WWW.TAHAWULTECH.COM

ADVISOR

FERAS AL JABI

ON HOW ATC AND DIGITAL OKTA CAN TRANSFORM YOUR DIGITAL VISION INTO REALITY



MIDDLE EAST

PREVIEW: BICSI EMEA CONFERENCE

HACKING THE SKILLS GAP

INTERVIEW: BOSCH'S HAKAN OZYIGIT

NANGATING HEDGENEER

CUTT

computer news middle east



Dark Fighter

DON'T BE LEFT IN THE DARK!

Hikvision DarkFighterX Network Cameras

Ultra low illumination

4 MP / 2 MP DarkFighterX 0.0005 lux illumination

25x / 35x / 45x Optical

Large Zoom

Hardware

Advanced

Zoom

Dual 1/1.8" Sensors



Hikvision Middle East & North Africa Office: 52nd floor, Almas Tower, Jumeirah Lakes Towers, Dubai, UAE T: +971-4-4432090 F: +971-4-8816057 salesme@hikvision.com

CONTENTS







How ATC and Digital Okta enable seamless and secure cloud transformation

8

MOVERS AND SHAKERS

The latest people movement in the regional security industry

20 WINNING IN THE CYBER BATTLEGROUND Why Gulf states need to boost their collaboration with private enterprises to win the fight against cybercriminals

24 HACKING THE SKILLS GAP Should organisations look into recr

Should organisations look into recruiting hackers to address the skills gap?

27 ROUGH SEAS

Industry experts share insights into the cyber risks and threats in the maritime sector

30 REVIEW We took Ri

We took Ring's first indoor-only security camera for a spin and found out why it deserves a spot inside your home

32 INSIGHT

Centrify's Kamel Heus on why organisations can no longer ignore Zero Trust

REGISTRATION NOW OPEN



Dubai, UAE • 13-15 April 2020

The Global Leader in ICT Education, Certification & Standards

e-CONNECTIONS THAT MATTER!

IoT • 5G Networks • PoE Applications and Standards • Data Centres • AV over IP • Wireless Technologies Artificial Intelligence (Al) • Smart Cities, Buildings and Infrastructure • Single-pair Ethernet • And More





EDITORIAL



Talk to us: E-mail: adelle.aeronimo@ cpimediagroup.com

Adelle Geronimo Editor

EVENTS



CLEAR SKIES AHEAD

The cloud has undeniably become one of the most overhyped technologies in decades and rightly so.

Analyst firm Gartner predicts that the cloud market is projected to reach a staggering \$266.4 billion this year.

Cloud computing technology entirely relies on the virtualisations of hardware and software and its service-oriented architecture delivers a number of value-added services. Whether it's on backing up, storing and recovering data; developing apps and services; or analysing data, cloud computing's "as-a-service" offerings have transformed business models. It enabled organisations, small or big, to achieve business agility, scalability, efficiencies and cost-savings.

2019 was a landmark year for cloud in the region. Global cloud players such as Microsoft and Oracle have launched their data centres in the UAE, adding to existing regional centres offered by SAP and Alibaba Cloud, Meanwhile, Amazon Web Services (AWS) also unveiled its first Middle Eastern data centre in Bahrain. Earlier this year, IBM has

"THE PRESENCE **OF THESE GLOBAL PLAYERS** IN THE MIDDLE **EAST HAVE** SPURRED REGIONAL **FIRMS' CONFIDENCE IN** THE CLOUD."

also launched two data centres in the country.

As businesses continue to enjoy its tangible benefits, cloud computing technologies will only grow in prevalence in the IT and business landscapes in the coming months. The presence of these global cloud players in the Middle East have spurred regional firms' confidence in the cloud as the move helped alleviate concerns around data security and sovereignty.

Many organisations in the region are now poised to take advantage of cloud benefits. As the adoption rate grows, so will the complexities and risks that surround rapid migration. This will prompt increased focus on cloud security and regulations, and require new

> approaches to security. This means legacy security solutions should be replaced with tools that can operate seamlessly and consistently across any environment, whether physical or cloud. More importantly, organisations need to make sure that CIOs and CISOs are on the same page when it comes to cloud projects. This ensures that security is integrated into cloud deployments from day one.

Web Developer

Photographer Charls Thomas

webmaster@cpimediagroup.com +971 4 440 9100

C P I M E D I A G R O U P. C O M

Published by

CPI MEDIA GROUP

Registered at Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Tel: +971 4 440 9100 Fax: +971 4 447 2409

Printed by Emirates Printing Press LLC, Dubai

> © Copyright 2020 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

FOUNDER, CPI MEDIA GROUP Dominic De Sousa (1959-2015)

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com +971 4 440 9139

ADVERTISING Group Sales Director Kausar Syed kausar.syed@cpimediagroup.com +971 4 440 9130

Business Development Manager Youssef Hariz youssef.hariz@cpimediagroup.com +971 4 440 9111

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com +971 4 440 9128

EDITORIAL Online Editor Adelle Geronimo adelle.geronimo@cpimediagroup.com +9714 440 9135

> **Contributing Editors** Daniel Bardsley Mark Forker Giorgia Guantario

Sharon Saldanha

marlou.delaben@cpimediagroup.com

PRODUCTION Operations Manager Cherylann D'Abreo cherylann.dabreo@cpimediagroup.com +971 4 440 9107

DESIGN

Senior Designer

Analou Balbero

analou.balbero@cpimediagroup.com

+971 4 440 9140

Designer

Mhar Delaben

+971 4 440 9156

DIGITAL SERVICES Jefferson de Jova Abbas Madh

Maksym Poriechkin

CLOUD TECHNOLOGIES DRIVE INCREASED CYBERSECURITY SPENDING: STUDY

The rapid migration to cloud-based

technologies is the biggest disrupter worldwide of operations and a key driver when organisations plan their spending increases, according to the results of the latest SANS 2020 Cybersecurity Spending Survey.

"The SANS survey showed that rapid movement of corporate services and business applications to cloudbased technology is the biggest factor causing breakage in existing security architectures as well as driving most new security spending," says John Pescatore, SANS Director of Emerging Security Trends. "Cloud monitoring and cloud security access controls were the top two spending areas, followed by spending to increase security staff skills to deal with new technologies, such as the cloud, and to keep up with changes in regulations as well as new threats."

According to the SANS study, more than 50 percent of respondents ranked the increased use of public cloud infrastructureas-a-service (IaaS) implementations as the biggest disrupter to security programmes in the next 12 months. Based on that, 71 percent of respondents reported seeing a need to increase spending on cloud security monitoring, followed by cloud access security broker cloud-specific tools (53 percent), staff skills training (52 percent) and strong authentication (46 percent).

Overall, 57 percent of respondents feel that out of people, process and technology, an increased investment in people would provide the biggest improvement to their overall security posture, followed distantly by process (19 percent) and technology (18 percent).

ETISALAT STRENGTHENS CYBERSECURITY UNIT WITH HELP AG ACQUISITION



Etisalat has completed the acquisition

of Help AG, a privately held regional company specialising in the delivery of cybersecurity solutions and services. Etisalat has been named the most valuable telecoms brand in the Middle East, Etisalat Help AG

According to both organisations, the move will see the integration of the cybersecurity capabilities of the two technology firms to create the region's strongest cybersecurity unit augmenting Etisalat Digital's portfolio of digital security services.

This development enables Etisalat

Digital established lines of business – comprising the cloud, Internet of Things, artificial intelligence, Big Data and analytics – to become more robust and resilient against modern day cyber threats. With its business and technological leadership and flexible business models, the company is uniquely positioned to create added value for its customers and business partners.

Salvador Anglada, chief business officer, Etisalat, said, "Help AG has established itself as the region's trusted security advisor. With cyber security playing a fundamental role in all aspects of digital business today, this acquisition fits perfectly into our strategy of being a key enabler of secure, seamless and effective digital transformation for our customers. We have full trust and confidence that Help AG's leadership will effectively add value to our security portfolio and amplify the cyber security capabilities of our clients."

The value of the deal was not disclosed.

VECTRA ELIMINATES ALERT FATIGUE WITH NEW SOLUTION

Vectra AI has announced the release of

OVERALL NUMBER OF USERS ATTACKED

BY MOBILE MALWARE IN THE UAE

Account Lockdown, the first NDR solution to confront enforcement based on prioritised, high fidelity attacker behaviors and surgical, identity-based enforcement action.

> "Effective enforcement has to begin with visibility. You can't fight what you can't see. The more clarity you have, the more definitive your outcomes will be," said Vectra CEO Hitesh Sheth. "Further, it's been widely established by now that most modern cyberattacks target users

HITESH SHETH, VECTRA

instead of infrastructure or devices. Security teams should take a page out of the attacker playbook and enforce based on users instead of the network or devices."

The Vectra platform generates prioritised signals that automatically identify behaviours rather than anomalies and ensures that analysts are spending their time and resources focused on the most important incidents. Account Lockdown takes this one step further, enabling automatic enforcement on these privilegebased, high fidelity signals.

