and analytics strategies a routine boardroom discussion topic. Leading organisations in every industry are wielding data and analytics as competitive weapons, operational accelerants and innovation catalysts.

Still, many companies continue to struggle under the weight of traditional business models and analog business process that discount the potential of data and analytics. Others recognise their potential but cannot make the cultural shift or commit to the information management and advanced analytics skills and technology investments necessary to realise that potential.

Strategies to elevate enterprise value

As the role of the chief data officer (CDO) takes hold — gaining authority and influence on par with other executives — organisations will move away from merely using data as a resource and analytics as reporting and decision-making support tools. Data and analytics will become the centerpiece of enterprise strategy, focus and investment.

These are our recommendations aimed at building and elevating an organisation's data and analytics competency within the organisation:

- **Collect and socialize** examples of the internal and external economic benefits from data and analytics that your organisation (or other similar organisations or industries) has generated.

- **Offer or insist** on being involved in corporate strategic planning to ensure that data and analytics competencies are incorporated, if not already featured, within these plans. Communicate this information internally and publicly in annual reports, investor conferences, etc.

- **Measure and communicate** the value of the organisation's information assets to help shift the culture into believing and behaving as if information is an actual asset.

- **Build, buy and borrow** advanced analytics competencies (such as data science or machine learning) beyond traditional business intelligence and embed them throughout the business.

GETTING SECURITY RIGHT

ALAIN PENEL, REGIONAL VICE PRESIDENT- MIDDLE EAST, FORTINET, IDENTIFIES EMERGING SECURITY TRENDS FOR THIS YEAR.

What are some of the cybersecurity trends to watch for this year?
IoT devices remain a focus for cybercriminals with 12 of the top global exploits continuing to target IoT, with IP cameras, printers, TVs, telephony equipment, and routers some of the most commonly targeted devices.

Opensource malware tools such as those made on sharing sites such as GitHub are available to anyone, so cybercriminals also access them for nefarious activities, such as evolving and weaponising them into new threats, especially ransomware.

At the same time, developments in steganography are bringing new life into an old attack type. Steganography is typically not used in high-frequency threats, although the botnet Vawtrak made the list of "bursty" botnets.

Adware Infiltration is another trend that should be on the radar of all security practitioners. Adware continues to be a threat and not just a nuisance. Globally, adware sits at the top of the list of malware infections for most regions. With adware found to be in published apps, this attack type can pose a serious threat especially to unsuspecting mobile device users.

What are the essential cybersecurity technologies enterprises should invest in?
In today's meshed and increasingly perimeterless networks, security teams need to be able to identify everything connected to their ecosystem. As enterprise networks become more distributed, SD-WAN will become the preferred networking choice to ensure performance along with essential agility and simplicity for critical business applications. The rapid migration to the cloud also means its introducing complexities and risks that few organisations are adequately prepared for – this will drive the need for cloud security solutions.

What advice would you give to organisations in the region to stay secure?
Apart from maintaining security hygiene and following best practices, we highly recommend that organisations invest in threat intelligence services to help them focus on the most pressing security matters of the day, along with new security controls and processes that enable them to share, correlate, and respond to threats in a coordinated fashion and at digital speeds.

What are you showcasing at GISEC 2019?
During GISEC our aim is to help organisations address new threat opportunities that are being created by the convergence of cybsercurity and physical spaces or Cy-Phy. We are showcasing our latest security innovations that will help companies combat threats associated with Cy-Phy. We will also showcase the Fortinet Security Fabric, in addition to the FortiGate Secure SD-WAN, and OT security solutions.

> “DURING GISEC OUR AIM IS TO HELP ORGANISATIONS ADDRESS NEW THREAT OPPORTUNITIES THAT ARE BEING CREATED BY THE CONVERGENCE OF CYBSERCURITY AND PHYSICAL SPACES OR CY-PHY. WE ARE SHOWCASING OUR LATEST SECURITY INNOVATIONS THAT WILL HELP COMPANIES COMBAT THREATS ASSOCIATED WITH CY-PHY.”

6 REASONS WHY DATA BACKUPS ARE IMPORTANT

BY GIRIDHARA RAAM M, MARKETING ANALYST, MANAGEENGINE

The increase in ransomware attacks and high-profile data breaches over the last few years has reinforced the importance of data security. Recent research indicates that an average of 2,244 cyberattacks happen globally each day, and many of these attacks are targeting sensitive business data. Large enterprises are clear treasure troves of data in the eyes of hackers, but small and medium-sized businesses (SMBs) are often targeted as well. Businesses are becoming more dependent on data in the 21st century, which means the demand for data security is increasing.

However, data security isn't just about protecting data from malicious outsiders; remediation is a critical aspect of data security. While you can't predict when data loss will happen, you can make sure your business has the right solutions to recover its critical data. IT managers are responsible for implementing the right data backup and disaster recovery procedures in their businesses. Mentioned below are a few reasons why your business needs to perform data backups and implement a disaster recovery solution:

> “WHILE YOU CAN'T PREDICT WHEN DATA LOSS WILL HAPPEN, YOU CAN MAKE SURE YOUR BUSINESS HAS THE RIGHT SOLUTIONS TO RECOVER ITS CRITICAL DATA. IT MANAGERS ARE RESPONSIBLE FOR IMPLEMENTING THE RIGHT DATA BACKUP AND DISASTER RECOVERY PROCEDURES IN THEIR BUSINESSES.”

