

THE NEW NORMAL

Navigating cybersecurity and remote working in the time of COVID-19





TOUCH-FREE, ACCESS IS EASIER THAN EVER

FACE RECOGNITION TERMINAL

- Access Control and Time Attendance Tracking
- Better Security and Improved Efficiency
- Accuracy Rate Over 99% and Recognition Speed Under 0.2 Seconds
- Fast Recognition in Low-light Environments Even in Complete Darkness



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



CONTENTS



How the coronavirus pandemic is impacting cybersecurity and the future of work

8

MOVERS AND SHAKERS

The latest people movement in the regional security industry

18 SECURITY AT YOUR FINGERTIPS

Smartphones are becoming increasingly vital in the way we do business, how can organisations keep mobile security threats at bay?

22 FUELLING SECURITY Industry experts discuss the

Industry experts discuss the cybersecurity challenges that oil and gas professionals should be aware of

28 ADVANCE GUARD As private cyberoccurity

As private cybersecurity organisations' roles in policing the cyber space grow, is there a need for increased regulatory control for this sector?







34 CYBERSECURITY TRENDS FOR 2020

Kaspersky's Amir Kanaan highlights the latest trends that will impact the ever-evolving cybersecurity space

38 CONNECTED CARS, CLOUD AND CYBERSECURITY

AWS on why cloud is vital in enabling the secure and seamless deployment of autonomous cars

OUTY SECURITY



OUFY

SECURITY

 $\left[\mathcal{S} \right]$

Human

Dectection

Night Vision

48HRs **Backup Battery for** HomeBase

100dB Siren Anti-Theft Protection Amazon Alexa

Google

Assistant

Apple Home Kit

eufy Security Range of Products



eufyCam 2 2+1 kit T8841



eufycam 2C 2+1 kit T8831



eufy Floodlight Cam T8420



eufy Doorbell 2K with Homebase E8210



Available at











EDITORIAL



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

Adelle Geronimo Editor

EVENTS



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

STAY SAFE, STAY SECURE

In the recent weeks, the way we live.

work, learn and connect have changed in unprecedented ways owing to the coronavirus (COVID-19) pandemic. With over 2 million confirmed cases globally, COVID-19 presents not only a tremendous public health predicament but also an economic crisis.

As cities shut down and people engage in social distancing as a response to curb the outbreak, many individuals and organisations are embracing technology to cope to what currently seems to be the new normal.

As the pandemic continues to proliferate, dependency on digital tools multiplies. However, while organisations are busy devising new methods to keep their businesses afloat - making sure they are still running during and after the lockdowns - many are likely to neglect cybersecurity. Unfortunately, cybercriminals are also taking advantage of the situation. In the past few weeks, there has been a significant rise in coronavirusthemed websites, with more than 30,000 new domains registered. The number of social engineering

attacks have also increased exponentially as threat actors try to exploit remote workers. In this month's Security Advisor ME, we spoke to industry experts on how organisations can address the cybersecurity challenges in the time of COVID-19, many of which have noted network security and phishing attacks as the biggest cyber threats today. For more on this, go to page 12.

For organisations operating with fully remote workforces, it is essential to take measures to protect your employees by keeping them aware on how they can secure their devices and home networks. It is also imperative to help them understand the

"JUST AS WE'RE PRACTICING **MEASURES TO PREVENT THE SPREAD OF THE CORONAVIRUS IN** THE REAL WORLD. WE SHOULD ALSO **DO OUR BEST IN KEEPING THE BAD GUYS AWAY IN THE CYBER WORLD.**"

cyber risks and how they can avoid falling victims to phishing and malware attacks. As what's been in reiterated in the past. cybersecurity is everyone's responsibility. Just as we're practicing measures to prevent the spread of the coronavirus in the real world, we should also do our best in keeping the bad guys away in the cyber world.

Stay safe everyone!

Published by

CPI MEDIA GROUP

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

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.

EDITORIAL Online Editor Adelle Geronimo adelle.geronimo@cpimediagroup.com

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

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

+9714 440 9135

Sharon Saldanha

DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com +971 4 440 9140

Designer Mhar Delaben marlou.delaben@cpimediagroup.com +971 4 440 9156

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

DIGITAL SERVICES Web Developer Abbas Madh

Photographer Charls Thomas

+971 4 440 9100

webmaster@cpimediagroup.com

Jefferson de Jova

Maksym Poriechkin

OOREDOO ACCELERATES CYBERSECURITY IN OMAN WITH NEW DEAL

Ooredoo, the digital partner of choice

for businesses in Oman, has entered into a strategic partnership with the National Security Services Group (NSSG) to deliver enhanced cybersecurity in the Sultanate.

The agreement, which was signed by Abdul Razzaq Al Balushi, CFO and NSSG Chief Executive Officer, Talal Al Zubair, will facilitate the joint delivery of cybersecurity services and cybersecurity consultancy, such as architecture security consultancy, phishing tests and vulnerability assessments to businesses in Oman.

It is the latest partnership to be added to Ooredoo's growing B2B portfolio, which helps business of all kinds meet the increasing demands of the digital environment.

Talal Al Zubair, NSSG Chief Executive Officer at NSSG, said, "As the country works towards achieving its grand vision of 2040, our vision in parallel strives to ensure this journey remains safe and secure. We are pleased to be joining hands with Ooredoo as we seek to fortify the nation through security, awareness, and innovation for a resilient digital future for Oman."

REMOVING ADMIN RIGHTS CAN HELP MITIGATE MICROSOFT VULNERABILITIES: STUDY



MOREY HABER, BEYONDTRUST

BeyondTrust has released the seventh

edition of its Microsoft Vulnerabilities Report, which showed provides the latest annual breakdown into security vulnerabilities facing organisations today.

The report also shows a fiveyear trends analysis to better equip organisations to increase their IT security posture and keep networks and systems safe.

Key findings of the report include statistics showing that during the

past year, a record-high number of 858 Microsoft vulnerabilities were discovered and the number of reported vulnerabilities has risen 64 percent in the last five years – from 2015-2019. It also revealed that removing admin rights from endpoints would mitigate 77 percent of all Critical Microsoft vulnerabilities in 2019.

The report also noted that 100 percent of critical vulnerabilities in Internet Explorer would have been mitigated by removing admin rights.

"The rate at which vulnerabilities are increasing is a significant concern for organizations committed to protecting their networks from data breaches," said Morey Haber, CTO and CISO, BeyondTrust. "Recent global events have highlighted the critical need to continue to focus on information security. The ability to remove admin rights and control applications is no longer difficult to achieve, and least privilege should always be considered as part of a proactive security strategy."

DUBAI WARNS AGAINST HEIGHTENED RISKS OF CYBER-ATTACKS



The Dubai Financial Services

Authority (DFSA) has called on financial institutions to stay vigilant as cyber-attacks, phishing attempts and fraud increase amid the coronavirus pandemic. "Firms in the DIFC firms are called to register to use the DFSA Cyber Threat Intelligence Platform (TIP) and make use of the cyber threat information available on TIP to enhance their cybersecurity," the organisations said in a statement.

The organisation has also highlighted that it continues to closely assess and address the implications of the evolving situation of Covid-19 crisis.

According to the DFSA, it will take all necessary proactive and precautionary measures to help Dubai and the UAE in their efforts to contain the spread of Covid-19 and will continue to work closely with all government agencies in that respect.

As the DIFC is a global hub for financial services, the DFSA noted that it is in close and regular contact with local and international supervisory bodies.

"As we have learned from our work in cyber resilience, public/private partnerships will provide the best path for solutions to this issue. The measures are vital to ensuring that the UAE and the DIFC, along with other markets around the globe, can recover when the current situation eventually passes," said DFSA.

THOMA BRAVO COMPLETES \$3.9 BILLION ACQUISITION OF SOPHOS

Sophos has announced the completion

of its acquisition by Thoma Bravo, a global private equity firm focused on the software and technology-enabled services sectors, in a cash transaction that values Sophos at approximately \$3.9 billion.

The acquisition offer was announced on 14th October 2019.

Under the terms of the agreement, Sophos stockholders receive \$7.40, per share. The price per share represents a 168 percent premium to its IPO share price in June 2015. Stockholders voted to approve the transaction on Dec. 3, 2019. With the completion of the acquisition, Sophos' common stock has ceased trading on the London Stock Exchange.

"Sophos is excited to work with Thoma Bravo as we begin our next chapter of growth and success, continuing in our KRIS HAGERMAN, SOPHOS



mission to deliver the world's most effective next-generation cybersecurity technology," said Kris Hagerman, CEO, Sophos.

"Our transition to become a fully next-gen cybersecurity leader continues to rapidly progress. Last quarter, our next-gen product portfolio represented over 60 percent of our entire business, and grew 44 percent yearover-year. And very recently, we launched our most significant network security technology ever, the Sophos XG Firewall with Xstream architecture. With Thoma Bravo as a partner, we believe we can accelerate our progress and get to the future even faster, with dramatic benefits for our customers, our partners and our company as a whole."

SANS OFFERS FREE KIT TO SECURE HOME WORKERS

Coronavirus has caused organisations

around the world to transition their workforce away from an office environment to work from home. Yet, many organisations lack the policies, resources or training to enable their people to do so securely.

In response, SANS Security Awareness, a division of the SANS Institute, has created the "Securely Working from Home" Deployment Kit. This free kit provides security awareness professionals with a step-by-step guide on how to rapidly deploy a training programme for their remote staff. All training materials and resources necessary to secure a remote, multi-lingual workforce are included in the kit.

SANS Director of Security Awareness Lance Spitzner said, "The training materials are a combination of both our public resources and paid training materials. This comprehensive kit includes videos, infographics, podcasts, newsletters



LANCE SPITZNER, SANS

and digital signage in multiple languages all bundled in a single package that we are providing as a free resource to all who need it. We understand that this is a unique situation and we want to do everything we can to help the community secure their workforce during these uncertain times."

