SUPPLEMENT OF ENTERPRISE CHANNELS MEA

BUSINESS TRANSFORMATION

SEPTEMBER 2018

THE CHANGE TO FUTURISTIC BUSINESS

biznesstransform.com

CYBORGS
CAN WE REBUILD THE HUMAN BEING

Developments in bioengineering have opened the doors to overcome human limitations.

NEIL HARBISSON
Cyborg and designer of artificial senses

TRANSFORMING THE WORKPLACE

Andy Brocklehurst, Cisco

Osama AlHaj-Issa, HPE Aruba

Mahmoud AlYahya, Xerox

Henrique Vale, Nokia

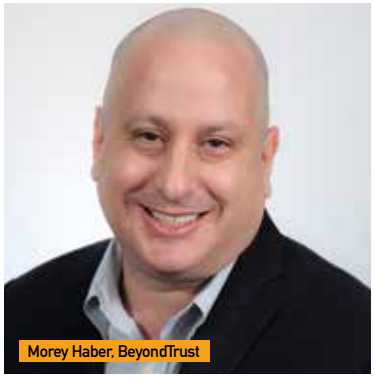
HOW TELECOS NEED TO MANAGE BIG DATA REPOSITORIES

David Warburton, F5 Networks

WHY THE BITCOIN BLOCKCHAIN IS TOO LARGE TO BE HACKED

Srinivasan CR, Tata Communications

WHY BANKS NEED TO START CONSIDERING OUTSOURCED SOCs



Morey Haber, BeyondTrust

IF YOUR APPLICATION IS HACKED SO CAN YOUR BLOCKCHAIN

CloudQuarks
By Redington

Cloud Fundamentals. Delivered.

CONTENTS

SEPTEMBER 2018

ZEBRA CAPTURE YOUR EDGE

Transportation & Logistics Solutions

Empowering your performance edge.

BUSINESS TRANSFORMATION
THE CHANGE TO FUTURISTIC BUSINESS

MANAGING DIRECTOR
Tushar Sahoo
tushar@gecmediagroup.com

EDITOR
Arun Shankar
arun@gecmediagroup.com

CEO
Ronak Samantaray
ronak@gecmediagroup.com

GROUP SALES HEAD
Richa S
richa@gecmediagroup.com

EVENTS EXECUTIVE
Shriya Nair
shriya@gecmdiagroup.com

SALES EXECUTIVE
Krishna Thanki
krishna@gecmediagroup.com

ONLINE SALES
Mohamed Mubin
mubin@gecmediagroup.com

BUSINESS DEVELOPMENT EXECUTIVE
Susan Paul
Susan@gecmediagroup.com

SALES AND ADVERTISING
Ronak Samantaray
Ph: + 971 555 120 490

PRODUCTION, CIRCULATION, SUBSCRIPTIONS
info@gecmediagroup.com

GEC MEDIA

UAE
223 DMC 9 Dubai Media City, Dubai
PO Box 500653, Ph: +971 4 368 8523

USA
31 Foxtail Lan, Monmouth Junction
NJ 08852, Ph: + 1 732 794 5918

Printed by
Al Ghurair Printing & Publishing LLC.
Masafi Compound, Satwa, PO Box: 5613,
Dubai, UAE

Published by
Accent Infomedia MEA FZ-LLC
223 DMC 9 Dubai Media City, Dubai
PO Box 500653, Ph: +971 4 368 8523

A publication licensed by
International Media Production Zone, Dubai, UAE

Dear Readers,

The challenge the industry faces today is to make robots more human-like or into humanoids. When this happens and which technology innovation cycles will make the global society reach an inflexion point, remains to be seen. The reverse challenge that is also happening is to rebuild human beings using bio-engineering and implants.

No more do such measures need to be seen as mere surgical procedures. There is now a growing interest in overcoming limitations of the human being and the human form by technology devices and engineering forms to increase the capabilities and enhance functioning to near normal levels. Sophistication in product design is not far behind.

In a CNN contributed article we look at three such human examples including Neil Harbisson, Amal Graafstra, and Viktoria Modesta. Says Neil Harbisson, "I define what I do as neuro-hacking rather than biohacking or body hacking because my ultimate aim is to change the mind. This project is artistic in intent. Because art has no rules, laws or boundaries, I feel like there is a lot of freedom when you contextualise a project in art."

Large scale connectivity and mobility is a key driver for change in the workplace. Aruba's global survey of 7,000 businesses indicates that digital technologies enabling work from home and work outside office are becoming a de-facto standard of expectation from the current and next generation of workers. The more digitally enabled is the workplace, the higher is the sense of wellbeing experienced by its workers, so indicates the survey.

According to the report, "Today's workforce is not just driving consumerisation of IT, but also accelerating consumerisation of the workplace. These changing employee behaviors and expectations are shaping the way organisations think about the role of technology in the workplace."

Continuing further, in the Opinion section, our guest contributors include Henrique Vale at Nokia, Kushal Nahata at FarEye, and Srinivasan CR at Tata Communications. And in our Industry Comments section, the guest contributors include Morey Haber at BeyondTrust, David Warburton at F5 Networks, and Santiago Madruga at Red Hat.

Flip these pages to read their exciting insights on business transformation as it unfolds here, now and today.

Arun Shankar
arun@gecmediagroup.com

WHY BANKS NEED TO START CONSIDERING OUTSOURCED SOCs

Possible losses from cyberattacks are rising and security operation centres are an added layer of protection, explains Srinivasan CR at Tata Communications.

SRINIVASAN CR
Chief Digital Transformation Officer, Tata Communications.

KEY TAKEAWAYS

- One of the main learnings of the 2008 crisis was that the industry needed to be more responsible in its approach to risk.
- Although DDoS attacks remain prevalent across industries, their effectiveness relies on the organisation paying up the ransom.
- Many organisations are looking to outsource their security services in order to ensure they have around the clock coverage.
- Investment in security operation centres is on the rise.

In early 2017, UK-based banks operating under Lloyds, Halifax and Bank of Scotland were hit by a significant Distributed Denial of Service attack over the course of 48 hours. More recently, a host of South Korean Banks were threatened by a damaging DDoS attack if they did not pay the $315,000 bitcoin ransom demand. Thankfully, banks are acutely aware of the criticality of the data they handle, and in both cases the attacks were successfully defended against.

Although DDoS attacks remain prevalent across a number of industries, the effectiveness of the method relies on the organisation paying up the ransom, which many organisations are refusing. Another more worrying form of attack for banks is one that quietly siphons off data across a period of time. These are often introduced in the form of malware driven attacks, such as banking Trojans.

An example of these kinds of threats is an evolving malware project called TrickBot which, while currently plaguing Latin America, has targeted banks in over 40 countries across the globe.

Attacks that lead to a systematic leakage of data over time do not have the immediate shock effect of a swift attack, but they can be just as damaging, and serve to weaken the banks' defences over time. An additional layer of complexity to this issue is that there will soon be more and more channels in which hackers can access the systems.

Securing all the various channels will only get more difficult for the industry as the way we bank continues to evolve and leaders must be armed with an agile cybersecurity plan to move into the next generation of finance with the confidence of their customers behind them.

Traditionally, the banking industry has been one of the main investors in security, and it is likely this will continue to be the case as we navigate the new threats landscape that the future of banking presents.

As open banking accelerates and the industry's data becomes more and more interconnected, the industry cannot afford to take risks with the data they hold on their customers. One leak could be the first symptom that infects the whole industry with a sickness that could have wider-reaching effects.

In order to combat this evolving threat, the industry needs an adaptive, 24x7 method of detection, defence and counter-attack. Many organisations are looking to outsource their security services in order to ensure they have comprehensive, around the clock coverage. Investment in security operation centres for example is on the rise.

One of the main learnings of the 2008 crisis was that the industry needed to be more responsible in its approach to risk. By keeping abreast of the latest security threats, and investing in security applications that are able to adapt to the future of banking, the industry will be able to avoid a similar crippling financial event. ■

TOSHIBA

14TB

The New Heavyweight Champion in the Capacity Arena.

Toshiba continues the long history of advanced Japanese technology, delivering the world's first 3.5-inch 14TB HDD using conventional recording, incorporating an industry leading 9 platter mechanical design. The Toshiba 14TB HDD delivers major advances in Enterprise storage capacity, reducing data center footprints and total cost of ownership.

The World's First 9 Disk HDD*

DESIGNED IN JAPAN

*Source: Toshiba Electronic Devices & Storage Corporation, as of December,2017 for the 3.5-inch, 26.1mm high Definition of capacity: A terabyte (TB) is 1,000,000,000,000 bytes.

HDD image is tentative and subject to change

ToshibaMEA Toshiba Gulf FZE 121@toshiba-tgfz.ae Toshiba.tgfz TOLL FREE 800-TOSH https://toshiba.semicon-storage.com

HOW TELECOS NEED TO MANAGE THEIR BIG DATA REPOSITORIES

Telecom service providers are the biggest aggregators of consumer data that is only growing and needs to be managed, explains Henrique Vale at Nokia.