QUEST AND ONE IDENTITY SIGN DISTRIBUTION DEAL WITH EXCLUSIVE NETWORKS MIDDLE EAST



(LTOR) NATHAN CLEMENTS, EXCLUSIVE NETWORKS AND AMER CHEBARO, QUEST

Quest and One Identity have announced

a new partnership with Exclusive Networks Middle East, which will allow them to distribute the full suite of products and services under the Quest Software Company umbrella.

Since 1987, Quest and One Identity have provided software solutions for the fast-paced world of enterprise IT. With Quest, an organisation can spend less time on IT administration and more time on business innovation. In an agile and highly collaborative world where achieving simplicity in business is often a concern, whether it's digital transformation, cloud expansion, security threats or something new, Quest helps organisations solve complex problems with simple solutions.

Nathan Clements, managing director

- Middle East, Exclusive Networks, said,

"Partnering with Quest was an easy decision to make. They tick all of the boxes that we look for when picking a new vendor – innovative and disruptive technology, high double-digit growth aspirations, a team of known and trusted people, and a clear channel strategy. We have no doubt that we can meet Quests' expectations.

"At Exclusive Networks, we believe in creating a competitive edge for our partners and customers and this newly inked partnership with Quest and One Identity is yet another great addition to our expanding portfolio in the fastest growing distributor in the Middle East," said Clements.

Amer Chebaro, general manager and sales director – EMEA Emerging Markets, Quest Software, said, "What attracted us to Exclusive Networks was the deep-driven expertise that the team has in cyber security solutions and the wide reach they have in the region as a value-added distributor. We have a history of great product solutions and Exclusive has a long-standing history of market reach and penetration, we are extremely confident this will be the start of a strategic and fruitful partnership."

INCREASED NETWORK VISIBILITY DRIVES BUSINESS INNOVATION: RIVERBED

Majority of UAE business leaders (85

percent) believe that business innovation and staff retention are driven by improved visibility into network and application performance, according to a recent study by Riverbed.

The survey findings unveiled in the 'Rethink Possible: Visibility and Network Performance – The Pillars of Business Success' report cites a positive correlation between effective technology and company health, a finding that is supported by the fact that 79 percent of C-Suite, IT decision makers (ITDMs), and business decision makers (BDMs) in the Emirates state that digital performance is increasingly critical to business growth.

It also noted that a little over half (53 percent) of UAE respondents have felt frustrated by current network performance, with IT infrastructure being given as the



MENA MIGALLY, RIVERBED

key reason for the poor performance. This problem is exacerbated by a lack of full and consistent visibility, as one in three ITDMs in the UAE report that they don't have full visibility over applications, their networks and/or end-users. Mena Migally, senior director, MENA at Riverbed Technology, said, "All leaders recognise that visibility, optimised network infrastructure, and the ability to accelerate cloud and SaaS performance are the next frontier in business success. Given this, it's time the C-Suite, business decision leaders, and IT decision makers come together to invest in the right solutions, prioritise measurement, and place visibility and infrastructure at the top of their agenda.

He added, "At Riverbed, we are helping businesses evolve their capabilities, whether it's by monitoring networks and the apps that run on them, application performance, or updating the network infrastructure that underpins their digital services. We fundamentally believe this is the key to supporting our customers' staff and their ambitions, driving innovation, creativity, and helping them Rethink what's possible."

FIREEYE GETS NEW VICE PRESIDENT FOR MEA OPERATIONS



FireEye has appointed Gordon Love as vice president for Middle East and Africa to help drive growth in the region and deepen relationships with partners.

He will report directly to FireEye's Vice President of EMEA Kevin Taylor and is based in the company's office in Dubai, UAE.

"With the growing and sophisticated threat landscape, there has never been a more critical time for organisations across MEA to build effective cyber security solutions," said Love. "Now is the ideal time to join FireEye as our range of offerings put us in a great position to capitalise on this growing market opportunity. I look forward to working closely with our team and MEA customers and as we work together to put efficient defense strategies in place."

Love brings engineering, management and sales experience spanning more than two decades in the IT security and enterprise software sectors. Prior to joining FireEye, Love spent 10 years at Symantec where he was Vice President of the EMEA Emerging Region, overseeing the Middle East, South Africa, Russia, South East Europe, Czech Republic, Poland, Africa and Turkey. He previously held roles with Faritec, IBM, FNB South Africa and Standard Bank Group.

VEEAM SOFTWARE APPOINTS NEW CISO

Veeam Software has appointed Gil Vega

as the new chief information security officer (CISO).

Vega previously served as the managing director and CISO at CME Group and as the assosciate chief information officer and CISO for the US Department of Energy and US Immigration and Customs Enforcement in Washington, DC.

As Veeam's new CISO, Vega will be responsible for establishing and maintaining the company's vision and strategy to ensure its information assets and solutions are adequately protected, and will be pivotal in driving strategies to help customers protect their critical data across multiple environments and ensure regulatory compliance.

Vega will report to Veam CEO Bill Largent and will be part of the company's executive management team.

"I am thrilled to join Veeam, not only because it is the leader in Cloud Data Management, but being in a position to have examined the



GIL VEGA, VEEAM

vision of where the company is going I firmly believe Veeam will continue to transform the industry," said Gil Vega, CISO, Veeam. "Veeam's DNA revolves around delivering the ultimate customer experience and ensuring that data is protected irrespective of its location. Veeam's vision and strategy is unchallenged in the market, and has an exceptionally solid roadmap through 2020 and beyond. I am excited about leading Veeam's effort for taking internal data security, governance and compliance strategy and processes to the next level."

TENABLE NAMES MARK THURMOND AS COO

Tenable has announced it has appointed Mark

Thurmond as Chief Operating Officer (COO).

In this role, Thurmond will lead Tenable's global field operations, including sales, professional services and technical support. Thurmond's appointment adds another layer of depth to Tenable's executive bench as the company continues to deliver on its Cyber Exposure vision to help business executives and security teams understand and reduce cybersecurity risk.

Thurmond has vast experience as an executive leading global sales, services, and operations organisations in high growth technology companies. He joins Tenable from Turbonomic where he served as COO and was responsible for aligning the company's global operations to help customers on their journey to hybrid cloud. Prior to Turbonomic, he was the executive vice president at Qlik Technologies where he led Worldwide Sales and Services. Thurmond also held multiple global sales and operations leadership positions for divisions



MARK THURMOND, TENABLE

of Dell EMC, including senior vice president of Worldwide Sales at VCE and RSA.

"Cybersecurity is fundamental to digital business and Tenable is transforming the industry with innovative solutions to help customers manage, measure and reduce their risk in enterprise environments," said Thurmond. "I'm excited to join this exceptional team and eager to get to work, furthering our Cyber Exposure vision and expanding our footprint around the world."

REDEFINING technology transformation



tahawul tech.com

+971 4 440 9100
info@cpimediagroup.com



@TahawulTech

www.tahawultech.com





cebook.com/tahawultech



CISO50 AWARDS AND FORUM

TAHAWULTECH.COM AND SECURITY ADVISOR ME WILL ONCE AGAIN HONOUR REGIONAL INFORMATION SECURITY LEADERS WHO HAVE FOSTERED INNOVATION AND DEMONSTRATED LEADERSHIP IN THEIR ENTERPRISES DURING THE THIRD EDITION OF THE THIRD CISO 50 AWARDS AND FORUM.





he digital revolution is increasingly reshaping the world in more ways that we can imagine. However, as technology continues to become more integrated into our everyday lives, new unforeseen challenges are bound to occur.

One of the biggest challenges will be cybersecurity, with the global cost of cybercrime expected to reach \$6 trillion by 2021, according to industry reports.

As a new decade kicks off, security leaders are at the forefront of addressing a new wave of threats and developing innovations that go beyond traditional security solutions.

With information security gaining serious traction in the business world, the role of today's CISO is now more important than ever to protect the credibility, integrity and profitability of the business. The CISO role has progressed into a mission-critical service that spans risk areas ranging from data protection to regulatory requirements for business continuity and compliance management. Today's CISOs are tasked with striking the right balance between risk management and business objectives making them integral stakeholders of an organisation and rightfully so.

Set to be held on 24th March at the Ritz Carlton Hotel in JBR, Dubai, TahawulTech.com and Security Advisor ME's CISO 50 Awards will recognise industry visionaries who have shown dedication and prowess in creating a cyber-secure world. The Awards is designed to celebrate the efforts of innovative and forward-thinking security leaders who have delivered real-world results for driving security transformation.