For additional details on SANS Security Awareness training, visit: https://www.sans. org/security-awareness-training

NEW HACKING GROUP TARGETS INDUSTRIAL FIRMS: KASPERSKY

Kaspersky has recently uncovered a new

hacking group that is currently targeting organisations in the industrial sector.

The cybersecurity firm's Global Research and Analysis Team (GReAT) team has noted that the group, which has been dubbed as WildPressure, has launched a campaign to distribute Milum—a malicious Trojan that gains remote control of devices in various organisations, including those representing the industrial sector.

So far, the team was able to identify several, almost identical samples of the "Milum" Trojan that share no code similarities with any known malicious campaigns. All possess solid capabilities for remote device management, meaning once a system is affected, an attacker can take control from anywhere.

Kaspersky's GReAT team first witnessed the spread of the "Milum" Trojan in August 2019. The analysis of the malware's code showed that the first three samples were created in March 2019. Based on available telemetry, Kaspersky researchers believe most of the targets of this campaign are located in the Middle East, and the campaign itself is still ongoing.

Unfortunately, much is still unclear about this campaign, including the exact mechanism of how Milum is spread.

OF ALL PRIVILEGE ACCESS ANOMALY BEHAVIOUR DETECTIONS COME FROM POTENTIALLY MALICIOUS PRIVILEGE ACCESS FROM AN UNKNOWN HOST

SOURCE: VECTRA

FORCEPOINT TO ACCELERATE CLOUD-FIRST Security Strategy With New CPO



Forcepoint today announced Nico Popp has joined the company as Chief Product Officer (CPO). In this newlycreated role, Popp will oversee the global execution and strategic evolution of Forcepoint's behavioral-based cloud security platform. This will include leadership of all product development, management and innovation, such as Forcepoint X-Labs, at the company while also leading the strategic integration of the overall product and customer experience to empower Forcepoint's global customers for success.

A cloud-technology veteran, Popp brings more than 15 years of cloud operations and product development experience to Forcepoint. "The race to embrace digital transformation has created enormous opportunities for global enterprises today. However, with these significant business productivity comes an added layer of security complexity. This complexity can only be addressed by moving traditional security to the cloud. Forcepoint is uniquely positioned to capture this industry shift towards security-as-a-service," said Popp.

SENTINELONE APPOINTS NEW CHANNEL CHIEF TO DRIVE EMEA EXPANSION

SentinelOne, the autonomous cybersecurity

platform company, has appointed cyber industry veteran Roland Stritt as Senior Director of Channel for EMEA.

As part of his new role, Stritt will be responsible for driving channel engagement across the EMEA region to deliver hyper growth and value for SentinelOne's growing community of committed partners. The move comes in the wake of a string of positive developments for the company, including \$200 million in new Series E funding, the appointment of Daniel Kollberg as VP EMEA, and the recent unveiling of the unique, AIpowered Singularity XDR platform.

With two decades of experience in senior sales and partner management roles at cyber and infrastructure vendors including Palo Alto Networks, Roland Stritt joins SentinelOne from Rubrik where he was formerly Director of EMEA Channels:

"Being closely aligned to the cybersecurity market for over 20 years, you understand



ROLAND STRITT

when a truly disruptive, unique and original technology comes along – this is exactly what SentinelOne represents and the opportunities are very exciting," said Stritt.

"The SentinelOne sales growth through 2019 and into 2020 has been remarkable, particularly in EMEA, and the timing is right to introduce a focused partner programme that recognises the expertise and commitment that existing and new partners bring to the table, and gives them all the support they need to be successful."

INDUSTRY VETERAN CHRIS PETERSON JOINS CENTRIFY

Centrify, a provider of cloud-ready

Zero Trust Privilege to secure modern enterprises, has announced the appointment of Chris Peterson as Vice President of Worldwide Channels & Alliances.

In this role, Peterson will accelerate Centrify's rapidly-growing channel partner ecosystem and will be responsible for leading all aspects the company's global channels and alliances, with an emphasis on partner alignment, demand creation, accelerated customer conversion and success.

"Our partners are essential to helping customers understand best practices for least privilege solutions, and how to best secure and manage their infrastructure as they go through cloud transformations," said Peterson. "I'm excited to join the Centrify team and optimize our partner ecosystem so we can more effectively communicate the value of an Identity-Centric approach to Privileged Access Management.



CHRIS PETERSON

That starts with providing a choice of solutions and deployment options to our customers, as well as a best-in-class selection of channel partners, technology partners and global systems integrators to reach and positively impact the enterprise and key vertical markets."

Peterson brings more than 30 years of enterprise channel, sales, and marketing experience to Centrify.

RAQMIYAT ANNOUNCES KEY CHANGE IN LEADERSHIP



Raqmiyat's board of directors has

announced the appointment of Saeed Mohammad Al Ghurair as the company's new managing director.

The company's CEO for four years Amer Khreino will be stepping down on 15th April 2020.

Saeed was elected as a board member to Raqmiyat since September 2018, since then, he was working closely with the CEO and his executive team on forming the vision and strategy of Raqmiyat 2023.

The handover process has started in early January 2020, to ensure smooth management transition. Saeed is expected to announce key new appointments in the coming few weeks, yet no immediate changes are expected on business structure, business offerings or GTM during 2020. Khreino will continue working closely with the board of directors and the designated MD, till the change management is completed.

The board of directors is committed to the growth and prosperity of Raqmiyat and hope the new appointment will only cement our market position and allow the company to further expand its operations and business.

"There has been tremendous growth and prosperity across all business lines during the past many years," said Shaikha Al Ghurair, Vice Chairman and Group Managing Director. "We are looking to cement our position further to accelerate our growth across digital banking, business transformation and IT Managed Services under the new leadership. Saeed enjoys a diverse experience across many industries, with strong leadership skills that will allow him continue our growth

Shaikha Al Ghurair, Raqmiyat

"WE ARE LOOKING TO CEMENT OUR POSITION FURTHER TO ACCELERATE OUR GROWTH ACROSS DIGITAL BANKING, BUSINESS TRANSFORMATION AND IT MANAGED SERVICES UNDER THE NEW LEADERSHIP." strategies with higher diversification and expansion. I also would take this opportunity to thank Khreino for his contribution and dedication to Raqmiyat throughout the past many years and wish him best in his future endeavor."

"It has been an honour and privilege to work with Raqmiyat, its board members and staff throughout the past many years," said Amer Khreino.

"Today, Raqmiyat enjoys a highly talented leadership dedicated to make customer experience more exciting and rewarding. The diversity of our offerings, the unique value proposition and high technical excellence remain key in retaining and expanding our customer base. I wish my successor, Saeed Al Ghurair all the best in making new successes and in taking Ragmiyat to new heights. Besides, I would like to record my appreciation and gratitude to my leadership team and all other staff members who were instrumental in transforming our business, let alone being supportive at all times. Last but not least, I sincerely wish our distinguished customers, vendors and communities all success, prosperity and above all safety, in such extraordinary times."

BUILDING A SECURE DIGITAL FUTURE

FREDY ISSA, SENIOR MANAGER – SURVEILLANCE AND SECURITY SOLUTIONS – MERAT, DELL TECHNOLOGIES, DELVES INTO THE NEED FOR MODERN IT INFRASTRUCTURES IN ENSURING THE SUCCESS OF SMART AND SAFE CITIES, AND DISCUSSES THE COMPANY'S ROLE IN ACCELERATING THE UAE'S DIGITAL FUTURE.

an you give an overview of Dell Technologies' surveillance solutions? Surveillance technologies are

becoming increasingly demanding and complex, particularly given the large spaces that organisations need to secure in today's world and the regulatory compliance that poses additional challenges. Dell Technologies' surveillance solutions have been developed with all of these nuances in mind. We have combined optimised hardware and software for surveillance needs along with management and orchestration capabilities to simplify the deployment of secure and scalable solutions for edge computing and IoT use cases.

Governments and private organisations across the globe are gearing up to build smarter cities, what are the challenges that they can expect?

With the rise of the smart city comes multiple benefits, some of which we

are already seeing as governments across the region embrace technology and digitalisation. However, there are a number of challenges that come with this too. Smart cities are made possible by integrating IoT, cloud computing, and big data analytics. This allows for things like intelligent transport systems, smart lighting and smart utility metering for electricity and water. These technologies and integrations are based on sensorcentered collection and analysis of data and offer innovative and cost-effective solutions to cities. Bearing this in mind. some of the challenges that governments and organisations may face revolve around technology coverage and capacity and digital security. In addition, one of the core of the technologies enabling a smart city is data, which means organisations that wish to harness the power of new emerging trends will need to take steps to effectively collect, process, store, analyse, manage and remediate data to keep up with the rapid pace of innovation.

As organisations and governments continue to adapt to the changing needs of citizens and employees, now more than ever, it is important to ensure that investments are made to modernise infrastructures and prepare for the future. Being dependent on legacy systems will stem organisations from being fully future-proof and will hinder customer and employee retention. Therefore, if organisations are to take advantage of emerging and transformative technology trends, infrastructures need to be set in place to accommodate them.

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

Dell Technologies provides advanced technologies essential for the digital transformation of the country. We enable the transformation of the country's safety and security by delivering innovations such as the Dell IoT Surveillance Solution and the Dell OEM computer vision solutions. Through these offerings, we aim to help the nation become future proof by supporting it in adapting to the changing demands in IT advancements and increasing the reliability of the systems quarding the country's security. A great example of our work in the UAE is our partnership with DEWA in Dubai. DEWA requires IoT technologies to connect solar energy to houses and buildings; smart applications that use smart meters and grids that contribute to fast-service connection, predictive analytics for fast response, and for proper energy use rationing. Dell Technologies is their foundational partner and has worked with them to facilitate this transition.