HENRIQUE VALE
Head of Nokia
Software MEA, Nokia.

KEY TAKEAWAYS

- Telcom service providers have access to unprecedented amounts of data.
- Telecom operators are among the world's biggest aggregators of consumer data.
- In addition to being meaningful, it is important that insights are available real-time.
- The icing on the cake is real-time actions on agile insights.
- Machine learning based advanced analytics helps in real-time decisioning.

Big Data and data analytics technologies transform the information into insights. They provide immense value for big organisations such as telecom companies and large enterprises. Big Data captures, analyses and helps in monetisation of huge volume of information and interaction data across multiple touch points in real time.

One of the clear beneficiaries of Big Data and analytics are the telecom service providers. In the past, the data was comprised of mainly call data records, then with the proliferation of Internet, we saw a surge in event data records. Now we have a deluge of social media feeds and with the advent of Internet of Things, data volumes are expected to grow exponentially.

Data assumes importance due to its nature and requires advanced processing capabilities as traditional application software cannot process this. The differentiation or key characteristics of Big Data include following five V's:

VOLUME
The name Big Data itself is related to the size, which is enormous.

VARIETY
The heterogenous sources and huge diversity of data type under the major category of structured and unstructured data.

VELOCITY
The speed of generation of data and access to it.

VERACITY
The quality of data.

VALUE
Relevance of data.

Telcom service providers have access to unprecedented amounts of data including consumer profiles, device data, network data, usage patterns, location data, apps downloaded. Telecom operators today are among the world's biggest aggregators of consumer data, and the volume of data will only continue to grow in the times to come.

In their Big Data journey, the following are some of the key points that telecom operators must keep in mind.

How to validate and ensure that accurate data is being aggregated. A data refinery solution, is helping service providers validate the incoming data and helping eliminate errors, duplication. Data refinery can take data inputs from varied sources including mobile networks, IMS, fixed networks, IP, broadband, cable, cloud.

It offers always-on, context aware data intelligence and is cloud ready with web-scale automation. More than 100 telecom service providers are using this solution and nearly 20% of world mobile data is passing through this system.

Many people say big data is better data, or data is the new oil, and so on and so forth. Big Data is the new soil. If nurtured properly with right tool sets and solutions, Big Data can yield benefits across industries. ■

DELL

DELL 24 GAMING MONITOR - SE2417HG

EXPERIENCE HIGH-QUALITY, GAMING ON THIS STYLISH, FULL HD MONITOR.

SMOOTH AND LIVELY VISUALS:

Experience high-quality visuals with an impressive 2-millisecond response time. Reduced deviation in transition time means the moving images in your movies or video games will be smooth and impressive.

solid

Available at:
SOLID SOLUTION TECHNOLOGY LLC
PO Box 242396, SOLID Showroom (Showroom & office)
Khalid Bin Waleed St. Bur Dubai, Dubai, UAE.
Tel: +9714 327 4545 ; E-Mail : sales@solid-me.com

USING MOBILE TECHNOLOGIES TO BREAK THE LAST-MILE BARRIER

Suitable mobile technologies like geo-location, track-and-trace, smart delivery, are required to bring down the cost and time of the last mile delivery.

KUSHAL NAHATA
Co-founder and CEO, FarEye..

KEY TAKEAWAYS

- To reduce delivery cycles and to cut down on operational expenses, companies have to give customers the feasibility to tag themselves.
- Logistics companies must adopt track-and-trace, last-mile delivery, integrated technology and smarter delivery management systems.
- The cost of last-mile constitutes 28%-32% of the total logistics costs and these are usually borne by the customer.
- Last-mile deliveries in the region are time-consuming with delivery cycle lasting 6 to 7 days or more.

Today's customers are digitally connected, engaged and influenced. In a quest to provide superior customer experience, the companies are incurring huge operational cost. The cost of last-mile constitutes 28%-32% of the total logistics costs and these are usually borne by the customer when he places the order or at the time of delivery.

The growing popularity of ecommerce has given rise to accommodate a new business model which is tech-driven logistics. Logistics players today are adopting unconventional solutions, smarter analytics and advanced processes to serve the digitally-empowered customer. With an eye on the growing base of ever-demanding customers, enterprises today are adapting to tailor-made solutions to suit their expectations.

To reduce the delivery time and in order to enhance the customer experience, enterprises must focus on adopting the right mobility solution that aids in running their field operations seamlessly. For example, last-mile deliveries in the region are time-consuming with the delivery cycle easily lasting for 6 to 7 days or more. The longer delivery window poses a challenge for the delivery personnel to carry the details of each and every parcel delivery.

With the help of mobility solution, that functions in 2G networks or even offline mode, the delivery personnel can save the information and update their managers in real-time. Adopting a flexible and future-oriented solution helps in generating automated reports on cash reconciliation, updating the task lists and the progress of the jobs allotted after the run-sheet is generated.

To reduce the delivery cycles and to cut down on the operational expenses, companies have to give customers the feasibility to tag themselves. Based on the geo-coordinates, the routing can be done by optimising all the nodal points where the delivery personnel should attend during the day.

Integration with multiple payment modules will give the flexibility to the customer to pay and finish the purchase. By using multiple payment options like Cash-on-Delivery and Card-on-Delivery, companies can reduce the cancellation at the time of delivery.

According to a recent report released by PayPal, Cash-on-Delivery in the Middle East is around 60%, while card payments and online payments occupy 25% and 15% respectively. These numbers have gone up from 15% and 5% in 2012.

Customers expect convenience and speed which entices logistics firms to venture into the possibilities of the virtual world. Innovative last-leg solutions, help in improving connectivity to ensure, speedy and affordable delivery. In order to ensure customer loyalty, logistics companies must adopt track-and-trace systems, efficient last-mile delivery methods, integrated technology and smarter delivery management systems. ■

WHY SERVICE PROVIDERS NEED TO FOCUS ON AGILE PROCESSES

Communications service providers need to build flexible processes allowing for change while adopting cloud platforms explains Santiago Madruga at Red Hat.

SANTIAGO MADRUGA
VP of Communications Service Providers Market, Red Hat EMEA.

Communications service providers across the world are looking to claim their position at the heart of the digital society, but they first need to become more agile and lean. There are many innovations that can help in this quest: network function virtualisation, software defined networking, the convergence of networks and IT, cloudification, DevOps, and more.

In most cases the required technologies are now available and ready for mission-critical environments. However, the surrounding operational processes and mindset are often in need of a review.

Communications service providers are already modernising. Examples include the likes of Altice Group, which is building a holistic network function virtualisation platform with ambitious timelines for getting the majority of mobile traffic running on it. Or Three UK, which has developed a world-first cloud-native core network, designed to be massively scalable so it can respond to subscribers' service demands.

> AGILITY AND EFFICIENCY DO NOT COME FROM TECHNOLOGY INNOVATION ALONE, BUT ALSO REQUIRE CHANGES IN PROCESS, MINDSET AND CULTURE.

Once communications service providers have these initial network function virtualisation use cases up and running, they need to turn their attention to how to scale these out, adapting and improving their operational processes and, in many cases, the way they think about their operation altogether in order to become more agile and lean.

Open source is a key change agent in this process. It brings the desired innovation, yet is fundamentally different, in the way it is engineered, to other technologies - and communication service providers need to understand how can they avoid the risks and reap the benefits.

Cloudification brings speed, efficiently. Digital-native businesses that are born in the cloud are more agile and innovative, including many over-the-top companies that now compete with communications service providers for the value-add services that drive margins and customer loyalty. These companies can more freely experiment with new services without huge amounts of upfront investment or commitment, and they are not afraid to fail fast. And when a service does take off it can scale quickly and reliably.

Most communications service providers were not born directly in the cloud, but are fast adopting it. They are making the move away from dedicated hardware, away from monolithic systems

MUCH FASTER CHANGE IS POSSIBLE WITHOUT JEOPARDISING OPERATIONS BUT REQUIRES A REVIEW OF ORGANISATIONS, PROCESSES AND MINDSET.

KEY TAKEAWAYS

- Cloudified environments are different and break the relationship between software and hardware.
- As old systems come to the end of maintenance lifecycle every new system is designed for modern architectures.
- Most communications service providers were not born directly in the cloud but are fast adopting it.
- Communications service providers are making the move away from monolithic systems running on a specific piece of equipment.
- It is unrealistic to expect sweeping reform among the communications service providers community.
- Building open cloud platforms to enable virtualisation is a first step.
- Most communications service providers were not born directly in the cloud, but are fast adopting it.

with proprietary software running on a specific piece of equipment.

However, this is a change that may take some time for communications service providers, which typically have significant legacy systems that may still not be fully paid off. But as their old systems come to the end of their maintenance lifecycle, or as new initiatives are launched, every new system is designed for more modern architectures.

These are typically based on open source, helping to avoid proprietary lock-in, and perhaps more dangerous: the customisation of open source code that deviates from standard upstream communities.