The awards ceremony will be

preceded by thought-provoking keynote presentations from regional security leaders. It will also see a panel discussion titled, 'Double edged sword: AI and machine learning's impact on cybersecurity,' which will how organisations can leverage AI and machine learning in various security and risk management areas. The session will also determine how security leaders can develop cybersecurity strategies that will enable them to anticipate and mitigate AI-enabled cyber-attacks. **1**

TO NOMINATE, PLEASE VISIT: *WWW.TAHAWULTECH.COM/*

CIS050/2020/

CONNECTING THE FUTURE

THE 2020 BICSI EMEA CONFERENCE AND EXHIBITION WILL SHED LIGHT ON THE LATEST TRENDS AND BEST PRACTICES IN THE ICT SPACE. **JOHN H. DANIELS**, CEO AND EXECUTIVE DIRECTOR, BICSI, GIVES US A LOWDOWN ON WHAT TO EXPECT AT THE SHOW.

lobal spending on information and communications technology (ICT) is expected to reach \$4.3 trillion this year, according to research and analyst firm IDC. The growth will be driven by purchases of devices (mainly mobile phones and PCs) and enterprise applications.

Technology is changing at an exponential rate with new innovations and systems emerging, and continually keeping pace with this is no easy task. The Middle East region, in particular, is on the verge of massive digital disruption, with countries such as the UAE, Bahrain and Saudi Arabia leading the charge. To maximise the myriad economic and social gains in the digital era, nations are proactively adopting requisite technologies and developing the associated human capital.

"The rapid pace of technological advancements requires organisations to spare no effort on being at the forefront of change if they intend to stand out and be successful," says John H. Daniels, CNM, FACHE, FHIMSS, CPHIMS, CEO and executive director, BICSI.

"As technology evolves, organisations such as BICSI are constantly evolving with new curriculum, standards and publications geared toward enabling harness the value of this technological evolution." BICSI is a professional association supporting the advancement of the ICT/ extra low-voltage (ELV) professions. To date, it currently serves more than 26,000 members and credential holders.

RP

With the aim of providing regional organisations with the latest trends and best practices in the ICT space, BICSI is hosting the 2020 edition of its annual conference for the EMEA region.

The 2020 BICSI Europe, Middle East and Africa (EMEA) Conference and Exhibition, which will be held at the Dubai World Trade Centre, is targeted towards a global audience of ICT/ELV professionals, including architects, consultants, engineers, cabling infrastructure installers and designers,

integrators, decisionmakers, and anyone else involved in the ICT/ELV profession.

Sheikh

Maktoum

Hall

Hosting The World

e 1979

"Like the ICT/ ELV profession, BICSI is evolving," says Daniels. "Attending BICSI events and keeping up with our latest information including manuals and standards help industry professionals keep up with the ever-evolving business landscape.

"Furthermore, by being a part of BICSI through membership and credentials, individuals will gain access to this knowledge and keep current on what is changing in the industry so they can remain relevant and competitive in their work," he adds.

BISCI promises to deliver an engaging agenda focusing on wide-array of topics including intelligent buildings, smart cities, the Internet of Things (IoT), the latest developments in ICT/ ELV standards, wireless and distributed antenna systems (DAS) and more.

aclo

الشيخ

Daiso

Two keynotes are scheduled throughout the conference namely the 'Global Trends in ICT Infrastructure' by Lone Hansen of BSRIA in the United Kingdom, and 'Developing Deeper Connections' by Eugene Seah of Trainium Academy in Singapore.

This year's BICSI EMEA Conference and Exhibition will also feature a fullday of pre-conference Masterclasses, where delegates can choose between 'Fundamentals of Passive Optical LAN'; 'Converged Networks – the Future of Intelligent Buildings as defined by BICSI 007'; or 'Effective Data Centre Cooling Strategies.' The annual EMEA Awards Ceremony will be held on the evening of the second day of the conference.

"THE RAPID PACE OF TECHNOLOGICAL

ORGANISATIONS TO SPARE NO EFFORT

CHANGE IF THEY INTEND TO STAND OUT

ON BEING AT THE FOREFRONT OF

ADVANCEMENTS REQUIRES

AND BE SUCCESSFUL."

John H. Daniels, BICSI

In addition to the robust conference agenda, the event also presents an excellent platform for industry peers to exchange insights and network with colleagues and other like-minded delegates from all over the world.

"Knowledge transfer is key in our industry and the best place to gain the latest insights is at a BICSI event," says Daniels. **1**



THE SCALING POWER OF DIGITAL PLATFORMS

CLOUD COMPUTING OFFERS A MULTITUDE OF BENEFITS FOR MODERN ENTERPRISES INCLUDING FLEXIBILITY, EFFICIENCY AND EVEN SECURITY. WITH CLOUD ADOPTION GAINING SIGNIFICANT MOMENTUM IN THE REGION, **FERAS AL JABI**, SENIOR VICE PRESIDENT FOR ADVANCED TECHNOLOGY CONSULTANCY (ATC) AND ITQAN GLOBAL FOR CLOUD AND DIGITAL COMPUTING SYSTEMS (DIGITAL OKTA), DISCUSSES WHY THE TWO COMPANIES ARE THE RIGHT PARTNERS OF CHOICE FOR A SUCCESSFUL, SEAMLESS AND SECURE TRANSFORMATION TO THE CLOUD.

loud spending in the Middle East and North Africa (MENA) region is expected to reach \$2 billion by 2020, according to research and analyst firm Gartner. The

main growth drivers are Platform-asa-Service (PaaS) and Software-as-a-Service (SaaS), which currently account for \$1 billion between them. The UAE is amongst the most advanced countries globally. When it comes to digital innovation, the country has one of the highest levels of ICT adoption across all market sectors.

A decade ago, the government launched the UAE Vision 2021, a national agenda aimed at diversifying the economy and making the country one of the best in the world including in the field of science and technology.

As part of the drive towards economic diversification, the UAE is embracing technological innovation with cloud

computing as its foundation. The data center has been disrupted as much as the desktop has in recent years, thanks to the rapid rise of cloud computing.

Despite predicted growth, the cloud is still an emerging technology in the Middle East and regional businesses need the expertise and guidance of entities such as systems integrators and cloud service providers to fully maximise its value.

Among such organisations are Digital Okta and ATC, which are both gaining significant momentum in the region with the firm's senior vice president Feras Al Jabi at the helm.

ATC is a systems integrator focused on enabling organisations translate their digital vision into reality. The company centres on three key areas namely smart workplace, application solutions, licensing, consultancy and support.

Established in 2016, the organisation has played a significant role in driving the digital transformation of several public sector firms, enabling their adoption of disruptive technologies such as cloud, artificial intelligence (AI), Internet of Things (IoT), mobility, software-defined networks and software-defined data centres.

"ATC prides itself as being an embedded player in the IT industry," says Al Jabi. "This means that we align our vision with the different shifts and trends in the industry by being constantly in touch with our customers. We are continuously innovating. We believe that every digital improvement in customer experience will open up new possibilities for a business to thrive. PREDICTED CLOUD SPENDING ATC has **IN MENA IN 2020**

numerous global IT brands in its portfolio including Dell EMC, Huawei, Juniper and Microsoft as well as other key players in the fields of Big Data, blockchain and Al.

"What differentiates ATC's services is that we provide holistic support to our customers from project planning to design and implementation. We drive innovation from core to the edge, demonstrating real added value to customers in their digital transformation journey," he says.

With a dedicated team of highly skilled professionals, ATC has become one

of the preferred local systems integrators for major organisations from the government, semi-government, education and healthcare sectors.

Another unique value proposition by ATC, according to Al Jabi, is its unparalleled trust with its customers.

SOURCE:GARTNER

"For us to be able to effectively drive our customers' digital transformation project, we provide our clients with an outside-in point of view to help them achieve their digital objectives. We make sure that we know exactly what's going on site, the data centre, and what industry shifts will affect them to ensure that

we bring them the right solutions and advisory for their projects."

Meanwhile, Digital OKTA is a cloud services provider focused on enabling business IT transformation journeys by leveraging cloud, mobility, IoT and Big Data solutions. Digital Okta boasts a diverse range of products and services including Microsoft Dynamics 365 Enterprise, Hybrid Transformation and Azure Managed Services to name a few.

"Digital Okta is a company that was born and created in the cloud," explains Al Jabi. "We started the company with the notion that cloud offers businesses unlimited opportunities to manage their data and resources, and we are the right partner to offer them with expertise and

consulting services to get ahead in the market."

Al Jabi highlights that the migration and advisory services Digital Okta offers has resonated well with their clients in the region who want to transition to the cloud.

"As a cloud services provider, our goal is to ensure that we design a correct and secure path towards cloud transformation for our

clients," he says.

"We provide a comprehensive and very hands-on approach to make sure everything is up and running for them. We ensure that there is an element of trust when it comes to our relationship with our customers, and we assure them that we are with them every step of the way."

Security and sovereignty

Over the last few years, despite increased digital transformation in the region, there was still a significant volume of resistance from some businesses initially when transitioning to the cloud. This is primarily due to the lack of standards when it comes to data privacy and sovereignty.