Mega events around the world are increasingly becoming connected as they utilise more advanced technologies, how has this trend impacted demands for smart surveillance?

With more and more mega events being planned globally, and the sheer volume and scale of data that needs to be analysed as part of surveillance

"WE ENABLE THE TRANSFORMATION OF THE COUNTRY'S SAFETY AND SECURITY BY DELIVERING INNOVATIONS SUCH AS THE DELL IOT SURVEILLANCE SOLUTION AND THE DELL OEM COMPUTER VISION SOLUTIONS." requirements, organisations now need a surveillance solution that can integrate surveillance data as well as business data, while being resilient, scalable and reliable.

Dell Technologies' IoT Solution for Surveillance has strongly integrated compute, storage, networking and virtualisation resources. This improves system performance and lowers total cost of ownership – allowing organisations and venues that cater to these mega events to reach time-to-value faster. It is purpose built to a complex camera-on-cloud infrastructure with support for demanding. mixed data sources including video, audio, barometric pressure and more. Our solution takes the complex surveillance requirements of these mega events into account and allows for automated deployment, centralised management and massive ondemand scalability while also minimising downtime and increasing system reliability.

What can regional customers expect from Dell Technologies this 2020?

Dell Technologies' end-to-end portfolio captures essential services of edge, cloud, IoT, surveillance and unique OEM capabilities. We will continue to maintain focus on smart surveillance and ensure a broad ecosystem of partners and solutions catering to the security requirements in the region through advanced video and sensor services. We're also currently focused on supporting organisations with business continuity; our research indicates that a decade from now, organisations that successfully achieve digital workplace transformations will be at an advantage over businesses struggling with legacy systems, massive amounts of data and workforces unprepared for change. Therefore, we are committed to helping organisations to modernise their IT systems and deploy next-generation technology infrastructure, which will lay the groundwork for their digital-future. 1

THE NEW NORMAL

THE CORONAVIRUS (COVID-19) PANDEMIC HAS FORCED BUSINESSES TO UNDERGO SEISMIC CHANGES IN THE WAY THEY OPERATE. AS FLEXIBLE POLICIES BECOME STANDARD AND REMOTE WORK BECOMES A NORM, ANOTHER IMPORTANT CHALLENGE IS TAKING THE SPOTLIGHT – CYBERSECURITY. he coronavirus pandemic presents a tremendous health crisis that nations across the globe are grappling with. With over 2 million confirmed cases of infected people globally, the virus is

causing a huge impact on people's lives, families and communities.

In addition to being a major public health issue, the COVID-19 crisis also brings about profound social and economic consequences, according to the World Health Organisation (WHO) Director-General Tedros Adhanom Ghebreyesus.

Crisis-response efforts are in full motion in many countries across the world. Healthcare organisations are explicitly increasing their capacities and maximising their resources to cope with the rising demands to contain the virus. Educational firms are shifting to online platforms to ensure ongoing learning opportunities. Moreover, companies are rapidly adopting new ways to operate to maintain their businesses, many of which have been compelled to embrace remote working.

However, with the coronavirus not showing any signs of slowing down anytime soon, enterprises are faced with the challenge of having to juggle a range of new systems priorities such as ensuring the stability of critical business processes, workforce productivity and, of course, cybersecurity.

Security Advisor ME speaks to industry experts to get their insights on how the pandemic is impacting cybersecurity and the future of work.

RISKS AND CHALLENGES

For many businesses, the move to a remote working model came too swiftly. Rather than being able to transition gradually, the quarantine measures demanded a quick response, which has left CIOs and CISOs with little time to prepare and address the cybersecurity challenges for remote working.



Harish Chib, Sophos

"NORMAL REMOTE WORKING IS NOT A CHALLENGE AS IT GIVES ORGANISATIONS TIME TO IMPLEMENT IT. THE CURRENT SCENARIO DUE TO COVID-19 IS DIFFERENT. THIS REMOTE WORKING IS RAPID, FORCEFUL AND UNPLANNED AND MANY ORGANISATIONS HAVE RELAXED THEIR CYBERSECURITY CONTROLS DUE TO THIS." The huge amounts of global uncertainty

and change that organisations are facing are what criminals are seeking to capitalise on, according to Harish Chib, vice president – MEA, Sophos. These risks are further amplified by the immediate and unforeseen IT challenges that companies are having to ensure their staff can work from home.

"Normal remote working is not a challenge as it gives organisations time to implement it," says Chib. "The current scenario due to COVID-19 is different. This remote working is rapid, forceful and unplanned, and many organisations have relaxed their cybersecurity controls due to this. There are two areas which are most likely to result in a cybersecurity incident due to the ongoing crisis: remote access and phishing."

With a majority of employees working from home, business networks have been exposed to countless untrusted networks and unsanctioned devices.

"When employees connect to their corporate networks from home, they expose numerous access points for hackers to exploit," says Subhalakshmi Ganapathy, Product Evangelist, ManageEngine. "These unprotected endpoints extend the corporate network perimeter, which increases the attack surfaces for the hackers."

Ideally, whenever an employee is working remotely, they should be accessing their organisation's network and any software-as-a-service (SaaS) resources they need via a virtual private network (VPN).

A VPN creates a safe, encrypted 'tunnel' from the user network, whether public or private Wi-Fi, across the public internet, and into the organisation's network.

According to Ganapathy, often enterprises don't have segment or limit their networks for VPN use as they are usually utilised by internal employees and/or trusted third-party vendors. However, with the sudden shift to remote working, most IT teams wouldn't have had the time to segment their network for the large VPN usage.

"This could lead to channels used for remote connections such as VPNs and other remote access platforms having umpteen security vulnerabilities that could be exploited by the hackers. A simple phishing attack on an unsecured network can expose the entire sensitive data of your company," she explains.

THE HUMAN ELEMENT

More critically, IT and security leaders need to bear in mind that attackers will first and foremost take advantage of human weaknesses.

In the last few weeks, there has been an increase in the number of incidents of individuals receiving a variety of emails, which impersonate authorities such as the WHO to persuade victims to download software or donate to bogus causes.



Robert Huber, Tenable

"SECURITY TEAMS SHOULD LOCK ARMS WITH IT TO SECURE ALL SOFTWARE-AS-A-SERVICE (SAAS) APPLICATIONS VIA CLOUD ACCESS SECURITY BROKERS FOR CONFIGURATION, SECURITY AND DATA LOSS PREVENTION."

Google's Gmail, which is being used by over 1.5 billion users globally, has blocked around 18 million hoax emails related to COVID-19 since the outbreak began.

There have also been numerous cases of coronavirus-themed emails being sent out, which have been designed to look like they came from an organisations' leadership team but are embedded with malware that would infect corporate networks.

"Humans are the weakest links in the security ecosystem," says Sam Curry, Chief Security Officer, Cybereason. "Today, the biggest blunders include opening email attachments that end up being laced with malware or ransomware, visiting dubious websites or downloading malicious software. The CEO of a company shouldn't be emailing you a message asking for you to wire transfer \$1 million to an account to deal with COVID-19. That should raise a red flag with any employee these days, but there are countless examples of this happening over the years."

Curry further notes that even as companies ramp up their security awareness programmes, the overall task of educating employees on the do's and



don'ts to reduce corporate risk remains a constant challenge.

Werno Gevers, cybersecurity specialist, Mimecast, says, "There is a general escalation in cybercrime during times of heightened disruption."

"Already, malicious actors are spreading disinformation with the sole purpose of creating panic. People are desperate to find out more about the crisis and are letting their guards down, clicking on just about anything sent to them. Even one misclick on a link could initiate malware and put the user – and the organisation – at risk.

"Webmail and private emails are unencrypted, leaving employee devices at significant risk of compromise via interception or 'man in the middle attacks,' and can make home networks



vulnerable to compromise as attackers may piggyback on these end-users to compromise an otherwise secure environment," he adds.

However, Centrify regional director for Northern, Southern Europe, Middle East and Africa Kamel Heus points out that one of the most common risks that organisations make is focusing only on securing remote access for regular employees. They often forget about the privileged users such as management teams, IT staff and database administrators among others, who often have privileged access to critical infrastructure and sensitive data.

"Those are the credentials that cyberattackers are most commonly after since they offer the most power and ability to move laterally, find and extract data, and sell it for profit," he says.

"They also forget about securing outsourced IT and other third-parties who are not employees but may have elevated privileges. Many times, those third parties are simply using a VPN to access the network, which leaves a gaping hole in the security of the enterprise. IT staff, whether employees or consultants, need to have secure remote access for privileged users that

goes above and beyond the solutions being made to the collective at-home workforce."

This being said, CIOs and CISOs need to ensure that their workforce maintains a comprehensive understanding of the cybersecurity risks. "It is hard to build a cybersecurity culture with employees and user slack is quite certain to take place," says Rohit Bhargava, Practice Head - Could & Security of Cloud Box Technologies. "Not every employee understands the risks that the organisation could encounter equally.

Bhargava emphasises that IT and business leaders need to look at training and cybersecurity awareness to be as regularly as possible. "Employees must be made aware of phishing emails and ransomware attacks, which must be reported in real-time to the concerned IT experts. There should be better systems in place to manage user sessions and strengthen IT processes and audits to ensure that information leaks are prevented."

NEW PLATFORMS

In order to maintain productivity and ensure business continuity, organisations have also opted to deploy new applications to allow users to perform work-related tasks remotely. However, the rapid escalation of the pandemic has left them with little

"Many companies that did not initially have remote work capabilities have rushed to use consumer-grade solutions like Zoom, Facebook and many others," says John Pescatore, director of emerging security trends, SANS. "Zoom has recently admitted it wasn't ready for this level and type of use and is focusing 100 percent on security and has already taken some steps. Also, users are often

time to prepare the security measures in

utilising such platforms.

sharing or storing business-sensitive information on these services, which increases the odds it will be exposed."