1 Preventive measures don't always work

Businesses should take a proactive approach to cybersecurity by equipping themselves with network security solutions, strong firewall configurations, and patch management tools, but they also need solutions for mitigating data loss. SMBs are clearly not immune to having their data stolen or encrypted by ransomware, but according to research by Nationwide Insurance, 68 percent of SMBs don't have a disaster recovery plan. Every organisation, big or small, needs to have a plan for mitigating the aftermath of natural disasters, server downtime, and other complex situations.

2 Cyberattacks are constantly evolving

According to a CNN report,

the average small business hit with ransomware in 2017 lost over $100,000 due to downtime. What's more, these businesses struggled to recover their encrypted data, if they were able to recover it at all. Ransomware is just the tip of the iceberg in terms of cyberattacks; malware, DDoS attacks, data breaches, supply chain attacks, and zero-day exploits are a constant threat.

These cyberattacks usually target sensitive business information stored in the cloud or on-premises. The frequency of cyberattacks has increased thanks to digital transformation, which has become a key driver for businesses in every industry. Businesses today are seeing a massive influx of data for every activity from lead generation to customer conversion, and attackers are ready to capitalise on this steady stream of data.

3 Natural disasters can halt business in an instant

According to Clutch, 60 percent of small businesses that lose their data will shut down within six months. Although data can be lost in many ways, you should never underestimate the occurrence of catastrophic natural disasters. Regardless of your business' size, you need to prepare for storms, earthquakes, fires, and any other natural disaster that could shut down your servers and data centers.

4 Lost data hurts your brand's reputation

According to a study by Small Business Trends, 58 percent of businesses don't have a backup plan for data loss. What businesses need to consider is that, in addition to the above points, data loss leads to a loss of customer trust. Being known as a company that has lost data, especially customer information, won't do your business any favors. In fact, having a poor reputation will likely lose you customers and may impact your organisation's productivity since new employees might hesitate to join your company.

5 Cloud computing demands additional backups

Moving your on-premises operations to the cloud can save your business money and reduce its management efforts, but the cloud isn't without its risks. When businesses store their corporate data on the cloud, they're placing the security of that data into the hands of the cloud provider.

6 Insider threats are often unseen

You never know whether one of your employees will pose a threat to your business' data. A disgruntled employee could easily steal or erase business-critical data if you don't have proper security controls in place. According to a survey by CA Technologies, 56 percent of cybersecurity professionals say regular employees pose the biggest security threat to organisations, with excessive access privileges being the main enabler of insider attacks.

Having proactive data backup procedures in place can add additional security for your business. It also allows you to handle any unforeseen data loss situations, keeping your productivity and brand stable. Since data loss can happen at any time and in a multitude of ways, just making backups is a good place to start. However, keeping consistent backups is the key. If a disaster strikes and your last backup is six months old, your business will have a hard time recovering. Likewise, your data backup plan should be coupled with a disaster recovery plan. This will give you an extra hand when you need to restore your failed devices as quickly as possible. Your corporate data management procedures should include software that automatically creates backups and makes restoring from different backup versions as easy as possible.

Additionally, the 3-2-1 rule is often recommended for maintaining backups: keep three total copies of your data, in two different mediums, with one copy stored off-site. Maintaining physical backups even if you use cloud storage is advised in case your cloud provider experiences downtime or faces a breach.

Best practices for data security

When it comes to databases in particular, here are a few security best practices that could help your business fight against database takedowns and breaches:

- Define strong password policies.
- Remove stale user accounts.
- Change the default username for admins.
- Restrict user privileges.
- Encrypt sensitive business data.
- Keep applications and firmware up-to-date.

Special note should be placed on that last point. According to Gartner's predictions, 99 percent of vulnerabilities exploited by 2020 will continue to be the ones that security and IT professionals have known about for at least one year. This extends beyond just databases and is something to keep in mind for all data storage operations.

Lastly, you need to audit employee login and logoff behaviour, manage USB connections, and provide employees with only the minimal amount of privileges needed for them to complete their work. You don't want to have an air-tight storage and recovery plan unraveled by a malicious insider or an irreversible mistake. ◤

REWRITING THE RULES

PERRINE JOUAN, MARKETING DIRECTOR - EMEA & APAC, SENTINELONE, HIGHLIGHTS WHY SIGNATURE-BASED TRADITIONAL SECURITY TOOLS ARE NOT ADEQUATE FOR ENDPOINT PROTECTION TODAY.

What are some of the broad industry trends in endpoint protection today?
Endpoint protection measures must evolve beyond signatures and static file analysis. Many solutions on the market today still heavily rely on signatures; these are typically legacy AV products. Signatures are ill-equipped to handle the rapidly changing threat landscape. Many next-gen solutions rely on static file analysis or AI to replace signatures. This is a much more effective and resilient approach to handling threats that present themselves in files, however, the threat trend we're seeing is a marked increase in fileless malware. These are attacks in which no malware exists in a file, and the payload is delivered via another mechanism such as a script. SentinelOne's proprietary behavioral AI technology is vector agnostic and extremely effective in blocking everything from garden variety malware to fileless attacks and even sophisticated nation-grade attacks.