However, 2019 has been a landmark year for cloud in the region. It saw cloud providers such as Microsoft and Oracle launch data centres in the country, adding to existing UAE centres offered by SAP

INNOVATION FROM CORE TO THE EDGE, DEMONSTRATING REAL ADDED VALUE TO CUSTOMERS IN THEIR DIGITAL TRANSFORMATION JOURNEY."

"WE DRIVE



and Alibaba Cloud. Amazon Web Services (AWS) also unveiled its first Middle Eastern data centre in Bahrain.

"This step that was taken by Microsoft and AWS is very strategic," says Al Jabi. "Businesses are now expressing a clear desire to move to the cloud. The establishment of these data centres has alleviated fears over the security and confidentiality of their data."

According to Al Jabi, in addition to the new local data centres by global cloud providers, the different security standards focused on data privacy and cloud security have also contributed to regional firms' being more open to the cloud.

"These global cloud providers adhere to international security standards ensuring the security of customers' digital assets. With all these players entering the regional market, we can expect more regulatory frameworks to be put in place. I believe that regional governments will become more active in developing cloud regulations."

As a systems integrator and a cloud services provider, Al Jabi notes that both ATC and Digital Okta respectively, are

"OUR EXPERTISE AND SOLUTIONS CAN HELP ORGANISATIONS NAVIGATE THE CYBERSECURITY CHALLENGES, ALL WHILE UNLOCKING THE POTENTIAL OF CLOUD."

well-positioned to enable customers to stay on top of the necessary regulatory mandate on cloud adoption.

"Cybersecurity will always be a challenge for any industry," he says. "No one is immune to cyber threats and the more our digital life becomes more active, the more vulnerable we become to cyber-attacks. Our expertise and solutions can help organisations navigate these challenges, all while unlocking the potential of cloud."

Looking ahead

Al Jabi highlights that the regional landscape can expect growing demands

for AI initiatives and programmes, to which cloud technologies play a key role.

"Al will be a gamechanger for any industry, but what many people don't realise is that cloud is a significant element for any Al implementation to succeed. So, this year we will be launching new programmes and announcing partnerships focused on driving Al initiatives on the cloud."

In the next few months, Digital Okta will also be launching a new online marketplace to help organizations to purchase and seamlessly optimize its software-as-a-service offerings.

ATC and Digital Okta will continue to play an important role in enabling seamless and secure digital transformation journeys for regional enterprises, according to Al Jabi.

"Since day one we know our identity and our value. We will remain a committed and loyal partner of choice for regional businesses. Finally, we will continue to value our customers' needs and help them drive their business towards a bright future," he says. **1**

ALL EYES ON THE FUTURE

HAKAN OZYIGIT, REGIONAL DIRECTOR, SECURITY SYSTEMS AND BUILDING TECHNOLOGIES, ROBERT BOSCH MIDDLE EAST, DISCUSSES THE EVOLUTION OF THE SMART VIDEO SURVEILLANCE AND HOW THE COMPANY CAN PLAY THE ROLE IN THE SECURITY SEGMENT'S FUTURE.

hat have been some of the highlights at Bosch Building Technologies over the past year?

Over the past year, we focused our efforts on highlighting the tremendous value that Video Analytics can bring to both organisations and governments by delivering unparalleled data for business intelligence. Our customised solutions are helping solve critical organisational challenges while delivering layered insights.

With several successful launches. during the last year we have introduced a number of security systems offerings including climate-resistant, easy to install, yet cost-effective smart video solutions. Our most recent camera range is the IP 3000i cameras with four form factors and Essential Video Analytics built in as standard. Featuring Camera Trainer technology are the FLEXIDOME IP starlight 8000i fixed dome cameras that offer remote wireless commissioning, detailed image capture in challenging light conditions, and data analysis for improved security Camera Trainer technology harnesses machine learning to enable the built in Intelligent Video

Analytics in Bosch cameras to function in ways that are even more accurate and application specific, opening up new revenue channels for businesses.

Our smart surveillance portfolio is rounded off by MIC IP 7100i extreme weather cameras (also with Camera Trainer technology), AVENAR 2000/8000 fire alarm panels, AVENAR 4000 alarm system and the PRAESENSA Public Address and Voice Alarm System, to name a few.

How has the smart surveillance segment evolved over the last couple of years? What are the latest trends impacting this space?

The increased demand for crisp image resolution and perimeter surveillance is resulting in widespread adoption of multi-sensor cameras, supported by capabilities within artificial intelligence and cloud computing. Such a landscape is providing immense opportunities to both service providers and vendors of residential and commercial security and surveillance solutions.

An increased reliance on Internet Protocol (IP) is supporting both video-based surveillance and related technologies. Deployment over IP is resulting in reduced costs due to widespread availability and high bandwidth speeds. With the proliferation of the Internet of Things (IoT), smart surveillance can integrate with energy management and building automation platforms. Such connectivity and data volumes increase the significance of protective security solutions. For instance, data security can be achieved through encrypting it at the hardware level, using a cryptographic key that is safely stored in a unique built-in Trusted Platform Module.

The surveillance platforms are also able to securely share data with mobile devices, providing both historical data and real time insights.

How will the hyper-connectivity brought by the impending Internet of Things era impact initiatives around smart and safe cities? What role can Bosch play in this era?

Within our hyper-connected smart cities, with its capabilities in sensor and analytics technologies, networked video surveillance will provide a host of benefits that enable faster detection and prosecution of accidents and crimes. The predictive analytics provided by these platforms and the ability to draw data from across the entire timeline (since the installation of these technologies) allows decision makers in cities address these challenges head on and reduce their reliance on physical security and need for engagement across different end users.

Such technologies are delivering higher resolutions and frame rates, resulting in several terabytes of rich data, but also creating uses well beyond security. We are committed to ensuring that such data needs to be managed efficiently without compromising image quality or making it less relevant.

What initiatives and technologies should governments and private organisations invest into?

Standardisation, connectivity, and seamless, cross-company integration are critical for the success of smart surveillance. It is important for organisations to work with each other and



with governments in order to establish a common standardised platform for security and safety solutions.

Bosch Building Technologies, Hanwha Techwin, Milestone Systems, Pelco, and Vivotek Inc. jointly established the Open Security and Safety Alliance to create a secure and reliable ecosystem for the security and safety industry that brings together hardware manufacturers, software developers, integrators, specifiers, consultants, users and many others.

The UAE is among the most active nations when it comes to smart and safe city initiatives, how does Bosch aim to support the nation in this endeavor?

We are committed to support Dubai's smart city developments and future ambitions on all aspects. We hold capabilities not just on a product and software level but also within providing central communication and integration

"WITHIN OUR HYPER-CONNECTED SMART CITIES, WITH ITS CAPABILITIES IN SENSOR AND ANALYTICS TECHNOLOGIES, NETWORKED VIDEO SURVEILLANCE WILL PROVIDE A HOST OF BENEFITS THAT ENABLE FASTER DETECTION AND PROSECUTION OF ACCIDENTS AND CRIMES." solutions that can link municipal and public services. Such solutions can connect city and community stakeholders (e.g. residents, tourists, government) together with parts of the public infrastructure and other service providers (e.g. mobility services).

How will the upcoming Expo 2020 impact organisations' investments around smart surveillance?

With a large number of visitors expected over the six-month event, adoption of smart surveillance technology is expected to peak. It is important for organisations to renew their focus on cybersecurity and data protection. We are committed to driving a systematic approach to maximise data security by considering physical safety and cybersecurity simultaneously.

What can regional customers expect from Bosch Building Technologies this 2020?

Our portfolio will increasingly feature video security cameras that incorporate built-in machine learning capabilities. Our solutions with built-in Video Analytics as standard will continue to evolve in their ability to repurpose captured video data for other uses than security alone.



WINNING IN THE CYBER BATTLEGROUND

INCREASED DIGITISATION HAS TRANSFORMED PARTNERSHIPS BETWEEN GOVERNMENT AND PRIVATE SECTOR ORGANISATIONS. WITH THREAT ACTORS USING INCREASINGLY SOPHISTICATED TECHNOLOGIES AND STRATEGIES, SECURITY CORRESPONDENT DANIEL BARDSLEY SPEAKS TO INDUSTRY EXPERTS ON WHY GULF STATES NEED TO BOOST THEIR COLLABORATION WITH PRIVATE ENTERPRISES TO WIN THE FIGHT AGAINST CYBERCRIMINALS.

> yberwarfare is now sometimes described as the fifth dimension of human conflict. There is air, sea, land, space and, now, the cyber realm, where nations are employing their technological

expertise in an effort to disrupt rivals – sometimes to devastating effect.

Myriad governments have fallen victim to attacks, some thought to have been perpetrated or backed by nation states.

From nearly a decade ago, when the French Ministry of Finance suffered a malware attack at the time of a Paris G20 summit, through to 2019, when local authorities in the United Kingdom were reportedly suffering hundreds of attempted cyber-attacks every hour, the risk of disruption to governments and their critical infrastructure and services has never been far away.