A majority of new home workers have also adopted third-party applications and use non-corporate remote access tools such as GoToMyPC and TeamViewer, which increases the risks of data breaches.

"Use of unapproved cloud storage makes it more difficult to detect attackers that are trying to exfiltrate data," says Matt Walmsley, director – EMEA, Vectra. "It also creates regulatory and compliance issues." "It is possible there will be heavier use of cloud-based storage (OneDrive, Google Drive, etc.) rather than corporate file servers to share information. This means more valuable information could be placed into cloud storage than would have with most workers on-prem. The way that the remote host is connected will impact what level of cloud storage visibility is available," he explains.

Walmsley reiterates that security teams must rigorously identify, understand and protect the newly expanded attack surface that the move to increased remote working has created.

Digital Guardian VP for Cybersecurity Tim Bandos shares these views as well, saying that with the rapid transition to remote work, data sharing has become a bit of a nightmare for organisations and their employees.

"With the right tools in place, transferring large files while at work may have been easy in the past," says Bandos. "Without these tools, employees may look for workarounds if they're unable to use corporate email. Employees may be tempted to leverage sites that are typically blocked while at work such as Dropbox or Box. These workarounds can add risk when it comes to exposing an organisation's sensitive data to the outside world. It's essential to educate employees on the risks associated with how data is transferred and offer them the tools they need before they go out on their own looking."

Furthermore, Bandos points out that inter-office chat platforms can come with inherent risks as well. "Companies that don't subscribe to an industry-recognised service like Slack or Microsoft Teams could be in danger of having data exposed. Chat platforms like WeChat, Telegram, Viber and the likes are all free but when it comes to experience and security, namely end-toend encryption, users' mileage may vary.

"Additionally, phishing attacks are no longer just an email issue. If you can be contacted by individuals outside your organisation via these apps, the platforms can open the door for phishing scams," he adds.

NEXT STEPS

So, what kinds of tools and solutions can organisations utilise to ensure cybersecurity amid the COVID-19 pandemic?

According to Help AG CTO Nicolai Solling, one of the key elements of a robust and secure work-from-home strategy is secure remote access as working remotely radically changes how users, services and data are protected. "As a bare minimum, any remote access solution should offer two-factor authentication (2FA)," he says. "2FA combines something the user knows – like

a password – with something that they have. Today, 2FA can be easily delivered as a smartphone app. It is quick, easy and cost-effective to deploy."

But it is important to understand that when evaluating your remote access solution there's no 'one-sizefits-all' solution.

"You may even have existing IT investments which can effectively support your remote workforce when evaluated and re-purposed correctly," explains Solling. "In these unprecedented times, several technology vendors have provided promotional programmes and extended licenses to help organisations overcome security challenges. With the support of a highly-skilled implementation and support partner such as Help AG, most of these solutions can be delivered with extreme speed and with fantastic security features." Robert Huber, chief security officer, Tenable, says, "Security teams should lock arms with IT to secure all softwareas-a-service (SaaS) applications via cloud access security brokers for configuration, security and data loss prevention. In tandem, integrate all SaaS solutions into one central identity and access management solution. This will not only save time but also reduce headaches too."

THE FUTURE OF WORK

If done correctly and securely, remote working can yield a range of benefits for both employers and employees.

"The COVID-19 pandemic has forced many companies to have to enable and exponentially ramp up remote working, for a vast majority of their workforces," says Marco Marco Rottigni, chief technical security officer, EMEA, Qualys.

"This has highlighted several risks which would otherwise not have been considered if remote working had been approached as an IT project. I believe that this experience will bring a better awareness in companies and among employees about the huge advantages of smart working; this will hopefully increase the overall operational efficiency once this crisis is behind us. Organisations will also gain a better understanding of the importance of SaaS



Marco Rottigni, Qualys

"I BELIEVE THAT THIS EXPERIENCE WILL BRING A BETTER AWARENESS IN COMPANIES AND AMONG EMPLOYEES ABOUT THE HUGE ADVANTAGES OF SMART WORKING; THIS WILL HOPEFULLY INCREASE THE OVERALL OPERATIONAL EFFICIENCY ONCE THIS CRISIS IS BEHIND US." to leverage business and IT processes."

In the past, remote employees often report flexibility and focus as the biggest benefits, which enables their productivity. It has also proven to be the best resort for many businesses who want to ensure the continuity of their activity amid the pandemic.

"We think that this crisis will drastically change the working habits in many organisations, and some of them might find advantages in remote working," says Asif Hashim, Middle East Business Manager, WALLIX. "Employees might enjoy the extra time at home, and employers might find that it reduces costs. If organisations opt to continue with this way of working moving forward, this will most likely increase the use of cloudbased services and remote connection tools and therefore make organisations more vulnerable to security breaches."

Remote working might not be the right option for everyone. But if the future of work drives a big portion of workforces to work remotely, then organisations will have to develop new solutions to the challenges of working remotely.

"Remote work is not the norm in many cultures and regions," says Huber from Tenable. "While I do not anticipate a monumental shift to remote work as a result of the crisis, it will certainly become a valid option for business continuity events. This will, however, require additional security policies, solutions and education to ensure that the same protections applied within an office will be sustained when working remote."

Whether this is the future of work for businesses is yet to be determined. However, in this unprecedented new reality that we're in, we are witnessing a dramatic restructuring of the economic and social order, which is shaping remote work as the new normal for the near term.

SECURITY ATYOUR FINGERTIPS

AS THE WORLD BECOMES MORE MOBILE, SMARTPHONES ARE BECOMING INCREASINGLY VITAL NOT ONLY IN THE WAY WE COMMUNICATE BUT ALSO IN THE WAY WE DO BUSINESS. AS SUCH, THEY BECOME REPOSITORIES FOR VALUABLE DATA THAT CAN BE TARGETED BY HACKERS AND MALWARE. SECURITY CORRESPONDENT DANIEL BARDSLEY SPEAKS TO INDUSTRY EXPERTS ON HOW TO KEEP MOBILE SECURITY THREATS AT BAY.



oday, the unveiling of a new smartphone model does not quite generate the buzz that it did a few years ago, yet manufacturers are still putting new devices onto the market at a brisk pace. Earlier this year.

we have been treated to the launch of Android mobiles including the foldable Samsung Galaxy Z Flip and Huawei P40, with the Asus Zenfone 7 and the OnePlus 8, to name but a few still to come.

For those with a few dirhams to spend on a top-of-the-range new mobile, times are still good, but many consumers and employees will, instead, stick with more modest devices, some dating back several years.

A recent survey shows how many mobile users may face cybersecurity risks as a consequence. Data from the consumer organisation *Which?* indicates that hundreds of millions of Android phones may no longer be receiving security updates, increasing their risk of falling victim to attackers.

Which? quotes Android's own information suggesting that last year there were no security patches released for devices using Android 6.0 or earlier operating systems.

Given that about 42 per cent of Android mobiles fall into this category, that works out at more than one billion devices not being updated.



Vibin Shaju, McAfee

"IF YOU HAVE CONFIDENTIAL DATA FROM YOUR BUSINESS ON YOUR MOBILE DEVICE, IT'S NOT ONLY ABOUT YOUR DATA, IT'S ABOUT YOUR ORGANISATION'S DATA." Among the malware they could be vulnerable to are BlueFrag, which uses up data and spreads further malware, as well as Joker, which can result in additional charges on a user's bill, and Stagefright, which can give ransomware hackers control over a device.

Given the scale of the threat, Which? says device manufacturers and Google should level with consumers as to how long updates will be available for and what they should do when they are no longer issued.

Marco Rottigni, chief technical security officer EMEA at the cybersecurity company Qualys, says there should be "much better attention" paid to the provision of security updates by the likes of device manufacturers and operating system providers.

"On the other side, we as users should increase our awareness that we should keep technology updated. If we're not able to do that, we're putting ourselves at risk," he says.

Morey Haber, the chief technology officer and chief information security officer for BeyondTrust, which provides privileged identity management (PIM) and other solutions, says that the updates issue is "truly a Google problem."

"In the licensing of the Android operating system, Google should enforce that vendors will incorporate security updates within a reasonable time frame from release, and that updates will be available for at least several years after the current model is end of life," he says.

"Trying to hold the device manufacturer to these service-level agreements without Google's enforcement is futile."

Haber does not, however, think that providers are obliged to provide security updates for as long as, say, Microsoft does for versions of Windows. Typically, security updates for Windows continue for more than a decade. One factor is that new mobile devices and versions of Android are released much more often than are iterations of Windows. Also, Haber notes that technology from Wi-Fi to biometrics is changing "at an accelerated rate."

"While Windows can add drivers and support for new technologies, since it is not 'married' to the hardware, mobile devices do not have that flexibility. Therefore, a shorter duration is reasonable based on the production cycle of the device," he says.

A lack of security updates on older mobiles may be a particular concern to companies whose staff use their personal mobiles for work purposes on a bringyour-own-device (BYOD) basis.

Rottigni quips that, from the perspective of chief information security officers, this can feel more like "bring your own disease."

Nonetheless, Vibin Shaju, director of sales engineering for the UK, Middle East and Africa for the cybersecurity company McAfee, which offers a free-to-download mobile security app, says that BYOD is "becoming very popular."

"We see more and more applications are getting a business use. If you have confidential data from your business on your mobile device, it's not only about your data, it's about your organisation's data," he says.

Shaju says devices that are not receiving regular security updates will suffer "some compromise", but adds that with the right security software installed, it should usually be possible to detect malicious software.