Agility and efficiency do not come from technology innovation alone, but also require changes in process, mindset and culture. Red Hat's recent Open Source Culture Survey revealed that 91% of respondents across industries thought that technological developments were changing the way their organisation had to operate in order to succeed. 81% respondents agreed that having an open organisational culture is important to their company.

However, only 67% of respondents said that their organisation has the resources necessary to build an open culture, with 59% of them identifying legacy systems and outdated technology as a barrier to change. When it comes to human resourcing a technology roll-out, having the right skill sets on board is only half of the challenge; having those people work in the most efficient way is the other.

Communications service providers have grown used to working in a certain way. Typically, they work on projects from beginning to end, ensuring that any new service or application is absolutely watertight before it is deployed. And rightly so. In the old inflexible world this is completely necessary. The ability to revise things on the fly is not an option.

Cloudified environments are different. They break the relationship between software and hardware, and even between different layers of software architecture, enabling flexibility and hybridity. Much faster change is possible without jeopardising reliability and operations, but this also requires a review of organisations, processes and mindset.

Knowing this and doing this are two very different matters though. It is unrealistic to expect sweeping reform among the communications service providers community. It is more likely to happen on a project by project basis, step by step. Building open cloud platforms to enable virtualisation is a first step, and communications service providers are well on the way with this.

The benefits of embracing the next-generation wave of technologies is well documented, and just about every communications service provider on the planet is looking at how it can accelerate the transition. ■

WHY THE BITCOIN BLOCKCHAIN IS TOO LARGE TO BE HACKED

For the blockchain to be hacked, it means 51% of the miners would need to be compromised all at one point of time, writes David Warburton, at F5 Networks.

DAVID WARBURTON
Senior Threat Research Evangelist EMEA, F5 Networks.

Blockchain technologies present opportunities for disruptive innovation. However, they also present controversy, especially with regards to the security of cryptocurrencies like Bitcoin. Released as open-source software in 2009, Bitcoins are created as a reward for a process known as mining and can be exchanged for other currencies, products, and services. Much has been discussed about its robustness, so, could the notion that a 51% attack on a blockchain could move from theoretical to possible?

Traditional money is created through central banks, but Bitcoins are mined by Bitcoin miners: network participants that perform extra tasks. Specifically, their computers perform complex mathematical operations in order to find the solution for a block of transactions. Once this problem has been solved, the miner submits their solution, along with the block itself, to the distributed ledger.

At this point, all transactions in this block are locked in and since each solution to the newest block is dependent on every block that has come before it, it creates a long chain of trust in which every transaction can be proved to be valid. This prevents a user from spending the same Bitcoin twice; it solves the double spend problem.

All blockchain miners are effectively in a race with each other. The first one to find the solution to the current block is the winner and gets awarded the prize of some amount of Bitcoin. Since the mathematical problem for each block is cryptographically based, each miner has, in theory, as good a chance as any other miner to find the solution. The only way to have a better chance of being the winner is to control more miners.

In theory, the larger the distributed network of blockchain miners, the harder it is to create a majority share. For example, the rate at which an individual might discover the correct block hash is extremely low – around 12.5 Bitcoins per block. To increase their earning potential, miners grow collective processing power in mining pools by partnering with others.

For organised criminals wanting to control a blockchain, possibly to submit their own fraudulent

FOR ORGANISED CRIMINALS WANTING TO CONTROL A BLOCKCHAIN THEY WOULD NEED TO CONTROL OVER 50% OF ALL MINERS FOR A PARTICULAR BLOCKCHAIN.

A COORDINATED ATTACK ON THE BITCOIN NETWORK WOULD REQUIRE OVER 1.2M MINERS TO ENSURE THEIR FRAUDULENT BLOCKS WERE ACCEPTED BY THE REST OF THE MINERS.

blocks which might allow them to double-spend, they would need to control over 50% of all miners for a particular blockchain.

There are an estimated 2.4 million Bitcoin miners today and this increase in miners on the network means 51% attacks on Bitcoin are practically impossible. Recalling this attack requires a majority share in miners and a coordinated attack on the Bitcoin network would require over 1.2m miners to ensure their fraudulent blocks were accepted by the rest of the miners.

However, even if this were possible, in order to ensure your fraudulent block was permanently accepted by the blockchain, a series of consecutive bad blocks is required before they are accepted by the rest of the Bitcoin network. The likelihood is that before any attacker can create this scenario, other miners on the network would have noticed this attack and invalidated the fraudulent blocks.

These attacks are still uncommon as it remains unfeasible, even for the big players, to finance and operate the huge number of miners required to attack Bitcoin. It used to be possible to mine for Bitcoin on relatively inexpensive computer graphics cards. However, due to the sheer number of miners on the network and the current pay-out of 12.5 bitcoin per block, specialist chips known as ASICs are now the only affordable way to mine.

However, this raises the bar further in terms of what is required to run a significant Bitcoin mining pool because it shifts the balance of power. Depending on the currency you want to mine or attack, the initial outlay would be higher, and the attacker would need significantly fewer ASICs compared to GPUs.

Today, attacks against cryptocurrencies are generally against the users of the system and not the cryptography itself. Therefore, 51% attacks still seem unlikely. It is easier to steal any cryptocurrency by getting access to a user's wallet private key or by attacking a cryptocurrency exchange.

Nevertheless, it is undeniable that they are possible and we are starting to see more of them occur. For example, Shift and Krypton, both based on Ethereum, were subject to a 51% attack in 2016 and in May of 2018, Bitcoin Gold, distinct from the more popular Bitcoin, was also subject to the same attack. ■

KEY TAKEAWAYS

- Attacks against cryptocurrencies are against the users of the system and not the cryptography itself.
- It is easier to steal cryptocurrency by getting access to a private key or by attacking a cryptocurrency exchange.
- Shift and Krypton, both based on Ethereum, were subject to a 51% attack in 2016.
- Traditional money is created through central banks, but Bitcoins are mined by Bitcoin miners.
- All blockchain miners are effectively in a race with each other.
- Each miner has, in theory, as good a chance as any other miner to find the solution.
- There are an estimated 2.4 million Bitcoin miners today.

IF YOUR APPLICATION IS HACKED SO CAN YOUR BLOCKCHAIN

The application that uses a blockchain technology needs to be secured as much as the blockchain itself explains Morey Haber at BeyondTrust using a checklist.

MOREY HABER
Chief Technology Officer, BeyondTrust.

I am simply amazed at all the buzz around Bitcoin, blockchain, and cryptocurrency. However, the truth is that blockchain has a limited place in business and needs to be secured just like any other application, with some twists.

Blockchains are not a database replacement, nor will future applications that utilize them. They are a multi-node distributed ledger system that secures entries based on volume and verification. Natively, blockchain can only process a limited number of transactions per second and cannot store complex records or blobs—only ledger-style information that has a finite start date, like shipping information.

As such, historical records, pictures, complex indexes, and other large datasets are just not good for blockchain technology. This is one of the problems security teams need to understand.

Think of a blockchain implementation like an old school peer to peer network technology from Napster or BearShare. Each node contains a database of all records and any new entries need to propagate to all other nodes for validity.

While a peer-to-peer network queries its peers for entries, blockchain actually contains a duplicate of all entries compared to its peers. This means tampering with one node does not invalidate the entire blockchain. As a consequence, every entry has to be properly validated to be accepted as a ledger entry and propagated to other nodes.

This is where security is so critical. Entries into the blockchain ledger need to be validated for fraudulent activity, and more importantly, the hosts containing blockchain implementations need to be secured against vulnerabilities and privileged attacks that could compromise or tamper with blockchain insertions.

There is no concept of blockchain ledger modifications — this is key to protect the integrity of the data. Once an entry is accepted, it is permanent. Therefore, if you can attack the server, application, and ledger processes, you can tamper with the blockchain. This is how some of the recent cryptocurrency attacks have been occurring.

To cite a recent example, on Monday, May 28th 2018, The Hacker News reported on a wicked vulnerability within the EOS Blockchain Platform. While the vulnerability is considered critical, and the method of exploitation fairly basic - a maliciously crafted file, the ramifications are truly astounding.

After the vulnerable parser reads the file, it forces an exploit on the node which could then be leveraged against the supernode on the EOS platform. The supernode is responsible for collecting transaction information and packing it into blocks. Once the threat actor owns the supernode, they can modify or create malicious blocks that would control the entire EOS network.

SEAGATE

Only the Strongest Thrive

Rely on your 14TB drive.

ASBIS®

Phone: +971-4-8663850
Email: info@asbisme.ae
www.asbisme.ae

KEY TAKEAWAYS

- Blockchain has a limited place in business and needs to be secured just like any other application.
- Think of blockchains as just another application for data storage, with limited capabilities and not very fast.
- Blockchains are designed to be highly distributed and 100% reliable.
- If your application or host can be tampered with, so can your blockchain.
- The goal is to secure the application and blockchain during their design and implementation so this can never occur.
- Modifications and deletions of blockchain records are not permitted.