Also, endpoint protection tools must be deployable. What good is buying a tool that is impossible to deploy or requires too many man-hours to manage? We see two phenomena appearing on the endpoint scene: Products that have noticeably low efficacy rates and products which are constantly throwing up too many false positives. What's the point of deploying endpoint protection if malware is constantly raiding systems? If the endpoint protection is flagging benign programs as malware, too much time and end user pain is part of the process. SentinelOne couples the industry's highest efficacy rates (as proven in testing and a variety of third parties such as NSS) with the lowest false positive rates, both online and offline. Testing in-production, both online and offline, is critical to experiencing a solution's deployment readiness in your enterprise.

Another key trend is the convergence of EPP and EDR. The notion that protection and visibility/response should require separate tools is flawed. We see customers desiring solutions that let them leverage intelligent automation to prevent, detect, and even respond to threats (if needed) in real-time. Endpoint protection requires a multilayered approach. While other vendors have preached "prevention only" approaches or focused on manual response measures, SentinelOne built a single code base which starts with visibility to prevent malware pre-execution while preserving forensic integrity to allow for both automated remediation or manual response if so desired, pre-execution.

When can we expect endpoint security to be automated with AI and Machine Learning?
That's exactly what we've done. We use machine learning to power our static file analysis and behavioral AI that's embedded in our agents. The decisions made by these technologies without the help of humans enable autonomous response - this is how we're disrupting the EPP (protection) and EDR (visibility/response) markets. Humans will always remain a critical part of cybersecurity programs: intelligent software helps humans scale and make better decisions.

Will endpoint protection platforms replace traditional anti-virus software?
Yes, we see this trend very clearly happening: while legacy AV still has significant market share, newer technologies that enable higher levels of protection and more capabilities are replacing legacy AV each and every day. 80% of our business is AV replacements, many of which are extremely high profile. We've already replaced legacy AV in thousands of accounts - particularly in 3 of the Fortune 10. The market is seeking a solution to a business problem that saves them time; cyber professionals across the globe are looking for highly effective, easily deployable, and fully integrable solutions. These are the key reasons customers choose SentinelOne to replace their legacy AV each and every day.

Next Generation Security Intelligence Solutions

QRadar®

Product: QRadar
Security Information and Event Management

Service:
SIEM, Alerts to accelerates incident analysis and remediation

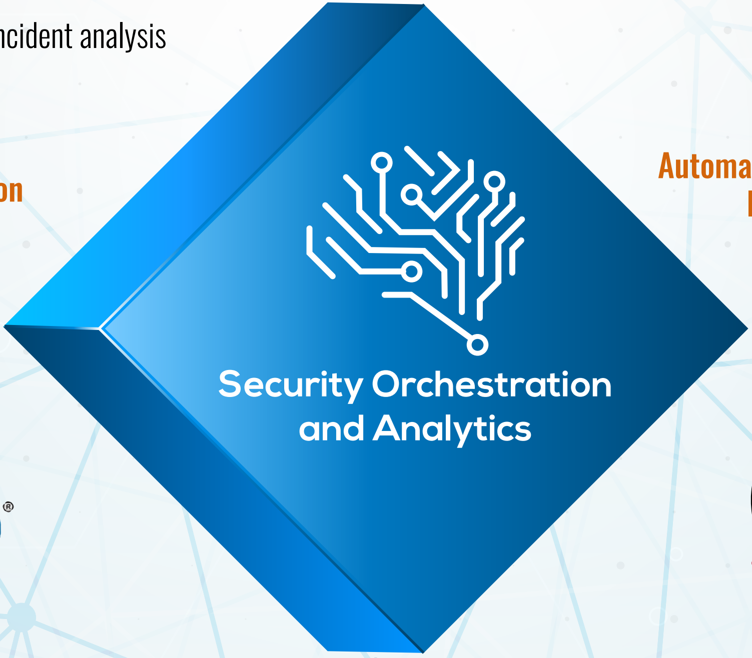
Comprehensive Visibility
Real Time Threat Detection

Resilient
an IBM Company

Product: Resilient
Incident Response Platform

Service:
Incident Response

Automated Response Mechanism
Improve SOC Productivity



MaaS360®

Product: MaaS360

Service:
Mobile Device Management

Transaction protection
Device management
Content security

Guardium®
SAFEGUARDING DATABASES™

Product: Guardium,
Multi-cloud Encryption, Key Manager

Service:
Critical Data Protection Service

Data Protection
Data Access Control

★ **BEST IT SECURITY SYSTEM INTEGRATOR AWARD 2018 - (6 YEARS CONSECUTIVELY)** ★

NANJGEL SOLUTIONS
▷ DETECTION ▷ PREVENTION ▷ REMEDIATION

IBM Silver Business Partner ™

☎ +971 44428910 ✉ sales@nanjgel.com www.nanjgel.com

#2204, Shatha Towers, Dubai Internet City, P.O.Box: 500804,Dubai, UAE.