"If [however] there's a completely new targeted attack and a weakness of the operating system, you're talking about a bigger problem," he says.

"There has to be a time the user or organisation has to decide that this operating system should not be allowed on their network." Even if the operating system is receiving security updates, if malicious activity is detected, the device will typically be quarantined.

Vibin notes, though, that the approach that companies take may vary according to the sector they operate in. A bank, in particular, is likely to be very strict when it comes to BYOD devices; a retail organisation may strike a slightly difference compromise between security and the adoption of devices.

The threat landscape that mobiles have to navigate is evolving fast, as shown by another report, "Mobile Malware Evolution" from Kaspersky.

The report notes that 7.6 percent of cyber-attacks in the UAE involve mobile threats, compared to almost 28 percent of cyber-attacks in Saudi Arabia, the ninth-highest figure in the world.

Rottigni at Qualys says, though, that accessing an account on a mobile device is not necessarily an action that is vulnerable to cyber threats. Indeed, he describes himself as "a big fan of mobile banking". However, he adds that mobile devices are "a bit more difficult to monitor" than laptops or desktops.

"It's harder for a monitoring solution to install apps or solutions that have complete visibility on the mobile state. It's harder but it's not impossible," he says.

Mobile security should, says Rottigni, include a "holistic" element: organisations should have a vision of what's happening on the mobile. To achieve this, he says that organisations can employ Qualys's Secure Enterprise Mobility cloud-based solution for mobile devices.

"Security should be ergonomic. It



Marco Rottigni, Qualys

"SECURITY SHOULD BE ERGONOMIC. IT SHOULD EMPOWER THE USER IN THEIR WORKING ENVIRONMENT AND NOT BE PERCEIVED AS AN OBSTACLE."

According to the report, there has been rapid growth in the number of mobile advertising trojans, which display intrusive banner advertisements based on the private information that they collect.

As well as facing the potential irritation caused by these advertisements, users may also risk having their data finding its way onto third-party servers.

Kaspersky also highlights the emergence of what it says is the first mobile financial malware, called Accessibility, which allows attackers to gain control of banking apps. Accounts may be stripped bare and ransomware Trojans and other malware may be installed. should empower the user in their working environment and not be perceived as an obstacle," he says.

By using mobile security solutions from companies like Qualys, Rottigni says that users can be protected by as many as four factors, including pin numbers and facial biometrics, when mobile banking.

Furthermore, users need to also keep in mind security measures advised by Kaspersky, such as not downloading apps from unknown sources, keeping devices updated (if possible) and regularly running system scans, they should keep their devices secure – despite the growing list of threats. Barracuda Cloud Security Guardian

Build fast. Stay secure.

Remove security as a burden in the cloud.

Developers like the speed and flexibility of the cloud—but many fail due to cloud security challenges. Cloud Security Guardian manages security for them, automatically.

Leverage industry best practices for security compliance.

Cloud Security Guardian is fully CIS Benchmarks-certified – their benchmarks are incorporated as pre-loaded policies in Cloud Security Guardian. Policies for PCI DSS and HIPAA are also included.

Full-stack cloud security.

Only Barracuda Networks integrates cloud security management with perimeter and network security solutions – i.e., control, data, and management plane security together in a single solution.

For more information visit: barracuda.com/products/cloudsecurityguardian or contact: MET_sales@barracuda.com

80 percent of cloud breaches are self-inflicted.

"Through 2020, 80 percent of cloud breaches will be due to customer misconfiguration, mismanaged credential, or insider theft."

Gartner Research



FUELLING SECURITY

AS THE OIL AND GAS SECTOR AND ITS SUPPLY CHAIN CONTINUE TO BUILD OUT DIGITALLY CONNECTED INFRASTRUCTURES, THEY FACE INCREASED CYBERSECURITY RISKS FROM BOTH EXTERNAL AND INTERNAL ACTORS. INDUSTRY EXPERTS DISCUSS THE CYBERSECURITY CHALLENGES THAT OIL AND GAS PROFESSIONALS SHOULD BE AWARE OF.



everal cyber breaches in the energy industry have hit the headlines, including tales of oil rigs riddled with malware or leaning heavily because they have become corrupted.

While some such stories have been distorted as they have spread online, there is no doubt that cybersecurity has become an increasing issue for the sector.

Indeed, a recent report from Deloitte, Protecting the Connected Barrels, stated that in 2016, energy was the second-mosttargeted industry in term of cyber-attacks.

Everyone from state-sponsored attackers through to ransomware fraudsters is looking to exploit vulnerabilities in the oil and gas industry.

"Most of the attacks we've seen have been to control the networks. It depends on who's running it. A lot of Iranian or North Korean attacks have been destructive – to wipe out hard drives," says Jonathan Couch, senior vice president for strategy at the cybersecurity company ThreatQuotient.

Few people have observed the oil and gas cybersecurity landscape in the Middle East more closely than Marcus Josefsson, the MEA sales director for Nozomi Networks. He says that in this region, in particular, cyber-attacks affecting the energy industry tend to be more targeted – and often state-sponsored – than is typically the case in other parts of the world. The Iranian-backed Shamoon attack on the Saudi Arabian oil and gas company Aramco is one prominent example.

There are many motivations other than cyberwarfare, among them cyberespionage in the form of stealing field data, and financial gain, such as when ransomware is deployed.

Looking at the threats facing the sector's operational technology (OT) and operational process vulnerabilities (as opposed to those targeting corporate networks), "criminal activity and ransomware impacts are on the rise and of growing concern," according to Tim Conway, a technical director at the cybersecurity training organisation the SANS Institute.

"Criminal threat actors are typically taking advantage of opportunistic attacks due to poor access control protections, segmentation within the OT environments, remote access, and general lack of OT detection capability," he says.

Threats are not all external, as they can come from inside companies, says Barak Perelman, the vice president of OT security at Tenable. There are disgruntled employees, third-party contractors and human error to consider.



Tim Conway, SANS Institute

"CRIMINAL THREAT ACTORS ARE TYPICALLY TAKING ADVANTAGE OF OPPORTUNISTIC ATTACKS DUE TO POOR ACCESS CONTROL PROTECTIONS, SEGMENTATION WITHIN THE OT ENVIRONMENTS, REMOTE ACCESS, AND GENERAL LACK OF OT DETECTION CAPABILITY." "Whether the intention is malicious or purely accidental, it can have the same impact. For example, a contractor may plug a malware-infected PC into a remote site," he says.

As well as disrupting operations, leading to financial losses, Deloitte's report points out that attacks can threaten worker safety, particularly because of the cyberphysical dimensions of systems, harm a company's reputation and cause environmental destruction if pollution results.

Given all of this, it is no wonder that, in recent years, cybersecurity has moved much higher up the agenda of the region's energy companies.

"Every single large customer and medium-sized customer has projects in this space, and they wouldn't be spending time and effort unless they were worried," says Josefsson.

As well as having diverse origins, the vulnerabilities are varied too, ranging from upstream to downstream and everywhere in between.

Among upstream operations, development drilling and production tends to face greater cyber risks than another key activity, seismic imaging, but because the latter is now digitising, new vulnerabilities are set to be exposed in future.

"The most destructive attacks are upstream because you have much more risk in the physical dimension," says Jean Abbal, strategic and channel partners manager for the MENA region at Nozomi Networks.

Abbal says that it is much more difficult to stop production upstream than it is downstream, where a suspension to allow things to recover is much easier.

Downstream there is, however, a wider range of potential threats, with "many different systems to optimise the chemical reactions," as Abbal puts it.

"Everything is run by computers," he says of downstream operations.

Pipelines too can be vulnerable to attacks that may, for example, attempt to increase the pressure of the oil passing through – with devastating consequences.

An incident as far back as 2008 in which a Turkish oil pipeline caught fire may, according to reports, have been caused by Russian attackers. They are suspected to have altered the pipeline's pressure after hacking into computers at valve stations.

The barriers to dealing with threats are numerous, including that attack surfaces can be large and spread across a wide area, with remote operational sites. It may also be difficult to pinpoint attacks.

"In OT networks we have large security gaps because many don't know which assets and devices are in the network," says Tenable's Perelman.

"And it's one thing knowing about these devices and keeping an inventory – it's a whole other thing to actually keep track of changes in configuration that alert you to risks and remediation taken."

Perelman also notes that much of a network's critical information is transferred using communications that are proprietary to the industrial vendors, be they Siemens, ABB, Honeywell, Rockwell or others.

"This makes standard IT monitoring tools blind to the most sensitive information in the network that requires analysis," he says.

Another issue is that the priorities of those working with operational



Jean Abbal, Nozomi Networks

"THE MOST DESTRUCTIVE ATTACKS ARE UPSTREAM BECAUSE YOU HAVE MUCH MORE RISK IN THE PHYSICAL DIMENSION."

technology, which is typically focused primarily on safety, are often not the same as those who work in information technology, where cybersecurity is the key aim.

The oil and gas sector may be particularly vulnerable because, as ThreatQuotient's Couch points out, there is widespread use of legacy technology. Indeed, he has dealt with companies still using Windows 95. Patching is often inadequate.

"A lot of it is driven by the consumer software as well as other regular commercial technology. It's not up to date," he says.

Perelman says that, when most industrial devices were designed and manufactured in the late 1980s and 1990s, "security wasn't a top concern and cybersecurity wasn't even a term".

"Obviously those devices have many more vulnerabilities, and those are the same devices used in most industrial networks globally," he says.

Many approaches are being taken to protect oil and gas companies from cybersecurity attacks. Perelman says that Tenable helps energy firms identify any threat that can disrupt their OT network by providing "a unified, risk-based view of IT and OT security".

"This allows security teams to view and manage OT security issues alongside IT vulnerabilities, from assessment through closed-loop remediation verification," he says.