This includes everything the EOS Blockchain Platform has been implemented to perform—from cryptocurrency, supply chain management, to identity storage. Let this sink in — the uncrackable blockchain as it is advertised, can be owned by the fundamental technology designed to protect it - WASM files, smart contract and a simple file upload.

So how do we secure blockchain implementations? We first start with cyber security basic hygiene:

1. ASSET INVENTORY

Identifying and managing the lifecycle of all software, code, applications, nodes, and operating system used in the blockchain.

2. CHANGE CONTROL

Ensuring changes to the operating system, application, and resources are documented and go through a formal change control process.

3. CONFIGURATION MANAGEMENT

The hardening and removal of default settings that are a liability for the operating system, application, or network.

4. VULNERABILITY MANAGEMENT

Ensuring that the operating system, application, web application, and source code are reviewed for vulnerabilities and risks are prioritized accordingly.

5. LOG MANAGEMENT

Centrally managing and parsing log files from all resources in the environment including transaction logs.

6. PATCH MANAGEMENT

Using a systematic and predictable methodology for deploying maintenance and security patches to all systems in the environment—from firmware to web applications and everything in between.

7. IDENTITY AND ACCESS MANAGEMENT

The predicable workflow management of identities, roles, and entitlements for all users that have access to resources of the system.

8. PRIVILEGED ACCESS MANAGEMENT

The management of all privileged access into the blockchain environment—from operating system to web applications including password management, least privilege access, session management, keystroke logging, and application to application key and password management.

New entries into the blockchain should be secured with dynamic privileges and only valid for one-time usage. This can be done with privileged password access solutions and keys or passwords using an API. An insecure insertion path into the blockchain can lead to devastating results.

Reads from the blockchain should be secured in a similar fashion to ensure the retrieval is not tampered with, like a man in the middle attack, before processing by the application.

Since modifications and deletions of blockchain records are not permitted, all entries must be 100% valid or the entire ledger model could be compromised.

Think of blockchains as just another application for data storage. It has limited data storage capabilities, is not very fast, but is designed to be highly distributed and 100% reliable. If your application or host can be tampered with, so can your blockchain. The goal — securing both during their design and implementation so this can never occur. ■

Rittal – The System.

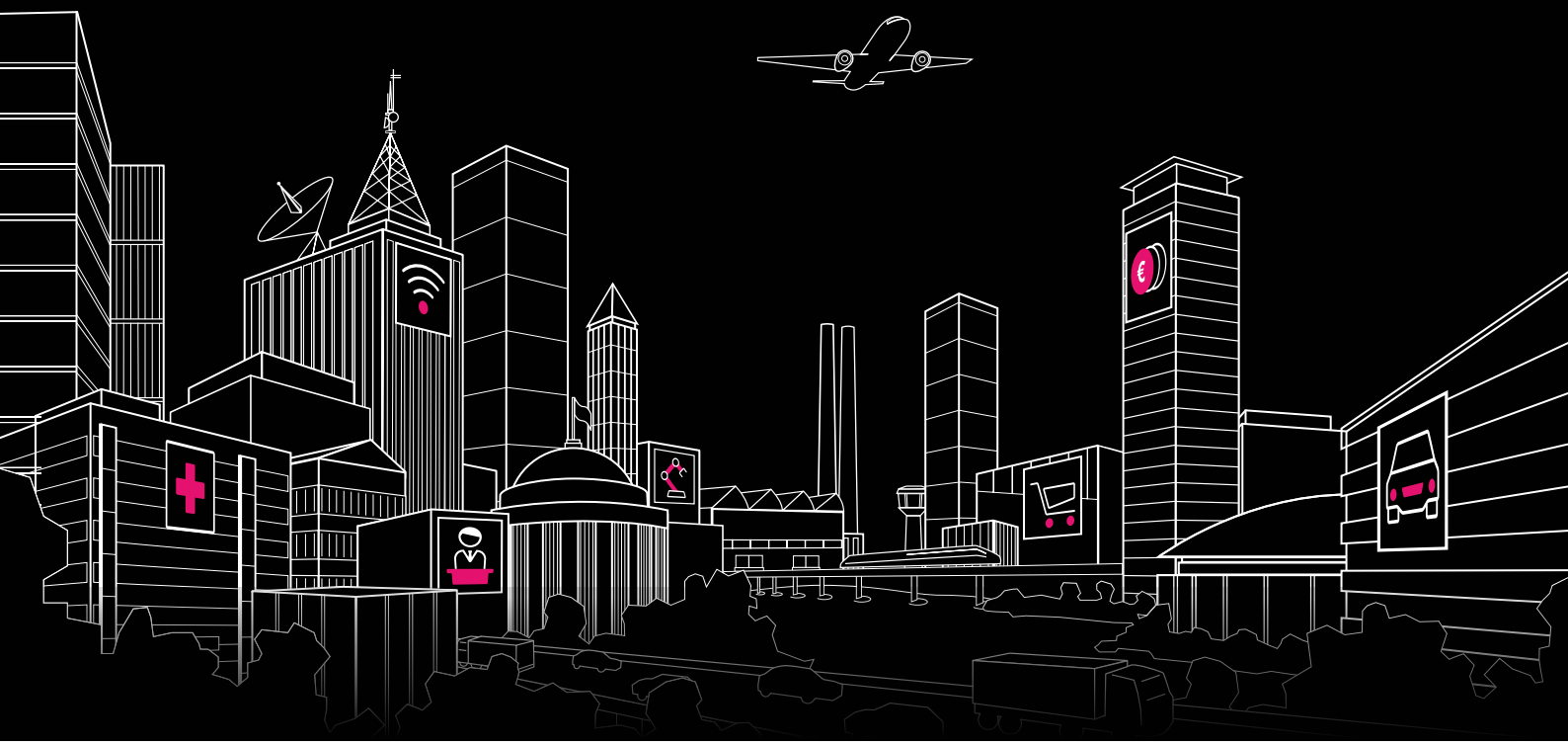
Faster – better – everywhere.

Discover the Edge.

Smart Solutions. Real Business.

Rittal solutions for the technology of the future.

Edge computing enables enormous amounts of data to be processed directly at the place where they arise. Securely and in real time. Rittal prepares you and your IT infrastructure for new challenges - flexibly, economically, and globally.



Visit us at

Sheikh Rashid Hall
Stand SR-E2

38TH **GITEX** TECHNOLOGY WEEK

14 - 18 OCT 2018
DUBAI WORLD TRADE CENTRE

For Enquiries:
Rittal Middle East FZE
Tel: +971-4-3416855 I Email: info-it@rittal-middle-east.com I www.rittal.com/uae-en

ENCLOSURES | POWER DISTRIBUTION | CLIMATE CONTROL | IT INFRASTRUCTURE | SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

RITTAL

ConsenSys to conduct three-day blockchain developer training, hackathon in Lebanon

ConsenSys announced it will be conducting a three-day blockchain developer training followed by a two-day hackathon in Lebanon on 17 October 2018. From the workings of blockchain technology to its applications and features, participants will receive in-depth training on how to create a development environment, build decentralised applications with Ethereum smart contracts and integrate the dApps with web applications.

With blockchain for social impact high on the ConsenSys agenda, 25 percent of the spaces available will be provided for free to refugees who are already adept at programing.

Strategy& and Beirut Digital District have been brought on board as Platinum Sponsors. Middle East Venture Partners and Flat6Labs will be Silver Sponsors and ArabNet and TechFugees as community partners are supporting this initiative with the aim to empower talent in Lebanon.

The website lebanonbootcamp.consensys.net is now live with applications closing on September 30. The 3-day training will be held at Beirut Digital District on October 17 followed by a 2-day hackathon. Prizes will be awarded to the top 3 winners.

ConsenSys is a venture production studio and custom software development consultancy building decentralised applications, enterprise solutions, and developer tools for blockchain ecosystems, focused primarily on Ethereum. ■

Honeywell Process recognised for engagement, costing, risk sharing by Maire Tecnimont

Honeywell Process Solutions has been named Best Instrumentation and Electrical Material Partner by global technology licensor and engineering, procurement and construction contractor Maire Tecnimont Group. Honeywell was recognised for results across six areas of its work with Maire Tecnimont, which included early engagement, competitive total costing, risk sharing and impeccable execution.

The award was presented to Honeywell at a ceremony during the SEENERGY event, dedicated to the group's supply chain. More than 70 CEOs of partner companies attended the event in Milan, Italy representing about €900 billion of revenue and almost four million workers.

Honeywell has had a long and successful relationship with Maire Tecnimont, which encompasses 50 operating companies and more than 8,500 professionals. Maire Tecnimont manages large turnkey EPC projects in more than 40 countries.

Honeywell has collaborated with the group to deliver numerous projects, providing and implementing automation controls, safety and cybersecurity solutions. It also has recently started to develop innovative business models with the group around its Honeywell Connected Plant solutions, which is a suite of applications that delivers higher levels of safety, reliability, efficiency and profitability. It is also a vendor Honeywell's Industrial Internet of Things solution.