GISEC
GULF INFORMATION SECURITY EXPO & CONFERENCE
معرض و مؤتمر الخليج لأمن المعلومات

1–3
April 2019
World Trade Centre

MEET US @ | HALL NO 8 B-16A

TOP 7 SECURITY AND RISK MANAGEMENT TRENDS

GARTNER IDENTIFIES SEVEN EMERGING SECURITY AND RISK MANAGEMENT TRENDS THAT WILL IMPACT SECURITY, PRIVACY AND RISK LEADERS IN THE LONGER TERM.

Gartner defines "top" trends as ongoing strategic shifts in the security ecosystem that are not yet widely recognised, but are expected to have broad industry impact and significant potential for disruption.

"External factors and security-specific threats are converging to influence the overall security and risk landscape, so leaders in the space must properly prepare to improve resilience and support business objectives," says Peter Firstbrook , research vice president at Gartner.

The top seven security and risk management trends for 2019 and beyond are:

Trend no. 1: Risk appetite statements are becoming linked to business outcomes

As IT strategies become more closely aligned with business goals, the ability for security and risk management (SRM) leaders to effectively present security matters to key business decision makers gains importance. "To avoid exclusively focusing on issues related to IT-decision making, create simple, practical and pragmatic risk appetite statements that are linked to business goals and relevant to board-level decisions," says Firstbrook. "This leaves no room for business leaders to be confused as to why security leaders were even present at strategic meetings."

Trend No. 2: Security Operations Centers are being implemented with a focus on threat detection and response

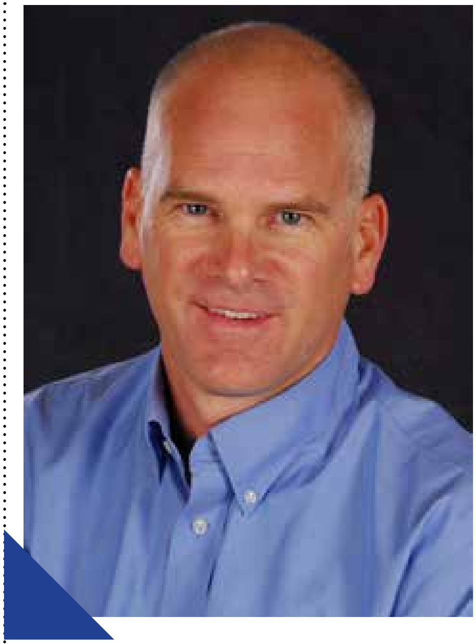
The shift in security investments from threat prevention to threat detection requires an investment in security operations centers (SOCs) as the complexity and frequency of security alerts grow. According to Gartner, by 2022, 50 per cent of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence and threat-hunting capabilities, up from less than 10 percent in 2015. "The need for SRM leaders to build or outsource a SOC that integrates threat intelligence, consolidates security alerts and automates response cannot be overstated," says Firstbrook.

Trend No. 3: Data security governance frameworks will prioritise data security investments

Data security is a complex issue that cannot be solved without a strong understanding of the data itself, the context in which the data is created and used, and how it is subject to regulation. Rather than acquiring data protection products and trying to adapt them to suit the business need, leading organisations are starting to address data security through a data security governance framework (DSGF). "DSGF provides a data-centric blueprint that identifies and classifies data assets and defines data security policies. This then is used to select technologies to minimise risk," says Firstbrook. "The key in addressing data security is to start from the business risk it addresses, rather than from acquiring technology first, as too many companies do."

Trend No. 4: Password-less authentication is achieving market traction

Password-less authentication, such as Touch ID on smartphones, is starting to achieve real market traction. The technology is being increasingly deployed in enterprise applications for consumers and employees, as there is ample supply and demand for it. "In an effort to combat hackers who target passwords to access cloud-based applications, password-less methods that associate users to their devices offer increased security and usability, which is a rare win/win for security," says Firstbrook.



Trend No. 5: Security product vendors are increasingly offering premium skills and training services

The number of unfilled cybersecurity roles is expected to grow from 1 million in 2018 to 1.5 million by the end of 2020, according to Gartner. While advancements in artificial intelligence and automation certainly reduce the need for humans to analyze standard security alerts, sensitive and complex alerts require the human eye. "We are starting to see vendors offer solutions that are a fusion of products and operational services to accelerate product adoption. Services range from full management to partial support aimed at improving administrators' skill levels and reducing the daily workload," says Firstbrook.

Trend No. 6: Investments being made in cloud security competencies as a mainstream computing platform

The shift to cloud means stretching security teams thin, as talent may be unavailable and organisations are simply not prepared for it. Gartner estimates that the majority of cloud security failures will be the fault of the customers through 2023. "Public cloud is a secure and viable option for many organisations, but keeping it secure is a shared responsibility," says Firstbrook. "Organisations must invest in security skills and governance tools that build the necessary knowledge base to keep up with the rapid pace of cloud development and innovation."