He says that covering every target in both the IT and OT networks is important, including not just Windows PCs and servers, but also ICS devices, including industrial controllers.

"We recommend organisations ensure that they have the most productive and comprehensive alerts. This means monitoring both the network itself for traffic by connecting to a SPAN port, while also collecting information from the devices themselves for a complete picture," he says.

The importance of developing the expertise of staff in ICS cybersecurity is emphasised by the SANS Institute, which provides education resources, training and validation for professionals responsible for defending OT environments in sectors including oil and gas. The organisation uses instructors who have real-world experience in the industry.

So, although the motivations of the attackers are numerous, and the vulnerabilities are many, there is plenty that energy companies can do and are doing to protect themselves. **1**



Barak Perelman, Tenable

"IN OT NETWORKS WE HAVE LARGE SECURITY GAPS BECAUSE MANY DON'T KNOW WHICH ASSETS AND DEVICES ARE IN THE NETWORK."

WE'RE NOT JUST FIREWALLS.

SonicWall automated, real-time breach detection and prevention layers proven cybersecurity across your entire organization.

You know SonicWall because of our rich history designing high-performance firewalls. But like your organization, SonicWall has evolved.

Today, the modern SonicWall Capture Cloud Platform delivers automated, real-time breach detection and prevention to safeguard your business or organization.

With this layered approach, you can stop the most malicious cyberattacks, including ransomware and encrypted threats, from compromising your network and damaging your brand.



ACCELERATING SECURITY

GOVIND HARIDAS, BUSINESS HEAD – CYBER SECURITY, HIPERDIST, SHARES INSIGHTS INTO THE LATEST CHALLENGES IMPACTING ENTERPRISES AND WHAT THE FUTURE HOLDS FOR THE SECURITY INDUSTRY.

> hat do you think will be the next 'game-changing' technology in the cybersecurity space? Artificial intelligence

(AI) and machine learning are increasingly playing big roles in transforming multiple areas of IT and cybersecurity is no different. Therefore, we can expect to see more and more AI-driven cybersecurity solutions

What are the biggest cybersecurity challenges regional enterprises need to watch out for in 2020?

Phishing attacks, financial crimes, ransomware and lack of skilled resources are some of the primary challenges that enterprises need

"AI-BASED MACHINE LEARNING, BLOCKCHAIN AND IOT/OT SECURITY ARE THE DISRUPTIVE TECHNOLOGIES THAT ORGANISATIONS SHOULD INVEST IN TO BOOST THEIR CYBERSECURITY STRATEGIES." to be wary of. Another issue that IT security leaders will also face is getting budgetary approvals for cybersecurity initiatives and investments due to the current economic conditions. Additionally, the recent coronavirus (COVID-19) pandemic has pushed many organisations to implement remote working schemes, which have increased their vulnerability to cyber-attacks.

Which disruptive technologies should organisations invest in to boost their cybersecurity strategies?

AI-based machine learning, blockchain and IOT/OT security are the disruptive technologies that organisations should invest in to boost their cybersecurity strategies.

How will your offerings be instrumental in enabling organisations become cyber resilient?

Our cybersecurity offerings focus on early detection, which is the key to becoming cyber resilient. Instead of

out some fantastic results in a short timeframe. We are also in the final stages of signing up one of the leading AI vendors in the world whose offerings will be a game changer in the market.

How do you see global regulations around IT security evolving in the next few years?

Hackers are becoming more sophisticated and organisations are increasingly adopting new and more complex technologies, which contribute to the expansion of the attack surface. I believe this will prompt increased global regulations around IT security, which are focused on data protection and cloud security. 1

focusing on protection solutions, our cyber portfolio has advanced tools which proactively detects threats before

What advice would you give organisations to ensure they succeed in their security transformation initiatives?

We advise our customers to follow the best practices of cybersecurity. We focus on the critical controls that would give enhanced protections to our customer which ensures business continuity. Followed by providing them with next-gen disruptive technology controls to protect against sophisticated attacks.

How are you leveraging technologies around artificial intelligence and machine learning to enhance your offerings?

Our digital marketing team already leverages an AI-based tool for lead generation and has churned

Govind Haridas, Hiperdist

they disrupt the business operations.

ADVANCE GUARD

AS PRIVATE CYBERSECURITY ORGANISATIONS' ROLES IN POLICING THE CYBER SPACE GROW, IS THERE A NEED FOR INCREASED REGULATORY CONTROL FOR THIS SECTOR? **DANIEL BARDSLEY** INVESTIGATES.





ago, researchers talked of a "quiet revolution" brought about by the growth of the private security industry. Where once only the police

held sway, in the brave new world of the 1970s and 1980s, a parallel private security sector developed.

Nightclubs, industrial facilities and other premises were being guarded by private operators who would sometimes use physical force against those who they felt had breached the rules.

While the quiet revolution term originated in North America, a similar phenomenon was seen in many other regions.

In response, governments and local authorities began regulating the private security sector, keen to ensure that it operated within reasonable parameters.

Now, a researcher has described the development of the private cybersecurity industry as being a "second quiet revolution" and has asked if regulations are needed to govern it too.

In a paper published this year in the Journal of Contemporary Criminal Justice, Professor Mark Button, of the University of Portsmouth in the United Kingdom, notes that this sector is fast eclipsing the physical private security industry in revenue and scale.

Button, whose paper is entitled. The "New" Private Security Industry, the Private Policing of Cyberspace and the



Jonathan Couch, ThreatQuotient

"I WOULDN'T SUPPORT REGULATION THAT **MAY SLOW DOWN OUR ABILITY OR IMPEDE OUR ABILITY TO BE MORE AGILE."**

Regulatory Questions, suggests that there has been little debate among researchers about the implications of the sector's growth or of the policies needed to govern the new landscape.

"Most of the issues, the questions that arise with physical security, also arise in the cyber world. There are some areas where I would be very surprised if there isn't need for some kind of regulation," savs Button.

"The issue off competence in the physical world, that's been a major problem – of cowboy operators. Is that the same in the cybersecurity world? Are companies offering services they're not capable of [delivering]?

"By making private cybersecurity providers stronger by some kind of control, would that be an opportunity to further enhance organisations purchasing their services because their performance would be so much higher?"

The paucity of official action against cybercrime is shown by the fact that there are just a few dozen prosecutions annually in, for example, the United Kingdom for crimes linked to hacking, viruses, ransomware and distributed denial of service (DDoS) attacks.

"The police do have good people, but the numbers that you would need to supply that to the large number of organisations and individuals who have been attacked is not enough," says Button.

Although governments have set up organisations to focus specifically on cybersecurity, it is largely private companies that try to keep a lid on cybercrime through actions that are as much preventative as reactive. Potential worries over these companies' actions are largely focused on privacy and the use of sensitive data.

"Imagine if you're doing work for a large organisation with large access to personal information of individuals. It's incredibly important that that information is protected," says Button.

The private cybersecurity sector may also wield, Button notes, cyber tools that can be used for harmful activities such as cyber-espionage. The sector carries out functions that private citizens would not undertake, something that Button suggests may indicate a need for regulation.

Another issue highlighted by Button concerns companies that offer datarelated services. Their use can result in customers being branded – often unfairly – as fraudsters when transactions are analysed. While some nations have tough data-processing rules, Button says that these do not cover many activities of the new security sector.

Although parallels can be drawn between the private physical security industry and the private cybersecurity sector, Button points out clear differences.

Barriers to entry in terms of skills are typically higher in cybersecurity, which may keep out some of the unsavoury element sometimes associated with physical security.

Also, although ethical hackers might sometimes be recruited into penetration testing roles, Button notes that there have been few scandals sparked by criminal involvement in private cybersecurity.

Nonetheless, he raises the question of whether penetration testers, security architects, chief information security officers (CISOs) and internet moderators (who may have access to illegal material and other information that should not be in the public domain) should be licensed.

Professor Eerke Boiten, director of the Cyber Technology Institute at De Montfort University, Leicester in the United Kingdom, says that it is unclear to him whether licensing is needed. He suggests that companies are able to assess the worth of cybersecurity services that they are buying.

"When you hire a company, you interview them and check their qualifications, and there are plenty of qualifications in the cybersecurity sector. I'm not convinced that we have a surplus of bad people in the sector," he says.

While the likes of CISOs could use their position to cause a great deal of damage, Boiten says that the same could be said of people in many other senior corporate roles.

According to Jonathan Couch, ThreatQuotient's senior vice president, strategy, regulations and licensing requirements could lead to box-ticking. He suggests that this has happened with the emphasis on governance, risk and compliance (GRC) in organisations.

"It would be like GRC – it gets so regulated, you have compliance and not security. [If] you have a CISO who has a tonne of credentials ... it doesn't mean they're any better at their job," he says.

Also, Couch suggests that more regulation could hamper the activity of a

"The certifications that have been developed even by industry don't necessarily mean that you're any better or you know any more than anyone else," he says.

Regulations over the use of data, such as the EU's General Data Protection Regulation (GDPR), mean that additional requirements such as licensing may be unnecessary, according to Professor Siraj Shaikh, a professor of systems security at Coventry University in the United Kingdom. Specific sectors, such as finance, have their own regulations.

"I don't think an introduction of another level of regulation would happen," he says.

He does, however, suggest that licensing could be used to promote training or continuous professional development (CPD, also sometimes written as continuing professional development), which is a requirement in



Professor Siraj Shaikh, Coventry University

"IN CYBERSECURITY, ONE OF THE ELEMENTS IS TO KEEP ABREAST OF THREATS. IT'S A VERY DYNAMIC AREA AND IT WILL REMAIN THIS WAY."

cybersecurity sector that is battling fastmoving attackers.