(Left to right) Elio Petruncelli, Purchasing Group Leader, Tecnimont; Ezio Pasqualon, Process Control and Automation Head Of Department, Tecnimont; Paolo Solzi, Global EPC Business Director, Honeywell Process Solutions; Paolo Mondo, Group Procurement Vice President, Maire Tecnimont Group; Pierroberto Folgiero, CEO, Maire Tecnimont Group. ■

Pure Storage launches new data hub to boost AI solutions and eliminate storage silos

MATT BURR, GM of FlashBlade, Pure Storage

Pure Storage, introduced a data hub, the company's vision to modernise storage architecture for unstructured, data-intensive workloads. Built on Pure Storage FlashBlade, Pure's data hub is designed to be data centric and enable organisations to effectively utilise today's most critical currency – data.

To innovate and survive in a business environment that is increasingly data-driven, organisations must design infrastructure with data in mind and have complete, real-time access to that data. Today's mainstream solutions were designed for the world of disk and have historically helped create silos of data. A data hub is designed to deliver, share and unify data to ultimately unlock unprecedented value.

Today, organisations rely on four inherently siloed analytics solutions: data warehouse, data lake, streaming analytics and AI clusters. A data hub integrates the most important features of these four silos and unifies them into a single platform.

A data hub must have four key characteristics:

HIGH-THROUGHPUT FOR BOTH FILE AND OBJECT STORAGE

Backup and data warehouse appliances require massive throughput for mainstream, file-based workloads and cloud-native, object-based applications.

TRUE SCALE-OUT DESIGN

The power of data lake is its native, scale-out architecture, which allows batch jobs to scale limitlessly as software -- not the user -- manages resiliency and performance.

MULTI-DIMENSIONAL PERFORMANCE

Data is unpredictable and can arrive at any speed – therefore, organisations need a platform that can process any data type with any access pattern.

MASSIVELY PARALLEL

Within the computing industry, there has been a drastic shift from serial to parallel technologies, built to mimic the human brain, and storage must keep pace.

"Organisational data silos are a universal pain point across every industry. Businesses need to realise value from data even when it is out of sight and out of mind, which is impossible without insight into the full picture," said Matt Burr, GM of FlashBlade, Pure Storage. "With a data hub, we have created a central storage system that satisfies current and future application requirements with a modern platform designed to work on customers' behalf."

"For decades, the storage industry has been a laggard. Not only has storage failed to keep up with advances in networking and compute, it has become a roadblock to innovation," said Ritu Jyoti, Program Vice President, Systems Infrastructure Research Portfolio at IDC. "In the era of AI and real-time analytics, roadblocks have the potential to disrupt Fortune 500 companies within a short span of time. It is time for a paradigm shift for storage -- a new dynamic architecture, purpose-built for modern challenges." ■

KEY TAKEAWAYS

- Pure's data hub is designed to be data centric and enable organisations to utilise data.
- Mainstream solutions were designed for the world of disk and have historically created silos of data.
- A data hub is designed to deliver, share and unify data to unlock value.
- Organisations rely on four siloed analytics solutions: data warehouse, data lake, streaming analytics and AI clusters.

Mobility MEA to boost corporate mobility as approved Android zero-touch partner

Mobility MEA, a systems integrator, enterprise managed mobility service provider and a GEMA alliance partner, is now the first approved Android zero-touch enrollment partner for the MEA region. The company will serve to accelerate automated deployments, reducing dependency on internal IT support, simplifying setup and management of Android mobile devices; and making time-consuming device configuration a thing of the past through processes that create better user experiences.

Zero-touch enrollment, which supports OEMs, carriers and companies, eliminates the need for users to configure their Android devices while ensuring corporate policies are in place. With this enrollment, companies can configure the devices they purchase and have them shipped with management and settings pre-configured, ready for immediate use by the employees. Support for end-users is also easy, as they can just sign in and get access to their work apps and data.

Since a majority of smartphones are based on the Android platform, zero-touch enrollment makes Android rollouts more seamless and secure, allowing IT to deploy corporate-owned devices in bulk without having to manually setup each device. It is a streamlined process for Androids set up especially for enterprise management offering efficient deployment, and making large scale roll outs fast, easy and secure for organisations and employees.

As workforce mobility is fast becoming an integral part of business, it is highly important for an organisation to manage its mobile workforce, ensuring staff is productive while also securing the devices and data. With the proliferation of smartphones around the world, millions of devices are being deployed by companies which are required to be managed in an efficient and smooth manner.

ZOFF KHAN, Co-founder and CEO of Mobility MEA.

Mobility MEA represents Global Enterprise Mobility Alliance across the licensed territories to execute Enterprise Mobility Solutions locally at all stages of MMS Consult, Deploy, Manage, and Assist. GEMA International is a world-wide mobility enabling partner that helps hundreds of mobile device companies to develop and operate mobile business solutions with simplicity and flexibility.

Mobility MEA offers global mobility services through in-country experts with local language and local insight to ideally support the global mobile workforce, while guaranteeing centralised governance, auditing and reporting. Mobility MEA provides fully scalable, worldwide mobility solutions to global enterprises everywhere, keeping the mobile workforce reliably connected, serviced and up-to-date with 24x7 help desk support, tailored device deployments and break fix support.

Mobility MEA offers enterprises, governments, and carriers fully agnostic support through EMM partnerships which include BlackBerry, MobileIron, Airwatch, SOTI and Nationsky as well as additional mobility solutions such as secure voice and omnichannel. ■

KEY TAKEAWAYS

- Accelerates automated deployments, reducing dependency on internal IT support, simplifying setup.
- Make time-consuming device configuration a thing of the past
- Supports OEMs, carriers, companies, eliminates the need for users to configure their Android devices ensuring corporate policies are in place.
- Set up for enterprise management offering deployment, large scale roll outs, easy and secure.


On-prem and remote workers.
Multi-platform workloads.
Security across domains.
Manual network operations.
A HEADHACHE-SOLVING SECURE AND AUTOMATED MULTICLOUD SOLUTION.
When you manage your physical and virtual networks together, you simplify operations throughout your multivendor IT environment. Where a workload resides or where users login shouldn't matter. Contrail Enterprise Multicloud satisfies IT's requirements to unify control and visibility for networking and security.
Learn more at juniper.net/cloud
Visit us at Gitex 2018
Dubai World Trade Centre
Hall 6, C6-01
JUNIPER NETWORKS
Engineering Simplicity

Dell EMC introduces analytics, cloud at Saudi Arabia's Princess Nourah University

In alignment with the Saudi Vision 2030 to promote a knowledge-based economy, Princess Nourah bint Abdulrahman University, the largest university for women in the world, partners with national and international organisations to provide distinguished degrees and certificates for Saudi female students and graduates. PNU partnered with Dublin City University to launch the first Masters in Computing degree with specialisation in Data Analytics in Saudi Arabia.

With the vision of providing a comprehensive learning programme for women and recognising the requirement for new skills with the influx of technological developments, the College of Computer and Information Sciences is embedding a variety of certifications and technical trainings into its curriculum for three bachelor degrees, Computer Science, Information Systems and Information Technology.

As a member of Dell EMC's External Research and Academic Alliance Programme, the college has successfully trained and certified 57 female data science and big data analytics students this semester with an additional 103 students certified in Cloud Infrastructure. The leading university also successfully introduced VMware Install, Configure and Manage course as an elective training course for senior students.

Advancements in education of the future workforce are at the core of the Saudi Arabia's Vision 2030 and the National Transformation Programme in addition to the focus of the national curriculum and training on innovation in advanced technologies and entrepreneurship.

A recent study by Dell Technologies titled Realising 2030: A Divided Vision of the Future highlighted the lack of workforce readiness as the leading barrier in the Middle East to becoming a successful digital business in 2030, further emphasising the need for skill development among existing employees and future generations. The explosion of data further fuels the requirement for individuals to build expertise in niche and specialised fields as digital environments continue to evolve.

Catering to the vision of driving workforce readiness through academic solutions, Dell EMC actively engages with academic thought leaders and business partners to foster research partnerships and unique programs including foundational IT courses. These courses cover information storage and management, cloud infrastructure and services, data science and big data analytics, and data protection and management. The programme also provides free e-learning technology courses to institutions.

Mohammed Amin, Senior Vice President and Regional Manager, Middle East, Turkey and Africa, Dell EMC, said "The unrelenting pace of digital transformation in the marketplace is creating new challenges for all of us where organisations as well as individuals are increasingly realising that investing in workforce readiness and the development of new skills is key to future success and competitive differentiation. Dell EMC recognises successful digital transformation requires more than technology and therefore we are helping leading universities develop the critical talent required for the future and ultimately fuel digital progress."

KEY TAKEAWAYS

- Advancements in education are at the core of the Saudi Arabia's Vision 2030 and the National Transformation Programme.
- A study by Dell Technologies highlighted lack of workforce readiness as the leading barrier in the Middle East to becoming a successful digital business in 2030.
- The explosion of data fuels the requirement for individuals to build expertise in niche and specialised fields.