Russia has been blamed for attacks on Ukraine, for example, including the 2017 NotPetya incident, which disrupted numerous government agencies and went on to spread widely. The secretive North Korean government is another regime thought to be a major source of cyber offensives.

In this climate it is no surprise that governments are prioritising cybersecurity. Singapore, for example, recently announced that it was setting aside \$1 billion (Dh2.63 billion) over the next three years to improve

"GOVERNMENTS RELY ON THESE PRIVATE CYBERSECURITY SECTORS TO COMPLEMENT THEIR CYBER CAPABILITIES, FOR EXAMPLE, IN PROVIDING THREAT INTELLIGENCE AND EXPERTISE DURING INCIDENT RESPONSE." government cyber and data security.

As a region affected by a complex web of tensions, the Middle East has inevitably had its share of politically motivated cyber incidents in recent years.

Among them was the disruption caused by the Stuxnet computer worm, which is thought to have been partly developed by the United States.

Discovered in 2010, Stuxnet caused centrifuges involved in Iran's nuclear programme to malfunction, setting back the country's ability to produce enriched uranium, which can be used in nuclear weapons.

While Iran was on the receiving end when it came to Stuxnet, the country has also been seen as one of the most active countries in the region in employing cyberwarfare, with the Islamic Revolutionary Guards Corps thought to be behind many attacks.

Among those attacks blamed on the country was the 2012 offensive against the Saudi Arabian oil and gas giant Saudi Aramco, during which Shamoon malware was reportedly used to overwrite tens of thousands of Saudi Aramco's hard drives.

Gulf region governments have made great efforts to promote digitisation, shown by the likes of the Smart Dubai 2021 initiative, which involves governments offering services digitally. Among Saudi Arabia's flagship digital projects, meanwhile, is the Neom smart mega-city.

Digitisation efforts, however, lead broaden the threat landscape. It results in a situation, says Dr Bushra Alahmadi, a researcher at the University of Oxford and faculty member at King Saud University, in which governments and the private sector in the Gulf region can be "increasingly vulnerable to cyber-attacks".

"Countries in the Middle East such as Saudi Arabia and the UAE recognise this threat and risk associated with digital transformation," says Alahmadi.

"As a result, there is a strong focus and commitment to investment in both

the human capital and the technological capabilities required by regional institutions to defend themselves from cyber-attacks."

Nations in the region want to protect their digital infrastructure and are especially focused on strategically vital sectors such as oil and gas.

"The cybersecurity attack on Estonia in 2007 that targeted both public and private sectors and led to huge disruptions to internet and e-government portals hints to what to expect of destructive outcomes of cyberwarfare on a state's digital infrastructure." says Alahmadi.

Efforts to make the Gulf states cybersecure have involved "huge investments", she adds, and encompass both the public and private sectors.

Among the government initiatives she highlights is the establishment by the Saudi Arabian government of the Saudi Federation for Cyber Security and Programming and the National Cybersecurity Authority (NCA).

The NCA has an agreement with the Ministry of Education to provide scholarships for students keen to study cybersecurity abroad. The NCA has also set up a cybersecurity training programme called CyberPro, which, says Alahmadi, is targeted at improving cybersecurity skills in the workforce and developing offensive and defensive capabilities.

There have also been initiatives from the Prince Mohammed bin Salman bin Abdulaziz Foundation (MiSK) to develop cybersecurity capabilities.

In Saudi Arabia they have a long-term view of the issue, with their aim of having sufficient qualified cybersecurity specialists being part of the country's Vision 2030. The country has also established an initiative to encourage more women into the field.

But, crucially, efforts are not focused on the state in isolation from the commercial sector: Alahmadi says the digitisation that is taking place means that there has to be "strong collaboration with the private



Bushra Alahmadi, King Saud University

"COUNTRIES IN THE MIDDLE EAST SUCH AS SAUDI ARABIA AND THE UAE RECOGNISE THIS THREAT AND RISK ASSOCIATED WITH DIGITAL TRANSFORMATION."

cybersecurity industry".

Demonstrating this, an aim of a Global Cybersecurity Forum (GCF) held in Riyadh in February was to "promote a thriving cybersecurity industry that fosters innovation and investment to address evolving cybersecurity risks".

"Governments rely on these private cybersecurity sectors to complement their cyber capabilities, for example, in providing threat intelligence and expertise during incident response," says Alahmadi.

"Many private organisations have attended and participated in the GCF, evidence of their successful partnership with governments in the region."

This all highlights, she says, the importance of cooperation between private and public sectors to strengthen cybersecurity across sectors such as healthcare and financial services.

"I would expect such collaborations to continue to grow, bringing more cybersecurity investments and businesses to the region," she said.

Alahmadi says one of the fruits of the cybersecurity efforts seen in the region has been a high ranking for countries such as Saudi Arabia in the Global Cybersecurity Index, which is issued by the International Telecommunication Union (ITU). Alahmadi highlights the way that Saudi Arabia has been ranked 13th globally by the ITU for its commitment to cybersecurity.

"Although cybersecurity capacity in the region may be in its nascent stages, it is rapidly developing and growing and we will see Gulf countries ranked even higher in the next report," she says.

Just as the Gulf states are promoting

both private and public sector cybersecurity expertise to safeguard themselves and their strategic assets, so in other parts of the world there are positive interactions between government and commercial cybersecurity capability.

Professor Clive Jones, a professor of regional security in the School of Government and International Affairs at Durham University in the United Kingdom, says it is known that, for example, "there are links between military research and the private sector".

"With the United States, we know cybersecurity companies have close interaction with the National Security Agency," he says.

Given the inevitable secrecy that accompanies the defence sector, academics and other analysts can find it difficult to work out definitively what is happening.

Jones notes that can also be hard to determine the ultimate capabilities of states when it comes to cyber-attacks and cybersecurity.

"We simply don't know the types of capabilities that these states can unleash through their cyber-attacks, and the attacks using third parties," he says.

"It could be an individual in his bedroom could be given some form of malware that finds its way into the critical infrastructure of a target state.

While attacks that take place are often well known, Jones says that these are by and large "probing attacks".

"We think we have an idea of these capabilities, but until we see them in action, we simply don't know what these capabilities are," says Jones. **1**



6-8 APRIL 2020

Dubai World Trade Centre

UNIFYING SECURITY FOR GLOBAL CITIZENS

FIRST TIME IN THE REGION KEYNOTE SPEAKERS



Bryan Seely

The only hacker to wiretap the US Secret Service & FBI, what he's going to share will absolutely blow your mind

Hector Monsegur

Anonymous' most notorious hacker and technical expert behind Anonymous/LulzSec collective

Enquire about exhibiting, speaking and visiting

OFFICIALLY SUPPORTED BY

<u>↓ +971 4</u> 308 6469 ⊠ gisec@dwtc.com

om 🌐 www.gisec.ae

UUBAI ELECTRONIC SECURITY CENTER

شطةدس

OFFICIAL DISTRIBUTION

ديــــي الذكيـة SMART DUBAI ON

STRATEGIC PARTNERS

SPIRE Carbon Black. I Recorded BLUVECTOR. proofpoint.

PLATINUM SPONSORS

ORGANISED BY



HACKING THE Skills gap

Й

ONE OF THE MOST OVERWHELMING PROBLEMS IN CYBERSECURITY IS A BALLOONING SKILLS SHORTAGE. WITH THE SHORTFALL OF CYBERSECURITY TALENT EXPECTED TO REACH AS HIGH AS 3.5 MILLION UNFILLED ROLES BY 2021, SHOULD ORGANISATIONS LOOK INTO RECRUITING HACKERS TO ADDRESS THE SKILLS GAP CRISIS? DANIEL BARDSLEY INVESTIGATES.

Й



omputer hackers tend not to come out well when they are depicted in the movies or featured on the television news.

A film might show a young man in a darkened room furiously typing away

on his keyboard as he gains unauthorised entry to a government's top secret defence network.

Meanwhile, hackers are often portrayed in the news media as dishonest loners who have got themselves into serious trouble.

Yet, there is a positive side to computer hacking, one that some researchers say companies could do more to harness as they look to fill cybersecurity skills gaps.

Those skills gaps are significant, with a recent survey by the IT analysis company the Enterprise Strategy Group recently finding that cybersecurity had the most severe shortages of any IT sector. Moreover, the proportion of companies reporting cybersecurity skills gaps in the survey has increased for four consecutive years.

A common misconception about hackers – and one reinforced by their appearances on the big and small screens – is that they are all engaged with unethical or illegal activities.

Whilst some do have malevolent intent, many are, by contrast, carrying out ethical hacking, which may involve investigating flaws in the security of networks or software with a view to highlighting them so that gaps can be plugged.

"Individuals round the world will look at a particular product, work out a weakness and go back to the product supplier and suggest how to patch things up," says Dr Christopher Richardson, a UK-based researcher who has looked at hacking communities.