> "RATHER THAN ACQUIRING DATA PROTECTION PRODUCTS AND TRYING TO ADAPT THEM TO SUIT THE BUSINESS NEED, LEADING ORGANISATIONS ARE STARTING TO ADDRESS DATA SECURITY THROUGH A DATA SECURITY GOVERNANCE FRAMEWORK (DSGF)."

Trend No. 7: Increasing presence of Gartner's CARTA in traditional security markets

Gartner's continuous adaptive risk and trust assessment (CARTA) is a strategy for dealing with the ambiguity of digital business trust assessments. "Even though it's a multiyear journey, the idea behind CARTA is a strategic approach to security that balances security friction with transaction risk. A key component to CARTA is to continuously assess risk and trust even after access is extended," says Firstbrook. "Email and network security are two examples of security domains that are moving toward a CARTA approach as solutions increasingly focus on detecting anomalies even after users and devices are authenticated."

CYBERSECURITY TRENDS IN 2019

FADY YOUNES, CYBERSECURITY DIRECTOR, MIDDLE EAST AND AFRICA, CISCO, REVEALS THE TOP FIVE THREATS TO WATCH OUT FOR.

With hackers becoming far more sophisticated in their attacks, they are now able to remain undetected for longer periods of time and extract valuable data.

Cisco's 2018 Security Capabilities Benchmark Study found that in MEA, an alarming 94% of companies admitted to experiencing cyberattacks in the past year. In order to address this, there needs to be an increased focus on cybersecurity. However, 25% of organisations in MEA lack the appropriate personnel to deal with such matters.

This is often one of the biggest obstacles to remaining secure, which is why it crucial to decrease the skills gap, increase awareness and train staff to address such threats. The damages incurred from a lack of planning can stem beyond financial issues and affect public opinion also. It is therefore in the interest of businessowners to consider how they can make their organisations more secure, to aid sustainable growth.

For over a decade, Cisco's cybersecurity reports have helped provide detailed accounts of the threat landscape to educate businesses on the importance of protecting their infrastructure.

Cisco's 2019 Threat Report identifies 5 key trends to be aware of:

1 Emotet

As a banking trojan and malware program, Emotet injects a particular code into a computer, allowing it to obtain sensitive data, such as financial information. The dangers of Emotet truly drive home how easy it is to experience a cyberattack. Emotet malware can come from something as simple as opening a malicious document or URL link within an email. Therefore, education on this matter is crucial.

2 VPNFilter

VPNFilter is a malware designed to infect routers and network attached storage devices. In May 2018, an estimated 500,000 routers were infected globally, a number which has surely grown since. VPNFilter can obtain data and also contains a 'kill switch', which is designed to disable the infected router on command. It can persist, irrespective of whether the user reboots their router.

3 Cryptomining

Cryptomining malware or 'cryptojacking' are relatively new terms which refers to software and malware developed to take over a computer's resources and use them for cryptocurrency mining – without a user's permission. Revenue generation is the key motivation for these attackers. They have grown to become the most common threat in this category, due to the repeat revenue they offer and the low risk if caught.

4 Unauthorised Mobile Device Management

Hackers can abuse mobile device management protocol to deliver malware. They work by bypassing the restrictions for app deployment and tricking users into installing a malicious configuration profile – something as simple as an update for VPN, Wi-Fi or email settings. They then pose as application updates which a user may already be expecting to receive. Even if the user declines the update, the update will continue to pester with multiple requests. This can essentially prevent the user from doing anything on the device until they agree to install the app.

5 The Olympic Destroyer

As an advanced threat, The Olympic Destroyer was a cyber-sabotage attack which spread a destructive network worm, targeting the organizers, suppliers and partners of the 2018 Winter Olympic Games in PyeongChang, South Korea. The breach was preceded by reconnaissance and infiltration into target networks, to select the ideal springboard for the self-replicating and self-modifying destructive malware. Since the Winter Olympics, there have been reports of similar activity and we expect this threat to continue to test organisations this year.

Cisco recognises that it is virtually impossible to know of every threat that we will encounter over the year. However, by considering past cases and monitoring current trends, we can create a relatively accurate picture of the current climate and consider how to equip ourselves with the right tools to remain secure. Addressing such threats at an early can free up time to deal with the unexpected and zero-day attacks.

INDUSTRY 4.0

BREAKFAST SESSION WITH THE ORIGINATOR

2019, APRIL 10
8:00AM - 11:00AM

ROCKSWATERS

EXCLUSIVE
CxO ROUND TABLE
YAS HOTEL , ABU DHABI

SPEAKER

HENRIK VON SCHEEL

A LEADER OF INDUSTRY 4.0

MORE INFO : 055 835 4770 WEBSITE : WWW.ROCKSWATERS.COM

Look Back to Move Forward

Have CISOs become better or worse over the last year? We picked three areas that were hot-button topics last year and graded you according to your responses this year.