Drones complete 10,000 km across Middle East and Africa for Dubai based Falcon Eye

Falcon Eye, Dubai based drone-powered solutions company, is celebrating 10,000 flights across the Middle East and Africa based projects. The company revealed its ambitious plans to double its operations in the next few years with the market promise of reaching the value of $1.5bn by 2022 only in the GCC according to the latest report.

After covering the area of nearly 34,000 kilometers since company's operational inception in 2014, Falcon Eye Drones are convinced that organisations that will adopt drone applications within their operations will play a central role in the development of the regional drone industry.

While the Middle East rapidly grows and innovates, drones will play an instrumental role in the development of multiple projects that are expected to be delivered in record times. Drones will not only support timely infrastructure developments but will allow citizens to experience their unlimited potential and benefits.

According to the statement released by the Dubai Future Foundation several months ago, His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai called on all Dubai Government entities to embrace disruptive innovation as a fundamental mantra of their operations and to seek ways to incorporate its methodologies in all aspects of their work when launching Dubai 10X initiative.

The proliferation of drone technologies in the region is also dependent on the various legislations and regulations that support them. Airspace regulators are conscious of the growth of drone technology and are looking for a balance between public safety and economic efficiency.

The progress of drone legislation and regulation in the region is underway. The drone traffic control center will soon serve as a centralised authority to manage drone traffic and ensure regulations are followed. Following dynamic drone market expansion insurance companies will be able to soon unlock new market potential.

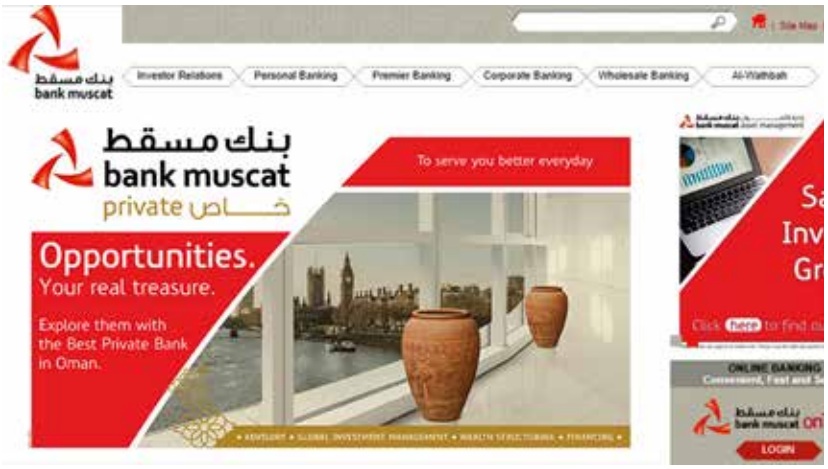
"Drones are becoming an instrumental technology for many industries such as oil and gas, utilities, telecom, construction, transportation, city infrastructure developments, agriculture, archeology, safety and security as well as photography and videography. Drone technology is quickly growing beyond its original military applications and is making a very big impact on the commercial sector", says Rabih Bou Rashid, Managing Director of Falcon Eye Drones.

Rabih added: "In order to harvest the full potential smart city developments represent, it is important for all the industries that make an impact on this transformation, to become cost-effective, agile and disruptive. Civil drones will help this region to excel by introducing drone applications to collect valuable data, make measured decisions, capitalise on data automation and imaging capabilities." ■

KEY TAKEAWAYS

- The proliferation of drone technologies in the region is dependent on various legislations and regulations that support them.
- Airspace regulators are conscious of the growth of drone technology and are looking for a balance between public safety and economic efficiency.
- Following dynamic drone market expansion insurance companies will be able to soon unlock new market potential.
- The progress of drone legislation and regulation in the region is underway.

Bank Muscat and SAS recognised for Best Data Analytics initiative in the Middle East



Bank Muscat, the flagship financial services provider in the Sultanate of Oman, and SAS have been awarded for Best Data Analytics Initiative, Application or Programme in the Middle East for 2018 at The Asian Banker Middle East and Africa Awards Programme.

Bank Muscat engaged SAS to implement customer relationship management, channel integration for their growing business demands. The bank integrated multiple customer data touch points with the SAS Marketing Automation analytics engine to analyse the customer behavior in cross-sell offers, digital offers and promotions. This involves multichannel integration, including mobile banking, internet banking, automated teller machine, cash deposit machine, SMS and emails.

Bank Muscat's implementation of the system allowed for greater customer scalability. The increase in customer reach through scalable solution implementation is helping the bank to increase the cross-sell revenue. In addition, the project improved operational efficiencies, increased lead conversion, and enhanced real time access to customer data, enabling personalised product offering for higher cross-sell.

It also allowed the analytics system to act immediately on data such as customer transactions, eChannel activity, and branch to generate relevant cross-sell offers for the sales team. Transactional data was also used to generate trigger-based events and alerts for other business teams to act accordingly.

Commenting on their win, Abdullah Tamman Al Mashani, DGM – Institutional Sales and Product Development, Bank Muscat, said, "We are proud to be recognised among the banking fraternity for our innovation-driven strategic initiatives. Our commitment to customers is key to providing industry-leading services and setting new benchmarks in banking excellence, in line with our vision and values. We chose SAS as our trusted partner on our journey to offer innovative services and products to our customers and stakeholders."

Abed Hamandi, Regional Director Professional Services, Middle East and Africa at SAS, said, "Today, customer experience is taking center stage and price is no longer the only determining competitive advantage of an organisation. Bank Muscat and SAS, both believe that the key to ensuring customer satisfaction is capitalising on data and analytics. Our strategic partnership is built on the approach of delivering data-driven customer intelligence that can optimise marketing efforts and result in authentic customer engagement."

Bank Muscat is a financial services provider in Oman with a presence in Corporate Banking, Retail Banking, Investment Banking, Islamic Banking, Treasury, Private Banking and Asset Management. The Bank has the largest network of 149 branches, 645 ATMs and CDMs, and more than 18,000 PoS terminals. The international operations include Riyadh, Kuwait, Dubai, Singapore and Iran. ■

KEY TAKEAWAYS

- Bank Muscat engaged SAS to implement CRM channel integration for growing business demands.
- The bank integrated customer touch points using SAS Marketing Automation to analyse cross-sell offers and promotions.
- Includes mobile banking, Internet banking, ATM, cash deposit, SMS, emails.
- Increase in customer reach through scalable solution implementation is helping the bank increase cross-sell revenue.

No.1 Trusted Software System Integrator..!

- Digital Transformation
- Blockchain
- Robotic Process Automation
- AI & Chatbots
- Customer Relationship Management / CEM
- Corporate Performance Management
- Big Data / IoT
- Business Intelligence & Analytics
- Enterprise Content Management
- Governance, Risk & Compliance
- HCM Solutions & Services
- Infrastructure Management

FINESSE

MENA | APAC | AMERICAS

300+ Professional Team **200+** Enterprise Clients **30+** International Awards
20+ Nationalities **10+** Global Locations

finessedirect.com finessedirect +9714 3687855 info@finessedirect.com

Emirates Transport initiates business transformation leveraging Oracle Cloud suite

Emirates Transport, one of the largest transport and logistics services companies in the Middle East, will implement Oracle Cloud Applications to drive a major digital transformation across all its core business operations. The initiative will help Emirates Transport introduce innovative offerings that create new revenue streams, deliver exceptional customer service and drive operational efficiency.

With Oracle Cloud Applications, the Emirates Transport leadership team will be able to take advantage of a complete and fully integrated suite of applications to increase business agility and reduce costs. The new cloud applications will provide Emirates Transport with full financial control, simplifying procurement processes and allowing the management to make data driven investment and business decisions.

The Emirates Transport management team will also be able to run simulations for new services and programmes to ensure an exceptional customer experience and high employee engagement.

"The UAE's transportation sector is experiencing sustained growth on the back of promising economic activities across infrastructure development, government investment and private sector expansion", said Faryal Tawakul, Executive Rirector of Support Services at Emirates Transport. "These changes have created significant growth opportunities for Emirates Transport and by using the latest cloud technologies to drive expansion and offer unmatched services to our customers; we will be able to establish a huge competitive advantage."

"We selected Oracle to support our transformation into a service focused company and to help establish Emirates Transport as the preferred transportation and logistics partner for the UAE's public and private sector. This is our first step towards implementing a more elaborate digital transformation roadmap which in due course will also explore the implementation of next gen technologies like Artificial Intelligence and Internet of Things to help us drive long term growth", added Tawakul.

"With more than a three-decade experience in the UAE, Emirates Transport is a true market leader and a key enabler for the country's economic progress. Emirates Transport is now embarking on its next growth phase and its decision to select Oracle to support its digital transformation initiative will help the organisation achieve its strategic business objectives", said Arun Khehar, Senior Vice President, Business Applications, ECEMEA, Oracle.

Emirates Transport is a federal government corporation, with financial and administration independence. Despite its prominence in the school transport sector, Emirates Transport has witnessed huge investment growth and diversification in its services during its 37-year history.