Militaries have to go through what American strategists have called the OODA loop – observe, orient, decide and act – faster than their adversaries. Similarly, effective cybersecurity requires organisations to complete these actions at a brisk pace.

"I wouldn't support regulation that may slow down our ability or impede our ability to be more agile," he says.

Couch is also sceptical about the value of the numerous certifications available in the cybersecurity sector, saying that he has tended to let his own lapse. some other professions, such as medicine, where practitioners are licensed.

"In cybersecurity, one of the elements is to keep abreast of threats. It's a very dynamic area and it will remain this way," says Shaikh.

While some experts are doubtful about the need for licensing, Button says that he is not so much calling for more regulation but is primarily focused on sparking debate about what rules could or should be introduced. In his paper, he says there is "a regulatory gap" when it comes to the new private security sector and in his view, more research is needed to fill this void. **1**



SMART ACCESS FOR SECURE CONTROL



SECNOR ACCESS CONTROL SYSTEM

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.





Norden Communication UK Ltd

Unit 13, Baker Close, Oakwood Business Park, Clacton-on-Sea, Essex, CO15 4BD, United Kingdom Tel: +44 [0] 1255 474063, E-mail: support@norden.co.uk, Web: www.norden.co.uk www.nordencommunication.com

HOW TO ENSURE SECURITY WHILE WORKING REMOTELY

MARCUS WHITTINGTON, CO-FOUNDER AND COO, SENTRYBAY AND **ABHIJIT MAHADIK**, DIRECTOR – CYBERSECURITY SOLUTIONS, RAQMIYAT, DISCUSS THE RISKS OF ENABLING REMOTE ACCESS FROM UNMANAGED DEVICES AND HOW SENTRYBAY'S SOLUTIONS CAN HELP ENTERPRISES STAY SECURE.

> ith the outbreak of COVID-19, there are widespread extended requirements for staff to work from home. The phrase "work-from-home" brings-in fears on data security and data-pilferage risks from unmanaged end-user owned remote desktops, PCs and laptops that would be used as endpoints by staff and external vendors, partners and contractors.

> Remote access from unmanaged devices introduces elevated risks. Often these devices have a lower security posture, possibly out-of-date anti-virus

or internet security software; they offer a higher risk of compromise because they might be running counterfeit or unlicensed solutions, or they are on untrusted networks. The enterprises have little or no control over what software is running or has previously been executed on the devices.

These unmanaged devices pose a higher risk of sensitive data being stolen (including corporate credentials) from attacks involving keylogging, which along with spyware is ranked the highest global malware, according to the NTT Security Threat Intelligence report. Other attacks to be wary of include screen-capture, screengrabbing, man-in-the-browser, saved account detail harvesting, screenmirroring, man-in-the-middle, DLL injection and RDP double-hop. During the coronavirus crisis, the risk is exponentially much higher.

VPN is the commonly utilised form of connectivity to ensure that remote devices can connect to corporate

Abhijit Mahadik, Raqmiyat

"BY PARTNERING WITH SENTRYBAY, WE ARE OFFERING THIS SECURED SOLUTION TO HELP OUR CUSTOMERS WITHOUT SACRIFICING THEIR SECURITY POSTURE."



Marcus Whittington,

Abhijit Mahadik, Ragmiyat

Sentrybay

networks. However, VPN does not protect the user from malware that records the keystrokes entered or takes pictures or videos of the user's endpoint in order to steal data. They scrape up passwords, credit card and banking information, personal details, and more, to use in identity theft and other malicious deeds. Every piece of data entered into applications such as Word, Excel, Outlook, other Office apps, corporate apps, browser, webmail and SaaS applications by the home-based employee, contractor or supplier such as, can be lifted from the endpoint itself by malware. This can then be sent out to the command and control server of the cybercriminal. In summary, all this data can be stolen by cybercriminals even before it enters the VPN tunnel.

Ideally, with virtually no time for preparation, customers should look for products that can be deployed quickly (i.e. within 24 hours) and which do not involve specially configured software or hardware - a simple download and

install from pre-configured software is the preferred option. This means selecting proven anti-keylogging software that can protect every keystroke into any application and prevent screen-scraping malware from stealing credentials and sensitive corporate data.

Ragmiyat, an authorised reseller of Sentrybay, provides secured workfrom-home solutions. "During this challenging time, organisations struggle to provide a secured workfrom-home solution. By partnering with Sentrybay, we are offering this secured solution to help our customers without sacrificing their security posture," says Abhijit Mahadik, director - Cybersecurity Solutions, Ragmiyat.

Unlike other cybersecurity vendors who only worry about cleaning and protecting endpoints, SentryBay cares about data security and uses patented technology of anti-keyloggers and antiscreen captures to achieve this.

Armoured Browser from SentryBay provides a browser on Mac & Windows,

which offers a very unique secured browser that provides anti-key logging, anti-screen capture and anti-screen scrap features, thus, enabling a secured browsing environment for sensitive work to be done irrespective these malwares on the PCs.

The best part of this offering is that it creates separate user and desktop sessions and leaves no-trace upon closing. With the latest enhancements, it can be installed as a pseudo-remote access solution to lock down use of, say, Office365, SaaS apps, web browsing and more. It can also be deployed for Citrix, Vmware or any other remote access solution deployed.

"We have experienced a huge surge in demand worldwide, especially in the UAE for this niche solution from Sentrybay. Some of our largest banking clients have added licenses in the past week, specifically to enable more employees to work from home," says Marcus Whittington, co-founder and COO, Sentrybay. 1

CYBERSECURITY TRENDS FOR 2020

AMIR KANAAN, MANAGING DIRECTOR, MIDDLE EAST, TURKEY & AFRICA, KASPERSKY, SHARES INSIGHTS INTO THE LATEST TRENDS THAT WILL IMPACT THE EVER-EVOLVING CYBERSECURITY SPACE.



Amir Kanaan, Kaspersky

he year 2019 was another busy one for the cybersecurity industry. Worldwide spending on security solutions is expected to achieve a growth rate of 9.2 percent over the 2018-2022 forecast period and total \$133.8 billion in 2022. The average cost of an attack, meanwhile, ranged from \$108,000 for an SME to \$1.4 million for a large enterprise.

We can be certain that the year 2020 will be another hectic one for cybersecurity professionals. As ever, cybercriminals will modify their strategies, particularly as more and more organisations migrate to the public cloud and 5G networks finally begin to come online.

As we do every year, Kaspersky has delved into its collective knowledge base to identify key cybersecurity trends for the vear ahead.

Confusion in the cloud

ICT departments are transitioning rapidly from on-premise models to assets deployed in the public cloud. As this migration takes place, there is a possibility that gaps may appear in corporate cybersecurity strategies. Organisations embracing the public cloud as they transform their ICT infrastructure should understand that they will retain at least partial responsibility for security of their data even after it has been migrated. It is up to both providers and users to keep cloudlocated data safe and responsibilities must be clearly defined in contracts between providers and customers. While agreements should be read closely, customers should assume that they are responsible for protecting the operating systems, applications and data that they themselves deploy in the cloud.

Continued attacks via IoT devices

There will be 75 billion connected, Internet of Things (IoT) devices around the world by 2025, according to Statista. While consumers love their smart TVs and connected baby monitors. IoT devices are typically perceived as being vulnerable to hacks, particularly on the default settings that home users usually forget to change when setting up devices. A hacked IoT device can represent a major vulnerability. As well as being used to spy on individuals, it could also become part of a botnet and used to carry out DDoS attacks, like the notorious Mirai botnet that brought down several online services in 2016. Hackers will keep on targeting IoT devices, so users must make sure to follow basic rules on how to keep them secure.

Phishing via messaging

Far from being immune to attacks, smartphones have become one of the

leading platforms for cybersecurity breaches. According to the RSA, more than 60 percent of online fraud originates from mobile devices and 80 percent of mobile fraud comes from mobile apps, rather than mobile browsers.

As consumers now do so much of their business on their phones, a phone is a potential goldmine of both personal and corporate information. Hackers will continue to focus considerable effort on phishing, spear phishing and malware attacks targeted at smartphones. Users will need to be much more aware of the threat and how to deal with it.

Artificial intelligence: a doubleedged sword

Artificial intelligence is a double-edged sword for the cybersecurity industry. On the one hand, organisations are using it to identify and prevent attacks. On the other hand, cybercriminals can use AI to make their attacks more 'intelligent' and thus able to avoid detection.

Artificial intelligence could also help hackers make their social engineering strategies more effective. This popular hacking technique effectively involves tricking individuals to divulge information that can compromise personal or corporate security. Al could be used to trawl for sensitive information on individuals and organisations, as well as being used to create content that can pass through typical cybersecurity filters, such as e-mail messages that look like they were written by humans.

5G networks will come under attack

The year 2020 will see 5G networks

start to finally come online. The boost it will provide to connectivity speeds will be significant and there will be even more data moving across networks than ever before. This will give a boost to the Internet of Things and it will allow companies to capture more data than ever before, supporting Big Data and AI strategies. There will, however, be significant risk as hackers target networks in an effort to retrieve data related to health, safety & the environment (HSE), personal health and corporate performance. A recent European Union report identifies potential key threats to 5G networks, particularly their increasing reliance on software. Any flaws in the applications used to manage networks could enable malicious actors to insert backdoors and begin to siphon off data.

Multi-factor authentication becomes prevalent

The password remains the most common method of protecting sensitive data, but it is now just a first of line of defence. While two and three-factor authentication is not a new concept, uptake has been slow, with just 20 percent of Office 365 subscribers using it as of the middle of 2018. Expect to see a much more rapid uptake of one-time passwords and biometrics over the next year as companies embrace the principle of multi-factor authentication (MFA). While MFA is often seen as cumbersome by users, it has benefits beyond offering more secure access to a particular application. It also counters the phenomena known as 'credential stuffing', where users tend to use the same password across several accounts. Gaining access to that one password by infiltrating a poorly secured service can open up access to all or many of a person's other accounts. MFA helps avoid this. 🚺

"HACKERS WILL KEEP ON TARGETING IOT DEVICES, SO USERS MUST MAKE SURE TO FOLLOW BASIC RULES ON HOW TO KEEP THEM SECURE."