	You Said 2018	You Say 2019	We want to know more because...
Technology			
Machine learning (ML) To what degree are you reliant on ML to reduce the level of effort required to secure the organization?	77%	↓67%	If anything, the negative trends in these first three questions probably stem from uncertainty and lack of confidence. Or that ML is not ready for prime time. Either way, we'd like to know more.
Artificial intelligence (AI) To what degree are you reliant on AI to reduce the level of effort required to secure the organization?	74%	↓66%	It could be that adoption is so widespread and integrated into your business processes that you don't feel it worth calling out.
Automation To what degree are you reliant on automation to reduce the level of effort required to secure the organization?	83%	↓75%	It's possible that you chose not to be "reliant," yet selectively automate. Even the largest organizations may not fully embrace automation.
Cost of a breach			
Thinking of the most impactful breach you experienced in the past year, what was the total cost?	8% said $5M+	8% said $5M+	Breaches remain a drain on resources and their impact is more than just financial.
	<$500K 47%	<$500K ↑51%	More than 50% of you are driving breach costs below half a million; excellent. Costs are down a little, or at least under control.
What improvements were made to better protect your company from security breaches?			
Separating IT and security functions	38%	↓35%	This is a controversial topic and the lack of a huge swing suggests you're equally divided as a group.
Increasing security awareness and training for employees	38%	↑39%	As long as people remain the weakest link, it remains an unknown just how much training is enough.
Implemented risk mitigation techniques	37%	↑39%	When you consider that this year, 20% of respondents claimed not to be very knowledgeable about risk and compliance, risk frameworks become standard operating procedure.
Increased investment in security defense technologies or solutions	41%	↑44%	Good, if paired with training and outcome-based measurement. Good for security metrics.
Cloud			
Moving security to the cloud has increased our efficiency, allowing our security personnel to focus on other areas	92% agree	↑93%	Continued adoption of cloud for the right reasons.
Leveraging cloud security solutions allows us to be more effective than operating with on-premises	91% agree	↑93%	A slight rise in cloud security confidence? We'll take it!
How challenging is it to defend cloud infrastructure from cyber-attacks	55% very	↓52%	A bigger drop in difficulty protecting cloud infrastructure? Even better!

Source: Cisco 2019 CISO Benchmark Study

Aruba names new hospitality business development manager

Aruba, a Hewlett Packard Enterprise company, has named Youssef Senhaji Rhazi as regional hospitality business development manager for Middle East, Turkey and Africa. In this new role, Youssef is responsible for developing and executing strategies to expand Aruba's customer base in the hospitality sector.

Youssef has over 18 years of experience in the ICT Industry, specialising in telecommunications and networking. He brings strong technical knowledge in the hospitality space, commercial acumen and analytical ability, excellent communication skills and the ability to build trusted relationships at all levels.

"When it comes to understanding hospitality customers, meeting their needs and winning their loyalty, we no longer have a choice. Customer obsession means not only focusing on customers, but providing them with what they demand. Customers expect us to be watching them, gathering data on their preferences – and providing them with personalized services right here, right now. Technology is critical to the hotel guest by keeping them engaged. But expectations have shifted and what was once considered surprise and delight has become now expected and assumed. Hotels need to keep up with these expectations. Aruba solutions can help meet guest expectations while delighting them and providing them with personalised and meaningful engagement." said Rhazi.

Eaton appoints new GM for Middle East

Power management company Eaton has appointed Ashraf Yehia as general manager, Middle East, with responsibility for the company's operational and commercial business across the region. He will replace Frank Ackland with immediate effect and will report directly to Tim Darkes, senior vice president & general manager PQED EMEA and Emerging Markets.

Ashraf began his career with Cooper Industries as Regional Sales Manager in 2004. In 2011 he became General Manager, Cooper Industries' Crouse-Hinds & B-Line businesses where he oversaw regional operations and strategy. Ashraf joined the Eaton team in 2012 as part of the company's acquisition of Cooper Industries. Ashraf holds an Engineering degree from Ain Shams University in Cairo, Egypt.

"The Middle East is one of the most dynamic, vibrant and growing regions. Eaton's power management expertise and growth ambitions are closely aligned with those of its customers in the oil and gas, utility, construction and data center industries in the Middle East. I have seen at close quarters how Eaton has established itself in the region over the years and I aim on continuing to increase the organisation's footprint and success in the region," said Ashraf Yehia.

Ericsson announces changes in management team

Ericsson has announced that Rafiah Ibrahim will leave her position as Senior Vice President and Head of Market Area Middle East and Africa and will take on a role as advisor to CEO Börje Ekholm. Rafiah Ibrahim, who has held her current position since April 01, 2017, will assume her new role effective August 31, 2019. She will leave the Ericsson Executive Team effective the same date.

Börje Ekholm, President and CEO, said: "Rafiah has been a very important leader in our sales and delivery organization. In her latest assignment she successfully led the merger of two important markets, Middle East & Africa, increasing customer value and securing scale and efficiency as well as implementing a robust operational structure. In addition, Rafiah has built strong customer relationships across the region not least visible in the recently announced 5G contracts [LINK]. Rafiah has been a valued member of the Executive Team and I look forward to continuing to work with her in her new role."

Rafiah Ibrahim joined Ericsson in 1996 and have held various managerial positions across the organization, the last five as head of a region. She will stay fully committed to driving the regional agenda forward until assuming her new position and transiting into an advisory role with focus on building strong customer relationships.