"[They will say]: 'I've done this. I've got in. If I can get in, anybody can get in.' That's the type of thing I'm in favour of."

Another academic to have investigated the hacking community is Dr John McAlaney, a psychologist and associate professor at Bournemouth University in the United Kingdom.

McAlaney and his co-researchers have got in touch with online hacking communities to learn more their activities and find out what motivates them.

"We found them to be a very interesting group – a lot of passion, a lot of skills, a very complex group, with a lot of people doing ethical hacking," he says.

Sometimes interactions with hackers, who often keep their identity secret by using pseudonyms, have been exclusively online. In other cases, the researchers have been in touch offline too.

The communities are more diverse than might be expected in terms of age, ranging from people in their early teens who have recently become interested in hacking through to adults in their 30s or 40s who may have families and full-time jobs – sometimes in cybersecurity – and decades of hacking experience.

"You do get lots of people in cybersecurity as a job who were very likely involved in hacking when they were younger. It's something they probably don't want to admit," says McAlaney.

While the secrecy that surrounds hacking means that determining the location of hackers is difficult, McAlaney says that they seem to be spread across the world.

Some of those who he has been in contact with appear not to be native English speakers, a further indication of the hacking community's diversity. So why do people become hackers? In McAlaney's experience they are not normally motivated by a desire to cause havoc or commit crime.

"I've never spoken to a single hacker saying, 'I was born to be a criminal mastermind.' You do get a small number who are criminally motivated; they became a hacker because of the financial incentives," he says.

Among the more legitimate financial incentives are what are known as "bug bounties": money offered by companies to people who expose cybersecurity flaws in their products or networks. But McAlaney says that such rewards are just one of many reasons why people hack.

"Hacking means exploring limits. Very few people I speak to are financially motivated. Bug bounties are nice, but for the vast majority of hackers, it's not the motivation," he says.

"It's about the passion and wanting to understand things. There's a bit of prestige. They want to be the best, to have the most knowledge."

Although some organisations offer payment to ethical hackers, not all respond in a positive manner. Some of them simply ignore them, tying in with Richardson's assertion that many digital organisations "don't respond to vulnerabilities in the digital world".

Other companies react in a hostile manner to the news that their systems have been breached, even if the hacker had no malevolent intent. The organisations may inform law-enforcement authorities, which could result in the hacker facing



Dr John McAlaney, Bournemouth University, UK

"YOU DO GET LOTS OF PEOPLE IN CYBERSECURITY AS A JOB WHO WERE VERY LIKELY INVOLVED IN HACKING WHEN THEY WERE YOUNGER. IT'S SOMETHING THEY PROBABLY DON'T WANT TO ADMIT."

prosecution. This can happen even when the hacker has exposed a basic security flaw that could, for example, put customer data at risk.

Richardson, a former university academic and founder of Digital Smart Solutions, a UK-based technology startup company, suggests that there should be better ways of dealing with hackers than criminalising them. Sometimes, he says, hackers do not know what type of system they have got into until they are actually inside.

Indeed it is probably the case that many hackers have, perhaps unwittingly, carried out activities that inhabit a grey area between legal and illegal, but are far from being hardened criminals.

"These are very capable individuals who are not doing criminal activity. Are we as a society punishing curiosity?" says Richardson.

"I've dealt with a lot of police forces where they've interviewed adolescents and adults about their hacking of other people's systems without their consent. They're curious young people and they can benefit society."

He would like the positive work they

Dr Christopher Richardson, Digital Smart Solutions

"THE FREQUENCY OF NEW VULNERABILITIES IS HIGH, SO YOU HAVE TO BE FLEXIBLE IN THE MARKET." do to be acknowledged. Instead, he says sometimes the response is to "stick them aside so they fall into traps they shouldn't have gone down".

It is a view shared by McAlaney, who says society needs to "stop threatening" people who unearth security flaws.

"There's a huge gap in cybersecurity. There's a massive need for more people and you have these younger kids who've got involved and don't understand the legality," he says.

"They're criminalised and when they're criminalised, they're blocked from working in legitimate cybersecurity jobs.

"If [companies] did hire someone known as a hacker and [who then] did something wrong, they would be potentially liable."

Analysts also say that having a slightly unconventional personality that might not naturally fit into the corporate world should not be a barrier to a career in cybersecurity.

Richardson says that many ethical hackers are "not the most sociable people", but they nonetheless have a lot to offer.

"You don't have to be in an office to do your job. You can be remote. As we become more digitally connected there's less need for physical connection," said Richardson.

"The frequency of new vulnerabilities is high, so you have to be flexible in the market. Employ these people or have these people on a short-term contract.

"It's about the talent. Anybody can come into the digital world. Autism and physical impairments need not impinge in the digital world. We can maximise the human capital coming into the digital world."

ROUGH SEAS

WHETHER YOU'RE ON LAND OR SEA, CYBERCRIMINALS WILL FIND A WAY TO EXPLOIT YOUR VULNERABILITIES AND FIND A WAY TO WREAK HAVOC IN YOUR IT SYSTEMS. LIKE ANY INDUSTRY, THE MARITIME SECTOR IS NOT IMMUNE TO CYBER RISKS AND THREATS AND INCREASED DIGITISATION IN THE FIELD PRESENT GROWING OPPORTUNITIES FOR CYBERCRIMINALS TO PURSUE.



ith immense power and scale coupled with a sense of mystery, it is no wonder

that the sea has long been a source of myth and legend.

There have been countless stories told of the ocean waves, but few are as eerie as that of the Flying Dutchman, a ghost ship said to have been condemned to continually sail the seven seas without reaching port. Sailors on other ships were hardly eager for this vessel to come into view, since a sighting was a portent of doom.

The legend is often linked to the Dutch East India Company of the 1600s, when the Netherlands was the unquestioned global maritime superpower.

Fast forward to the 21st century, and the era of the ghost ship – one that sails the seas without a soul on board – could be with us again, albeit in a very different guise.

Autonomous shipping is now fast appearing over the horizon, as evidenced by, among other things, the fact that a 12-metre autonomous vessel crossed the sea from the United Kingdom to Belgium in the middle of last year.

Norway, meanwhile, is building the Yara Birkeland, a full-sized autonomous cargo ship that could be launched later this year. The vessel will sail up and down Norway's coast.

As with autonomous road vehicles, such ships raise obvious cybersecurity risks, such as the danger that hackers might gain access to the navigation systems. Would criminals be able to start guiding the vessel so that it became a modern-day Flying Dutchman, under the control of a shadowy malign power?

There are, of course, myriad cybersecurity threats associated with conventionally crewed ships too, with the Automatic Identification System (AIS), which is based on the use of transponders, GPS and chart display systems potentially vulnerable.

Experts have said that, as ships have become more automated, opening up new opportunities for hackers, the industry has tended to lag when dealing with threats, especially when compared to other transport sectors, notably aviation. Ports too have been highlighted as being poorly protected.

"It's taken a while for the shipping industry. There's quite a lot of legacy equipment in the maritime industry. It's



Professor Keith Martin, Royal Holloway, University of London

"THERE'S QUITE A LOT OF LEGACY EQUIPMENT IN THE MARITIME INDUSTRY. IT'S HARDER FOR EVERYONE TO REALISE IT'S CONNECTED TO CYBERSPACE."

harder for everyone to realise it's connected to cyberspace," says Professor Keith Martin, a professor of information security at Royal Holloway, University of London.

"Shipping is very aware that it relies on communications, but the communications have been very closed off – ships talking to ships, ships talking to ports.

"They imagine themselves in this isolated world. But what's happened is that that network is connected to the rest of the world – ships talking to cyberspace, ports talking to cyberspace.

"It's moving from a mindset of isolation to realising they're now connected. It takes a while for people to realise a ship could be attacked from the land."

One cybersecurity weak point is that the computer systems may be old and outdated. Systems may be based on designs that are a number of years old even at the time of installation, and the ship is then typically operated for a couple of decades.

"You're looking at equipment that's 25 years old before it hits the end of its life, and you have new systems plugged into it," says Rory Hopcraft, a maritime cybersecurity researcher at Royal Holloway, University of London.

Also, because crews switch, the people operating these systems change frequently, which can make it harder to ensure that they are operated in a secure manner. Crews are in any case becoming smaller and may have only limited understanding of how systems work



2

280

270

because maintenance is carried out by outside contractors.

In addition, vessels may be connected to land-based systems with vulnerabilities of their own.

"Ship operators are very aware of the cybersecurity issues and they're aware they're going to lose money, but it feels like there are a lot of other pressures on them at the moment," says Hopcraft.

Many cybersecurity issues that could trip up shipping organisations, including weak passwords and phishing emails, are the same as those faced by other sectors.

Reports have said that ships sometimes retain the default username and password for satellite communications equipment, which could lead to hacks in which a vessel's Electronic Chart Display and Information System (ECDIS) gives false readings, which could lead to, for example, a collision.