ET continues to witness a steady growth, making it the largest federal corporation in the United Arab Emirates, particularly in terms of the number of its human resources, which currently stands at more than 24,000 employees. In addition, the Corporation boosts a large fleet, numbering more than 25,000 vehicles, and a vast infrastructure with its headquarter in Umm Al Ramool, Dubai, as well as 43 work sites throughout the UAE. ■

KEY TAKEAWAYS

- Emirates Transport will implement Oracle Cloud Applications to drive a major transformation across its core business operations.
- The initiative will help create new revenue streams, customer service and operational efficiency.
- With Oracle Cloud, Emirates Transport will take advantage of a suite to increase business agility and reduce costs.

PURESTORAGE®

WE HELP YOU BUILD A DATA-CENTRIC STRATEGY

We're in a new world: data is now a strategic asset, and enterprises will need data-centric strategies to succeed and thrive. So it's time to re-think IT infrastructure from the bottom-up.

Visit Pure Storage at Gitex 2018: Booth A7-10 Hall 7

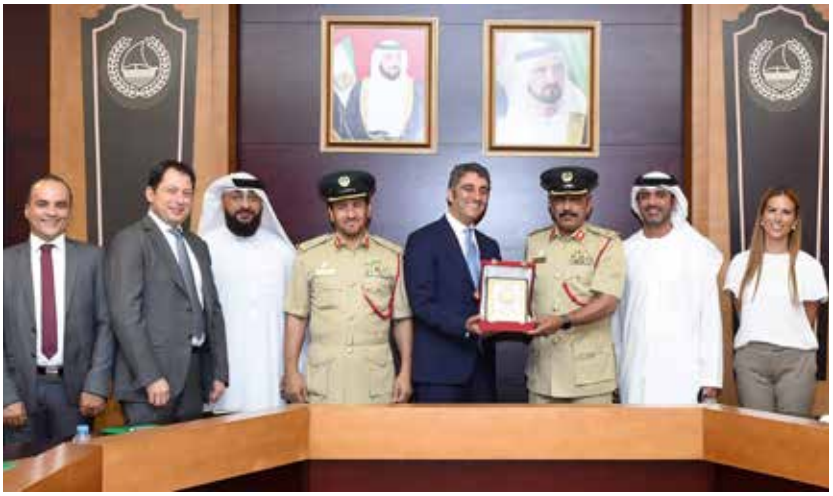
purestorage.com

Smart police station to be developed at Majid Al Futtaim's community Tilal Al Ghaf

Dubai Police and Majid Al Futtaim, signed a Memorandum of Understanding to collaborate in areas that empower, deliver and promote an efficient, seamless, safe and impactful city experience for residents. Under this agreement, a Smart Police Station will be developed at the company's flagship new Dubai Community, Tilal Al Ghaf, as part of its innovative Smart Districts plan.

The MOU was signed by Major General Muhammad Saeed Al Marri, Assistant Commandant for Community Happiness and Equipment at Dubai Police, and Hawazen Esber, Chief Executive Officer of Communities at Majid Al Futtaim, Properties at a signing ceremony held in Dubai.

Major General Muhammad Saeed Al Marri, Assistant Commandant for Community Happiness and Equipment in Dubai Police, said: "Smart Police Stations are part of our vision to support happiness in Dubai, improving access to police services for members of the public. It will provide members of the public with



24-hour access to police services in a neighbourhood setting, where the construction of a conventional police station would not be possible."

"The smart police stations will offer innovative, high-quality services, including 27 criminal, traffic and community services as well as 33 allied services that will operate without any human intervention," Maj Gen Al Marri added.

Hawazen Esber, CEO of Communities at Majid Al Futtaim, Properties, commented: "This agreement demonstrates Majid Al Futtaim's commitment to Dubai's Smart Cities vision by providing residents at Tilal Al Ghaf with the highest standards of community living. The Smart Police Station is in line with the community's innovative 360-degree plan to promote happiness and public safety by using smart technology. Offering services locally, close to people's homes, also reduces the need to travel, which will support sustainability within the community."

Dubai Police opened the first Smart Police Station in 2017, in line with its Smart Plan to provide completely virtual access for the public to police services by 2030.

Tilal Al Ghaf is Majid Al Futtaim's new flagship mixed-use community in Dubai that will be home to more than 20,000 residents once complete. The community spans over three million square metres at the intersection of Hessa Street and Sheikh Zayed Bin Hamdan Al Nahyan Street. The phased project will include more than 6,500 freehold homes, ranging from apartments, townhouses and bungalows, through to substantial luxury villas. ■

KEY TAKEAWAYS

- Dubai Police opened the first Smart Police Station in 2017 in line with its Smart Plan to provide completely virtual access for the public.
- The Smart Police Station is in line with the community's 360-degree plan to promote happiness and public safety by using smart technology.
- Offering services locally, close to people's homes, also reduces the need to travel, which will support sustainability within the community.
- Smart police stations will offer services including 27 criminal, traffic, and community services as well as 33 allied services that will operate without human intervention.

Oman Arab Bank invests in Trend Micro to secure digital transformation into cloud

Trend Micro, a global vendor in cybersecurity solutions, announced that Oman Arab Bank, has selected Trend Micro to secure its digital universe. In their next step towards endpoint segmentation on the network, Oman Arab Bank has selected Trend Micro for its DR security because they wanted to have that same comfort level, and ensure best security practices.

Oman Arab Bank faces stealthy targeted attacks, custom designed to penetrate standard defences, and poised to monetise intellectual property and customer information, or to encrypt essential data for ransom. Oman Arab Bank's evolving IT infrastructure needed an instinctive security solution that was forward-looking, easily scalable, and capable of meeting the constant security demands.

Trend Micro Deep Security was enlisted for datacentre server protection. The solution delivers security capabilities for physical, virtual, and cloud servers in a single integrated platform. Its single dashboard allows continuous monitoring of multiple controls across physical, virtual, and cloud environments. And, centralised management with vulnerability shielding abilities saved Oman Arab Bank considerable time and resources.

For Oman Arab Bank, Tipping Point, has been instrumental in getting signatures on a daily basis. This solution is dynamic enough to catch those vulnerabilities and the solution itself works on an online module the GOI interface allows for easy to use.

Trend Micro Integrated DLP helped the bank minimises the complexity and cost of data security by integrating DLP functionality directly into the Trend Micro solutions and management consoles. With a lightweight plug-in, providing increased visibility and control of sensitive data, while preventing data loss via USB, email, SaaS applications, web, mobile devices, and cloud storage.

Fabio Picoli, Regional Director GCC, Trend Micro; Rashad Al-Musafir, Acting CEO, Oman Arab Bank; Mustafa Surour, Oman Arab Bank.

The DLP plug-in required no extra hardware or software, and it leverages built-in regional and industry-specific templates to simplify deployment. Integrated DLP allows Oman Arab Bank deploy data security for a fraction of the cost and time of traditional enterprise DLP solutions.

Trend Micro Deep Discovery, Advanced Threat Protection gives the power to detect, analyse, and respond to today's stealthy ransomware, its variants, including WannaCry, and targeted attacks in real time.

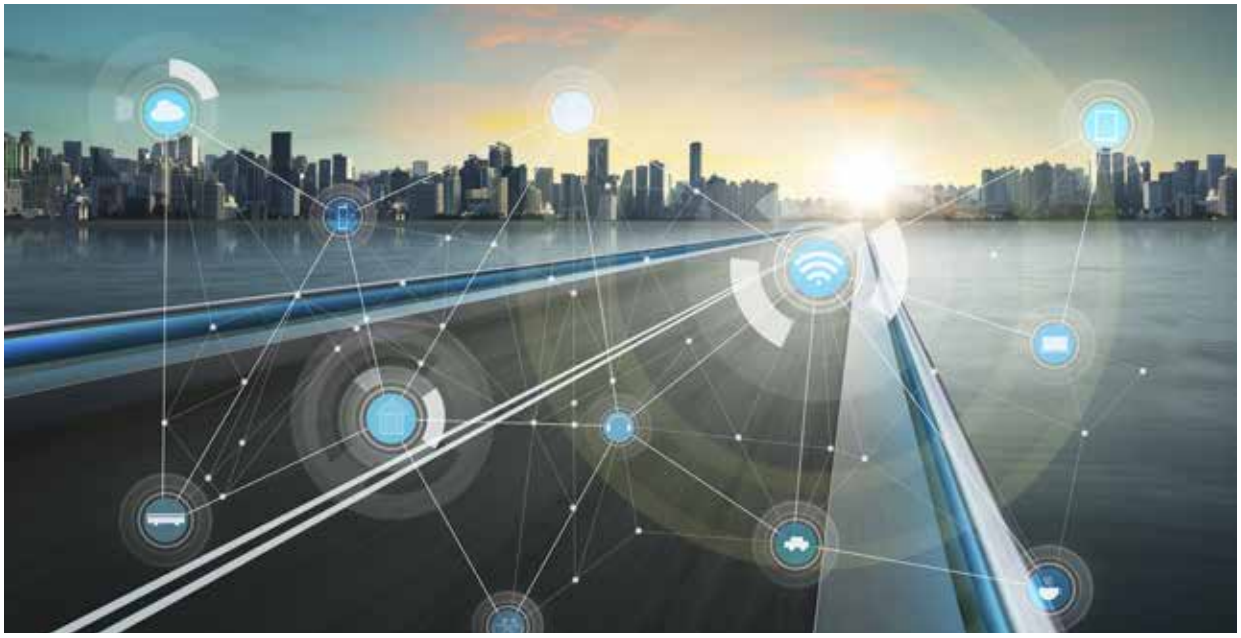
Established in 1984, Oman Arab Bank SAOC is one of the largest banks in the Sultanate of Oman. Currently Oman Arab Bank operates more than 65 branches and representative offices, and over 148 ATMs across the Sultanate.