A recruitment process has been initiated to appoint a successor.

OFFICIAL GOVERNMENT CYBER SECURITY PARTNER

DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY

دبي الذكية SMART DUBAI

شرطة دبي DUBAI POLICE

# GISEC

GULF INFORMATION SECURITY EXPO & CONFERENCE

معـرض و مـؤتـمـر الـخـلـيـج لأمـن الـمـعـلـومـات

ioTx

THE WORLD'S MOST FAMOUS HACKER AND EX-#1 ON THE FBI'S MOST WANTED LIST TO HACK LIVE IN DUBAI

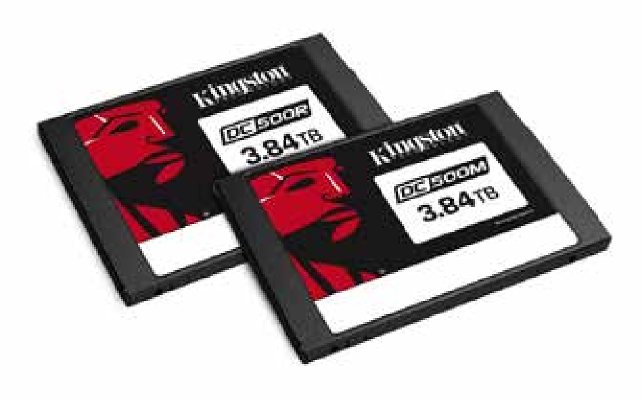
See the jaw-dropping
live hack by **KEVIN MITNICK**
for as little as AED 1,999.

#GISEC

www.gisec.ae I gisec@dwtc.com I +971 4 308 6805

OFFICIALLY SUPPORTED BY	STRATEGIC PARTNERS	IOT PARTNER	PLATINUM SPONSOR	DIAMOND SPONSOR
DUBAI ELECTRONIC SECURITY CENTER شرطة دبي DUBAI POLICE دبي الذكية SMART DUBAI	SPIRE INFORMATION SECURED Carbon Black. Recorded Future	vodafone business	proofpoint.	FireEye

GOLD SPONSORS	POWERED BY	CO-LOCATED WITH	ORGANISED BY
CREDENCE SECURITY CROWDSTRIKE KnowBe4 Human error. Conquered. SentinelOne	GITEX TECHNOLOGY WEEK	FUTURE BLOCKCHAIN SUMMIT قمة مستقبل البلوك تشين	مركز دبي التجاري العالمي DUBAI WORLD TRADE CENTRE



KINGSTON ENTERPRISE SSD

Kingston Digital Europe has launched its new Data Center 500 Series Enterprise SSDs. DC500R is optimized for read-intensive applications while DC500M is optimized for mixed-use workloads. Both SSDs in the DC500 Series implement Kingston's strict Quality of Service (QoS) requirements to ensure predictable random I/O performance as well as predictable low latencies over a wide range of read and write workloads.

DC500R is ideal for read-intensive applications such as boot up, web servers, virtual desktop infrastructure, operational databases and real-time analytics. Cloud service providers and software-defined storage architects can leverage the drive's consistent I/O and latency performance to deliver the QoS needed in demanding read-centric environments. At .5 DWPD (drive writes per day), DC500R allows IT administrators to maximise their investment in storage hardware with a drive that delivers on performance, endurance and reliability.

XIAOMI MI9

Mi 9 is Xiaomi's first flagship with an AI triple camera, with the main camera utilising the latest 48-megapixel Sony IMX586 1/2" sensor. Users can choose to shoot high-resolution 48-megapixel images, or in low-light conditions, take even clearer and brighter photos as Mi 9 will combine four pixels to one, resulting in very sensitive 1.6μm large pixels. The AI triple camera combination of the main camera, 16-megapixel ultra wide-angle camera, and a 12-megapixel telephoto camera gave Mi 9 a score of 107 by the authoritative DxOMark website, giving it the second highest score of all tested smartphones. In addition, a video score of 99 puts it at number one on DxOMark for video capture.

Mi 9 has an all-curved back cover design, allowing it to fit comfortably in the hand. An advanced back cover color process gives Mi 9 a stylish holographic rainbow spectrum, so it looks different every time it is picked up. Inside the Mi 9 is a large 3300mAh battery, featuring a fast charging solution for both wired and wireless charging. This solution has received certification from renowned German institution TUV Rheinland for safe quick charging.The 27W wired charging supports Qualcomm's QC4+ standard, and enables Mi 9 to safely charge to 70% in just 30 minutes, and fully charge in 60 mins.

CANON ZOEMINI

Canon Middle East has launched two instant camera printers, the Canon Zoemini S and Canon Zoemini C.

The Canon Zoemini S is ideal for those wanting to capture, print and share their holiday adventures, a spontaneous selfie, photos with friends or an Instagram-worthy plate of food. Consisting of an eight-megapixel camera, front-mounted mirror, ring-light and remote shutter capability, the Canon Zoemini S is easy to use and will ensure its users are ready to take the perfect selfie in an instant. The Canon Zoemini S comes in three stylish finishes; rose gold, matte black and pearl white and fits seamlessly into the palm of a hand, pocket or backpack for exceptional portability.