While the cyber vulnerabilities facing the maritime industry are numerous, the number of actual reports of incidents tends to be low. Accounts have suggested



that shipping companies prefer not to publicise attacks because of concerns over how insurers, investors and others might react. In some other cases the attacks might simply go undetected.

Often, however, the effects are all too widespread and obvious. One of the most serious cyber-attacks to have affected a shipping company is the 2017 NotPetya ransomware incident that caused significant disruption to the Danish conglomerate Maersk, among other companies.

The largest carrier of seaborne freight in the world, Maersk was not an intended victim of NotPetya, which was thought to have been aimed at causing disruption, for political reasons, in Ukraine. Nevertheless, Maersk had tens of thousands of infected endpoints in scores of countries, leading to months of turmoil and a final cost estimated by the company to be as much as \$300 million.

While Maersk was collateral damage for NotPetya, Hopcraft highlights other politically motivated cyber-attacks that may be aimed specifically at shipping companies.

"Last year the United States reported a lot of ships' navigation systems had been giving false readings. They think that was



Rory Hopcraft, Royal Holloway, University of London

"SHIP OPERATORS ARE VERY AWARE OF THE CYBERSECURITY ISSUES AND THEY'RE AWARE THEY'RE GOING TO LOSE MONEY, BUT ← IT FEELS LIKE THERE ARE A LOT OF OTHER PRESSURES ON THEM AT THE MOMENT." Iran trying to get ships to go into their waters so they could detain them," he says.

On the other hand, ships might themselves be involved in underhand cyber activities, such as by transmitting false AIS readings when they are involved in smuggling or illegal fishing. Vessels may also give false data if they want to prevent being detected by pirates.

The slow pace of change in the maritime regulatory regime, laid down by the International Maritime Organisation (IMO) – which mandates the use of AIS and other systems on larger vessels – could be one reason why vessels are not as secure as they might be.

It may take several years for regulations that have been already been agreed to actually be brought into force, a degree of responsiveness that is unlikely to be adequate for dealing with fastdeveloping threats.

"It's interesting to see a large organisation like the IMO trying to find a way through and make shipping safe and secure in a world where it doesn't quite understand what cyber and cyber technology means," says Hopcraft.

Organisations offer certifications in cybersecurity for shipping operators, including, in the case of Bureau Veritas, a listed company, "Cyber Managed" for existing vessels that adhere to certain cybersecurity standards, and "Cyber Secure" for new builds. This could encourage more shipping companies to improve their defences, especially as certification may reduce insurance premiums.

The impending arrival of autonomous ships could also represent a wake-up call that results in a greater focus on cybersecurity across the industry.

"The autonomous ship is clearly connected; the risks are upfront. I would hope that would move things in the right direction. A lot of the thinking there will rub off onto the broader maritime world," says Martin.

RING INDOOR CAMERA

RING'S FIRST INDOOR-ONLY SECURITY CAMERA EXCELS FOR EASE OF INSTALLATION AND SHARP 1080P VIDEO, MAKING IT THE PERFECT ADDITION TO ANY SECURITY SYSTEM, WRITES DEPUTY EDITOR GIORGIA GUANTARIO.



ing has been making some of the best outdoor home security cameras and video doorbells for years, so it is no surprise that the newest addition to

their portfolio, Ring Indoor Camera, fully lives up to expectations.

The first thing that positively struck me was its size - the body of the camera is as small as a can of Coke and blends so well in the room that you're likely to forget that there's a camera watching you. As a huge fan of Ring Door View Cam's ease of installation. I was thrilled to find out the Indoor Camera is probably even easier to set up. The camera doesn't include a battery, but instead needs to be plugged into a power socket to function. I am not a fan of drilling holes into my wall, so I was glad to see the camera comes with a stand set on the bottom. Ring also includes screws and wall anchors in case you'd prefer a wall setup to the tabletop.

Ring customer will find that the indoor camera is an easy addition to their other Ring devices – the camera works with the same mobile app as the others, and it takes about a minute to add it to the list by scanning the QR code at the back of it. If you're not a Ring customer already, all you'll need to do is download the app and set up an account – again something that can be done in five minutes at most.

The Indoor Camera captures videos at 1080p, a quality that we've come to expect from Ring, and features a wide 140-degree diagonal field of view. Placed on top of my tv stand in one of the corners of the room, the camera was able to pick up movement three or four meters away. The camera also includes IR LED for night vision and 2.4GHz 802.11n Wi-Fi radio to connect to the home network. Setting up a motion zone on the app is fundamental to avoid receiving notifications every time someone, or something, moves around the room. The motion detection and motion-activated recording work brilliantly, providing push notifications instantly when the camera detected motion. As with the Door View Cam, the level of customisation is outstanding: besides being able to disable motion alerts, the app also allows you to disable audio, adjust sensitivity,

choose how your camera operates through the three different modes (home, away or disarmed) and access live view. The previously mentioned motion zone setting allows you to focus on just one section of the room, may this be a window or an entrance, increasing the motion detection's accuracy.

The camera also features a twoway talk with noise cancellation, allowing you to speak to anyone in the room through the camera although one of my favourite features in outdoor cameras. unfortunately I failed to see the utility of this to an indoor camera besides freaking out whoever is sitting in the room and is unaware you're watching them. Overall, Ring has

delivered a good indoor camera with amazing video quality and the easiest setup anyone could have asked for. Ring customers will be pleased to add this to their security system, managing it all through one app.

Ring Indoor Cam is also the most affordable Ring's camera to date – it's available in the United Arab Emirates at Amazon.ae, Dubai Duty Free, Jumbo, Sharaf DG, and Virgin Megastore for just AED 249 (including VAT).



WHY ORGANISATIONS CAN NO LONGER IGNORE ZERO TRUST

WEAK PASSWORDS ARE A MAJOR SOURCE OF BREACHES AND BY ADOPTING A ZERO TRUST APPROACH WITH LEAST PRIVILEGED ACCESS, ORGANISATIONS CAN INCREASE THEIR COMPLIANCE LEVELS, EXPLAINS **KAMEL HEUS**, REGIONAL DIRECTOR, NORTHERN, SOUTHERN EUROPE, MIDDLE EAST AND AFRICA FROM CENTRIFY.

he recent Gartner Security and Risk Management Summit held in Dubai, UAE revealed that the Middle East and North Africa region has the highest number of reported breaches in the world. In 2018, more than 36,000 incidents were reported from this region, the highest in the world. Along with this statistic, Gartner presentations revealed that the region also has the highest mean time to identify the breach. At 260 days, it is the highest in the world. What are the weaknesses in organisations that allow such a high number of incidents? Post incident analysis usually reveals that prevalence and usage of weak passwords amongst end users, and especially privileged end users like administrators, is the root cause for such breaches. Most incidents that happen are not necessarily of an advanced nature, and mostly stem when threat actors or hackers are able to crack weak passwords, and gain entry into an organisation's network using

compromised credentials of end users and administrators.

Gaining entry into an organisation's network through the credentials of an actual end-user or privileged end user like an administrator, remains the easiest entry strategy for threat actors. Forrester Research points out that 80 percent of security breaches result from privileged access abuse. In the past, it used to be assumed that access granted through a login including a username and password was sufficient



Tuesday, 24th March 2020

LouLou'a Ballroom, Ritz Carlton, JBR, Dubai

https://www.tahawultech.com/govtech/2020/

Kausar Syed Group Sales Director kausar.syed@cpimediagroup.com +971 4 440 9130 / +971 50 758 6672 For sponsorship enquiries

Youssef Hariz Business Development Manager youssef.Hariz@cpimediagroup.com +971 4 440 9111 / +971 56 665 8683 Sabita Miranda Senior Sales Manager sabita.miranda@cpimediagroup.com +971 4 440 9128 / +971 50 778 2771

PLATINUM PARTNERS



Experiences That Matter

DIGITAL TRANSFORMATION PARTNER



STRATEGIC PARTNER



CLOUD TRANSFORMATION PARTNER



GOLD PARTNER

F

HOSTED BY

OFFICIAL PUBLICATION



ORGANISER







to guarantee the authenticity of the user. With the increasing sophistication of threat actors to brute force passwords to gain access, especially weak and repeated passwords, this assumption is no longer valid, and has spawned the creation of the Zero Trust model.

The Zero Trust model, first suggested by Forrester Research and National Institute of Standards and Technology in 2010, reinforces the modern belief that login identities can no longer be trusted, inside or outside the organisation, especially with the expanding threat surface. The Zero Trust model today covers the following elements with the objective of not implicitly trusting any access for any user without verification.

Networks: Verify access to segment, isolate, and control the network.

Data: Control access to secure and manage data, develop classification schemes, encrypt data at rest and in transit.

Workloads: Verify and control access to the application stack.

Devices: Verify and control access of every device on the network.

Identities: Limit the access of users

and secure users.