WHAT THE CORONAVIRUS OUTBREAK CAN TEACH US ABOUT CYBERSECURITY

BRIAN PINNOCK, CYBER RESILIENCE EXPERT, MIMECAST, DISCUSSES THE UNCANNY SIMILARITIES BETWEEN THE HUMAN RESPONSES TO THE CORONAVIRUS OUTBREAK AND CYBERSECURITY INCIDENTS.

n 2015 the World Health Organisation raised the risk of "Disease-X". At the time it was unknown and they projected it had the potential to trigger a global pandemic, with no known treatments or vaccines, leading to loss of lives and massive economic disruption. In a slightly similar vein, Lloyd's of London annually model a cyber-attack pandemic, started by threat actors who hold the only known cure. The predicted consequences for economies and human lives of both predictions are devastating.

Today, both of these forecasts have real-world comparisons. In 2017 the NotPetya virus became a global cyberpandemic that spread from the Ukraine around the world in a few short hours. NotPetya paralysed organisations, crippled shipping ports and shut down government agencies globally. It caused over \$10 billion in damages. In the world of healthcare, the Coronavirus (now named Covid-19) has infected more than 170,000 people in 157 countries and could cause in excess of \$1 trillion of economic damage. That's more than 3 times that of SARS - a similar virus that broke out 17 years ago.



Brian Pinnock, Mimecast

One reason for the seismic disruptions caused by both medical and cyber pathogens is the interconnectedness of the global economy. Supply chains now span multiple continents. Air travel passenger volumes have doubled. Disruption in China is leading to disruption everywhere. The same dynamic is true for cyber-pandemics because digital supply chains span continents and cloud computing has become ubiquitous, leading to a digital interconnected web which is fragile and can be easily broken. The coronavirus has brought into stark relief some elements of basic human nature that come into play in both a health crisis and a cybersecurity incident. There is initial complacency along with a tolerance for risky behaviour. Only once visible danger strikes is there a frantic, even draconian response, usually focused on saving the image of the infected organisation rather than protecting their stakeholders and the wider community.

A deeper look shows that the similarities between the human responses to the coronavirus outbreak and cybersecurity incidents are not just superficial but remain uncannily close in many respects.

Risky behaviour exposes everyone to danger

Reports suggest that the coronavirus originated from animals such as bats, pangolins or civets. Cross species transfer possibly occurred in a market in Wuhan. Researchers found that the tolerated risky behaviour of consuming exotic animal parts triggered a single introduction into humans, which was followed by human-to-human spread. Similarly, employees engaging in risky behaviour that is tolerated outside of work, such as visiting adult or dark web sites or downloading files from nonwork-related portals, can let malware into the organisation that spreads from one user to another.

Transparency is critical in containing outbreaks

Too often, keeping silent exacerbates the situation and puts business communities at risk. China has received some backlash from global observers, with reports emerging that the Chinese government at first played down the risk of outbreak and later the extent of the problem. Transparency is a major contributor to effectively managing the potential fallout from a viral disease. Even today, we are unsure of the extent of the coronavirus outbreak.

Similarly, by the time senior management are made aware of a serious cyber incident, the infection has usually been incubating and spreading in an organisation for weeks or sometimes months. The organisation can become the source of further infection via their own email systems. Coverups mostly don't work and hide the extent of the problem to the wider community which leads to misinformed complacency about the risks we face.

Many organisations don't share threat intelligence effectively or at all. This is a gift to cyber criminals who employ the same attack method repeatedly against multiple organisations because it keeps working. Instead of making

"CYBERSECURITY AND HUMAN INFECTIONS SHARE ONE LAST SIMILARITY: WE CAN NEVER PREVENT ALL INFECTIONS AND WE CAN NEVER ANTICIPATE EVERY EVENTUALITY."



cybercriminals' tasks harder we enable them by staying silent and ineffectually sharing the symptoms and preventative measures of the cyber disease.

The importance of basic (security) hygiene

Demand for face masks is surging in countries close to the epicentre of the coronavirus. But face masks aren't as effective as most people think. Unfortunately, people are drawn to visible controls rather than invisible ones. But medical authorities suggest that basic practices, like regular handwashing, are more effective at preventing the spread of the virus.

The equivalent of handwashing in cybersecurity is focusing on basic controls first. Have effective and regular patch management practices, implement controls to detect and prevent the spread of malware, adopt regular employee awareness training to equip people with the appropriate knowledge to avoid risky behaviour. It is mostly invisible and not very sexy, but it is a critical layer in the defence against cybercrime.

Herd immunity and misinformed complacency

Organisations who can't or won't patch

and protect their systems or train their people are the equivalent of the those who won't or can't vaccinate their families. An expectation of herd immunity is often misplaced both when it comes to human health and for cybersecurity.

In the UK an auditor general report on NHS disruptions caused by the WannaCry virus, showed they all had unpatched or unsupported operating systems. In addition, other security controls in the NHS would have prevented the rapid spread and subsequent deaths and fiscal costs. But they were incorrectly configured which allowed the virus to spread.

Cybersecurity and human infections share one last similarity: we can never prevent all infections and we can never anticipate every eventuality. Diseases will continue to jump the species barrier and zero-day malware will continue to appear. What we can do however is become more transparent, be more community focused and make ourselves more resilient. If not, we remain exposed to a "Disease-X" – either in the medical or cyber domains – with no known treatments or vaccines and at the risk of devastating economic and human losses. **1**

CONNECTED CARS, CLOU AND CYBERSECURITY

AMAZON WEB SERVICES (AWS) SHARES INSIGHTS INTO WHY CLOUD IS VITAL IN ENABLING THE SECURE AND SEAMLESS DEPLOYMENT OF AUTONOMOUS CARS.

utonomous or self-driving cars will make driving safer, smarter and more efficient. Equipped with internet connections. often wireless local area networks, enables self-driving cars to speak to each other and the environment around them. One feature allows the cars to keep their distance and synchronise braking to avoid accidents. Autonomous cars will include features such as lane assist. collision avoidance and automatic calls to emergency services to create a safer driving experience. Some automotive brands are taking automation a step further, innovating to enable vehicles to communicate with nearby infrastructure and even pedestrians, adding a new dimension to how automation can benefit society.

AWS believes that the right technology infrastructure is critical for the production of these vehicles, which require highperformance computing capacity, seamless cybersecurity, and the ability to manage vast data sets. Here are some of the key reasons why many organisations are turning to the cloud to develop and deploy autonomous cars at scale:

Training and testing

Autonomous cars strive to create vehicles that operate more safely than humans. Delivering on this ambition requires extensive modelling and testing. The ability to collect, store, and manage data is critical, as are advanced machine learning techniques.

Toyota Research Institute (TRI) believes that accurately training autonomous cars requires trillions of miles of testing. To deliver on this, it has a fleet of test cars equipped with Light Direction and Ranging (Lidar) Sensors to record data, collecting terabytes of data every day, needing quick retrieval and analyses. TRI uses AWS to manage this data and access the processing power required to train machine learning models quickly. Using cloud infrastructure, it has gained the ability to spin up compute and storage resources on demand and blend these with management and orchestration services. TRI now retrains vehicle models. increases accuracy, and introduces new features faster. By following similar models. more automotive businesses will accelerate the development of safer cars.

Edging forward

Enabling autonomous cars to make rapid, data-driven decisions will make our roads safer. These machines need backing by reliable infrastructure with low latency and high availability. They also need to analyse information in real time, including data on road conditions, weather, and the behaviour of other vehicles. Applying AI allows the car to react swiftly and safely to road conditions.

Edge computing allows this core in-car technology to perform its in-car data crunching. When a second of lag can make the difference between a safe or dangerous response, autonomous vehicles do not have the luxury of waiting for data processing in the cloud. Therefore, organisations need to look for cloud providers with integrated edge solutions. These allow analysis of mission-critical data at the source and reducing the cost of transmitting additional data to the cloud.

Security in the cloud

Cybersecurity is important when developing safety-focused autonomous cars. Each vehicle becomes a new endpoint which must be secured. Protection from hackers and malware must be a top priority to ensure they cannot gain access to driving controls or the data that runs through each vehicle.

Autonomous car producers are turning to the cloud in order to support and run connected cars. AWS delivers automated security services which apply machine learning to proactively manage tasks including security assessments, threat detection, and policy management. By having security baked in, manufacturers can be confident that they have the solutions in place to detect new and emerging vulnerabilities and threats which will reduce harm to drivers and lower the risk of a breach.

Autonomous cars are our future; however, to drive adoption, manufacturers must ensure they are secure and supported by robust infrastructure. With the right cloud infrastructure, organisations to focus their resources on building differentiated automotive experiences, rather than managing IT infrastructure.





Future-Proof Connectivity Solutions



COPPER



FIBER





FTTH

RACKS

Optimize your ICT infrastructure with D-Link innovative, yet reliable Structured Cabling Solutions

www.dlinkmea.com





POWEREDGE

POWEREDGE TOWERS, RACKS, MODULAR INFRASTRUCTURE



INDUSTRY'S **#1** Server Portfolio*



* IDC QUARTERLY SERVER TRACKER, Q2 2019

Ingram Micro Innovation Hub | Dubai Internet City - UAE | P.O.BOX: 33550 Tel: +9714 2428486 | Fax: +9714 3697110 Website: www.nit.ae | http://meta.ingrammicro.com