For those seeking a streamlined version of the Canon Zoemini S, the Canon Zoemini C is available without the Canon Mini Print App compatibility and packs a five-megapixel camera, a selfie supporting reflective mirror and a Micro SD card slot. The Canon Zoemini C is available in four eye-catching colours; bubble gum pink, bumblebee yellow, mint green and seaside blue for instant keepsakes on the go.

LOOKING INTO THE FUTURE

SUNIL PAUL, COO AND CO-FOUNDER OF FINESSE, ON WHY TRANSLATING DATA INTO FORESIGHT IS A BUSINESS IMPERATIVE TODAY.

Can present and past experiences provide a window into the future? It is an open debate on the individual front but not so much for businesses as predictive analytics holds the alluring promise of visibility and predictability into what will happen in the future.

If we consider the exponential growth in devices connected to the Internet of Things (IoT), with estimates ranging from 20 million by 2020, according to Gartner and 25 million by 2025, according to GSMA Intelligence, predicting the future could only get better. In fact, greater availability of data, storage and computing power has helped bring predictive analytics into the mainstream from its high-perch a decade or so ago.

Machine learning, data mining, artificial intelligence and predictive modelling constitute the core elements of predictive analytics solutions. An example of predictive analytics at work in our daily lives is perhaps weather forecasting, where current and past data are used to predict the weather for the days ahead. But for businesses, its advantage lies in identifying trends, understanding customers, improving business performance and driving strategic decision making. It wouldn't be incorrect to state that predictive analytics could be used produce deeper insights to drive specific business outcomes.

> **“AN EXAMPLE OF PREDICTIVE ANALYTICS AT WORK IN OUR DAILY LIVES IS PERHAPS WEATHER FORECASTING, WHERE CURRENT AND PAST DATA ARE USED TO PREDICT THE WEATHER FOR THE DAYS AHEAD. BUT FOR BUSINESSES, ITS ADVANTAGE LIES IN IDENTIFYING TRENDS, UNDERSTANDING CUSTOMERS, IMPROVING BUSINESS PERFORMANCE AND DRIVING STRATEGIC DECISION MAKING.”**

Predictive analytics is being employed across varied industry verticals, businesses and functions. In manufacturing, for example, firms are using predictive analytics to achieve better inventory control by track stock levels using IoT and automating the replenishment process. In fact, in asset-heavy industries like oil and gas or power generation, the power of predictive analytics is being harnessed to service components and equipment based on their actual performance instead of time-based schedule. In healthcare, there are opportunities to use predictive analytics to improve patient care to better hospital management. The telecom industry was one of the first verticals to use predictive analytics for applications ranging from predicting consumer churn to managing network assets. In the insurance industry, predictive analytics is being used not only to control risks in underwriting but also detect insurance fraud claims.

To get started on predictive analytics, the fundamental requirement is data availability. In fact, the maxim is more data you have, the better. And more accurate the data, more accurate are the predictive models and their predictions. This data can be from both sources that are internal and external to the company. There is also the question of whether to hire data scientists to build predictive models in-house or use external providers, which is a decision best left to the company's leadership.

However, do remember that it is easy to become enamoured with predictive analytics, so much so that making predictions purely for the sake of predicting the future could become a habit with zero benefits. As predictive analytics solutions get more and more accurate, and competitors scramble to get on board, the challenge would be to act on those predictions, and act quickly enough.

Remember, predicting the future is useful only when that data and information can be transferred into action before your competitors beat you to it. ◤

POWEREDGE

TRANSFORMATION WITHOUT COMPROMISE

Explore the potential of the next generation of the Dell EMC PowerEdge server portfolio powered by the latest Intel® Xeon® processors

DESIGNED TO POWER TRANSFORMATION

The most cutting-edge portfolio of Dell EMC PowerEdge servers, featuring the next generation Intel® Xeon® Processor Family yet is designed to help customers to drive IT transformation. And it has the power to transform your business too.

There are loads of business-boosting features to help you win new orders and help your customers bridge the IT resources gap and transform their business:

> Scalable business architecture
On-demand capacity & performance to meet every core challenge

> Intelligent automation
Enhanced server room efficiency and embedded diagnostics – no more amber light patrols

> Integrated security
Built-in IT lifecycle protection and security embedded into hardware and firmware

SUPPORTED BY: Extraordinary new Partner Program
Take a no-compromise approach to building your business by leveraging the potential of the best server platform and the best Partner Program in the industry.

Discover the difference – visit **www.storit.ae**

StorIT
Harnessing the value of information

PO Box 17417 Jebel Ali Freezone Dubai, United Arab Emirates
Tel: +971.4.881.9690 | info@storit.ae | www.storit.ae

DELLEMC
PARTNER
AUTHORIZED DISTRIBUTOR

Increasing Security Without Additional Complexity

Today's cyber security solutions must be effective against the most complex attacks without adding complexity.

The Fortinet Security Fabric integrates multiple security technologies into a seamless architecture delivering increased security capabilities and reduced complexity.

FORTINET

www.fortinet.com