By limiting and securing privileged access to the above, the organisation is moving away from a perimeterbased approach

to a Zero Trust approach. The Zero Trust approach boosts prevention, detection, response, and compliance towards standards such as HIPAA, FISMA, PCI, and others. Moreover, it can be extended to the cloud, mobility, Big Data lakes, DevOps, containers, microservices, and others.

Organisations begin their Zero Trust journey with the following initiatives:

#1 Vault all privileged credentials

Access to the credentials of privileged users and privileged resources need to be secured and controlled, raising the level of security management control. Rigorous multi-factor authentication also needs to be enabled and added around privileged users and privileged resources.

AN ORGANISATION'S NETWORK THROUGH THE CREDENTIALS OF AN ACTUAL END-USER OR PRIVILEGED END USER LIKE AN ADMINISTRATOR, REMAINS THE EASIEST ENTRY STRATEGY FOR THREAT ACTORS."

#2 Consolidate identities and introduce least privilege

All identities need to be consolidated to eliminate redundant ones at the same time

limiting privileges to the minimum required to get the work done. Along with limiting privileges, workflows need to be limited in the similar manner to restrict lateral user movements.

#3 Hardening the environment

Once the above two initiatives have been implemented, the organisation can move to the next level of compliance. This can include introduction of air gapping around hardware and resources, usage of host-based intrusion detection systems, and development of advanced behavioral analytics.

By going through these steps, organisations can ensure they are no longer vulnerable in the area of security breaches and password theft.



Recognising excellence in security

Security Advisor Middle East CISO 50 Awards recognise 50 top organisations and the people within them that have delivered groundbreaking business value through the innovative application of risk & security concepts and technologies.

#CISO50

www.tahawultech.com/ciso50/2020

CLOUD TRANSFORMATION PARTNER



GOLD SPONSOR



SILVER PARTNERS





OFFICIAL PUBLICATION



ORGANISER

CPI MEDIA GROUP

HOSTED BY



DON'T LET DATABERGSING YOUR BUSINESS

JOHNNY KARAM, REGIONAL VICE PRESIDENT, EMERGING REGION, VERITAS TECHNOLOGIES, DISCUSSES WHY GETTING RID OF ROT CAN HELP GROW YOUR BUSINESS.

ig data holds the power to fuel transformational growth, yet, as a World Economic Forum report on 'Data-Driven Development' observes, we live

in a 'fog of data ignorance.'

Today, advanced analytics is being used by organisations to inform strategic decision-making and steer their business into new levels of enhanced productivity and efficiency. It's also being used to improve consumer experience, leading to higher satisfaction and brand loyalty in the long-term. Just think of ridehailing apps like Careem and Uber, or food delivery apps like Deliveroo and UberEATS – by using real-time data analytics, they are able to anticipate their customers' likes and preferences and stay one step ahead of the game.

The challenge in data management

Yet, when it comes to understanding the complexities of data management, there has been very little concerted action on it. Latching on the cloud bandwagon or having 'data analytics' as an add-on



function brings little value unless the data at your command is extrapolated and used effectively.

And that is a challenge that many organisations in the UAE face. Our Value of Data study earlier this year identified that organisations in the UAE are losing an average of \$2.1 million every year due to challenges in day-to-day data management, in addition to a loss of more than one hour daily in trying to locate data.

Building further on the study, our 2019 Middle East Databerg Study surveyed 100 IT leaders across multiple sectors and job roles in the UAE, to dig deeper into how they manage data and its impact on their overall business strategy.

Rise of 'databergs'

The key finding of this report is that many UAE businesses are failing to adequately manage their dark (unclassified) and Redundant, Obsolete or Trivial (ROT) data, leading to voluminous 'databergs' that not only slow cloud adoption but also unnecessary cost inefficiencies.

With 88 percent of total company data in the dark and ROT realm, respondents said they are failing to reach their own targets for cloud migration. Compared to last year's prediction of cloud storage uptake at 55 percent, the actual uptake this year was just 45 percent - ten percent lower than anticipated!

This continued prevalence in the volume of dark and ROT data is a matter of concern. Between 2016 and 2019. while there wasn't much change in ROT and dark data management. The amount of ROT and dark data decreased by only two percent over the three years while the amount of clean data

"AS THE REGION MOVES TOWARDS THE CLOUD THE LACK OF SYSTEMATIC AND STRUCTURED EFFORTS TO CUT DOWN DARK DATA IS ALSO IMPACTING THE CONFIDENCE OF IT PROFESSIONALS IN MIGRATING THEIR DATA TO THE CLOUD AS QUICKLY AS THEY NEED TO."

spiked just three percent. This underlines a missed opportunity in harnessing the power of data for enhanced business efficiency and competitive advantage.

As the region moves towards the cloud – with Microsoft having opened its first cloud data centre region in the UAE in 2019 – the lack of systematic and structured efforts to cut down dark data is also impacting the confidence of IT professionals in migrating their data to the cloud as quickly as they need to.

With the UAE focused on digital transformation, underpinned

UAE FIRMS LOSE AN AVERAGE OF

EVERY YEAR DUE TO DATA

MANAGEMENT CHALLENGES

by the country's initiatives such as the UAE Strategy for Artificial Intelligence and Emirates Blockchain Strategy 2021. the need to rapidly tap into data, to garner its true significance and value, cannot be overstated.

www.tahawultech.com

Reasons for poor data hygiene

Poor data hygiene arises from a number of factors, including slow data deletion, with only 15 percent of organisations deleting data weekly, according to the research. Further, nearly two-thirds of organisations are wasting money on orphaned data with only 33 percent of the respondents stating they had a regular process to reclaim and repurpose orphaned capacity.

This is compounded by the threat dark and ROT data poses to organisational security with many of the UAE organisations surveyed stating that they are running high levels of risk around ransomware.

A quarter of the businesses said it would take them a week to recover from a ransomware attack. Just 55 percent of businesses are prepared for ransomware attacks and have backup and recovery plans in place.

Digital data hoarding is becoming increasingly commonplace and a 'fear of deleting' mentality ultimately costs companies a huge amount of money in the storage and protection of volumes of data that may no longer hold any value to the organisation but does create unnecessary increased risk. This money would be better spent in securely storing and protecting the data that holds value and is mission-critical.

With the findings confirming that data hoarding is increasingly becoming the cultural norm in the UAE, a fundamental shift in mindset is needed to prioritise data as a business-critical function.

Three steps to remove 'data fog'

To remove 'data fog', improve data management and reduce complexities within their IT environments, organisations should aim to:

Shed light on dark data by removing any vulnerabilities in the system. Storage environments must be managed proactively to identify dark data and classify it – which will also help generate insight on how storage resources are consumed and thereby help optimise the process.

Ensure that storage costs are managed by regularly deleting ROT data. A failure to do so, before the entire data (including ROT) is moved to the cloud, will mean higher expenses that are avoidable in the first place.

OF ORGANISATIONS HAVE

EITHER DARK OR ROT

DATA

Move towards a hybrid model that will help balance the IT budgets in addition to bringing more savings on storage costs, as well as improving backup and ransomware abilities. "DIGITAL DATA HOARDING IS BECOMING INCREASINGLY COMMONPLACE AND A 'FEAR OF DELETING' MENTALITY ULTIMATELY COSTS COMPANIES A HUGE AMOUNT OF MONEY."

These measures will help navigate spiralling IT costs and missed opportunities arising from poor data management. Further, prioritising the optimisation and protection of valuable, missioncritical data, while illuminating dark and deleting ROT data, will help boost operational efficiencies and support the organisation in its digital transformation with greater efficiency.

As the saying goes – prevention is better than cure. Organisations that are proactive in ensuring that data that is highly available, protected regardless of where it sits in the organisation, with the ability to provide insights that enhance operational efficiency and regulatory compliance,

> will be the ones that thrive in today's digital economy. With 'smart cities' being driven by regional governments across the Middle East region, businesses must step up the game and invest in properly managing their most valuable digital asset: their data.



Huawei HoloSens IVS Intelligent Video System

Central Cloud

Lite Cloud

Micro Cloud

Collective intelligence

Converged intelligence

Compact size highly intelligent



Contact Us: enterpriseME@huawei.com e.huawei.com/ae

CUTY SECURITY

eufyCam 2 1080p Wireless Security Camera

Protects You, Your Family and Your Privacy





Night Vision



48HRs **Backup Battery for**

HomeBase



 \odot

100dB Siren Anti-Theft Protection Full HD

, 1080⋼

Amazon Alexa

Google

በ

AES 256

Assistant

CUFY SECURITY

FREE

ENCRYPTED LOCAL STORAGE

Military-Grade Encryption

1 Charge =

Days

Q Two-Way Audio

Apple Home Kit

eufy Security Range of Products







eufycam 2C 2+1 kit T8831



eufy Floodlight Cam T8420



eufy Doorbell 2K with Homebase E8210



Available at





MULLER & PHIPPS

Sharaf DC.com