"Investing in the best security for our IT infrastructure is of supreme important to us, as we continue to expand our business. We needed a security solution that was flexible enough to integrate into our existing landscape, and had the ability to help us evolve, whilst protecting our digital platforms. In Trend Micro we have found the ideal security partner," commented Mustafa Surour, Oman Arab Bank. ■

KEY TAKEAWAYS

- Trend Micro Deep Security was enlisted for datacentre server protection.
- The solution delivers security capabilities for physical, virtual, and cloud servers in a single integrated platform.
- Its dashboard allows continuous monitoring of multiple controls across physical, virtual, and cloud environments.

Consumerisation of IT driving IoT adoption in Saudi Arabia, UAE, Linksys survey



Linksys, announced that there is rapid adoption of IoT in the Middle East with a growing number of people investing in smart devices for their home, according to latest study by Linksys on consumer Wi-Fi usage trends.

The possibilities of IoT in the home are endless, from smart lighting and thermostats to smart fridges to machine learning devices. Linksys' study shows there is growing use of voice assistants and TV signals that are primarily Internet based.

SMART TVS

According to the Linksys study, 85.4% of respondents from the Middle East own at least one smart TV, out of which 27.9% respondents own multiple smart TVs. UAE ranks above Saudi Arabia in the adoption of smart TVs, with 86.6% and 84.2% respondents respectively.

Watching TV through the Internet is very popular in the Middle East, with Internet-based entertainment being the primary source of TV for 22.3% of respondents. This is widely seen in the UAE, among 26.8% of respondents, and 17.8% seen in Saudi Arabia.

Subscribing to TV services is still big in the Middle East and the study highlights about 25.5% of Middle East respondents using their smart TVs for subscription-based TV services. Of this figure, 52.1% use it to download TV series and movies, and 31.4% use it to live-stream sport events.

VOICE ASSISTANTS

The use of chatbots and virtual assistants, commonly called voice assistants, is rapidly increasing. The use of voice assistants such as Amazon Echo, Amazon Alexa, and Google Home is on the rise, with 35.7% ownership amongst respondents.

Other smart devices that have reached the 40% adoption barrier include connected security cameras and smart lighting, with 39.3% and 39.6% of Middle East respondents owning such devices respectively. While the use of smart doorbells is very popular – they are owned by almost half of the Middle East respondents 46.5% –thermostats by Nest and Netatmo lag behind, with only 24.6% of respondents owning such devices.

NUMBERS BY COUNTRY:

UAE

- Most likely 24% of all to be classified as smart home adopters
- Most likely of all to own a smart or connected TV 87%, and smart plugs 43%
- Most likely of all to consider purchasing a smart or connected TV 88%, and smart plugs 64%

SAUDI ARABIA

- Most likely 38% of all to be classified as extreme smart home adopters
- Most likely of all to own smart doorbells 48%, smart lighting 42%, smart switches 41%, connected security cameras 40%, voice assistants 38%, and smart thermostats 27%
- Most likely of all to consider purchasing smart lighting 68%, connected security cameras 67%, smart doorbells 63%, smart switches 63%, voice assistants 62%, and smart thermostats 47%

Amanulla Khan, Managing Director Linksys Middle East, Turkey and Africa.

Living in the digital age, the Internet is increasing a part of our daily lives and a new normal for all. Linksys' study forecasts that 58.5% of respondents who do not own any smart home devices are keen to adopt IoT in their homes, with UAE at 55% and Saudi Arabia at 62%. Adoption of smart lighting was higher, at 58%, and 52% of respondents are considering investing in this by 2020. The Middle East will see a steady adoption of voice assistants such as Amazon Echo and Google Home, with 28.5% of respondents considering such a purchase by 2019.

"The number of people using smart devices in the home is increasing rapidly, which means there is also a growing need to upgrade to bigger, faster home Wi-Fi systems," says Amanulla Khan, Managing Director Linksys Middle East, Turkey and Africa. "People may not realise that even if they only stream Netflix on a smart TV, it affects the overall Wi-Fi experience for others in the household by using bandwith."

Khan explains: "While we are now talking smart lighting and voice assistants, in the next couple of years we will move to even smarter connected devices in the home driven by Artificial Intelligence and machine learning. Solutions include Phyn, a smart water management system that protects your home from leaks by learning from your usage, and Whirlpool's smart kitchen range, which automatically preheats the oven and cooks dishes based on recipes.

These innovations will accelerate the number of IoT devices in the home and also the need for up-to-speed Wi-Fi. Whoever wants a smart home needs to be smart and futureproof his or her home network too."

Vanson Bourne conducted this research on behalf of Linksys part of Belkin International. The results are based on a web-based survey of 8,000 consumers. Respondents were interviewed in May and June 2018; they came from the UK 2,000, the Netherlands 2,000, Germany 2,000, France 1,000, the United Arab Emirates 500 and Kingdom Saudi Arabia 500.

In order to qualify for the survey, respondents needed to meet the following screening criteria:

- They had to be between 18 and 64 years old
- They had to have some form of decision-making responsibility in their household for purchasing new technology
- They had to use either a Wi-Fi router or a Wi-Fi router or modem combo device at home ■

TRANSFORMING THE WORKPLACE NO LONGER A CHOICE

Digitally transforming the workplace is no longer a choice for organisations and increasingly will be a key factor for future employee productivity and retention, indicates a global Aruba HPE survey.

Today's business world is increasingly being driven by digitally savvy, digitally demanding employees at all levels, called Digital Revolutionaries. The expectation is that employers will not just provide computing and communications tools and a dumb physical workspace, but a digitally-powered workplace that is increasingly smart, interactive, personalised and automated.

Workplace technology is no longer simply a plug-in enablement tool to help people do their work; it is a defining set of adaptive and interactive experiences that help shape the identity of a company's culture.

Companies need to embrace this new reality, not just because it is what their current and future employees want, but because there are advantages in doing so. As employers battle to recruit and retain the best talent, technology will increasingly become a core area of competitive advantage.

Today's workforce is not just driving consumerisation of IT, but also accelerating consumerisation of the workplace. These changing employee behaviors and expectations are shaping the way organisations think about the role of technology in the workplace.

More digitally-driven workplaces not only foster productivity, but employee wellbeing, motivation and job satisfaction. The organisations that capitalise on implementing a digitally-enabled workplace will gain a competitive edge. The advantages of deploying new workplace technology go beyond helping employees finish tasks quicker, but also make the process more collaborative and enjoyable.

There is a need for companies to empower their IT leaders with the budget and authority to invest in new technologies, develop cyber awareness and best practices, and provide employees with the workplace and tools that they increasingly demand.

The companies that thrive as digital workplaces will be those that start to see technology less as a series of tools and more as fundamental ambient infrastructure. And to do that, they have to start seeing the role and purpose of their IT departments in a new light too.

At the same time, companies must not lose sight of the security threats inherent in being a more connected organisation. The relatively lax attitude of employees towards cyber security is exposed by surveys, presenting one of the most pressing challenges. It suggests that people will not always act in accordance with their level of knowledge about cyber threats, and that more advanced behavioral security tools may be required.

The goal for every organisation must be to maximise productivity without compromising security in any way. This requires inter-group cooperation throughout IT, and greater focus on end-user experiences as well as system capabilities.

A total of 7,000 employees were interviewed in April and May 2018. The respondents were from organisations of all sizes, across both public and private sectors, but with a focus on the industrial, government, retail, healthcare, education, finance, and IT, technology, telecommunications sectors.

Interviews were conducted both online and via telephone using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Respondents were interviewed in the UK, Germany, France, Netherlands, Spain, UAE, US, Singapore, Japan, Australia, India, Brazil, Mexico, China and South Korea.

Two groups, Revolutionary and Laggard, were identified in the study by those that reported having a

completely digital workplace, where new technologies are in widespread use throughout the organisation, against those who said technology was in limited use or not used at all.

Aruba's findings suggest that the problem is as much about human failures as it is digital workplace design. The key trends appear below.

THE DIGITAL WORKPLACE

Workplace technology is no longer just about the tools that a company provides, but the entire working environment it creates. Organisations and workplaces that fail to get ahead of the curve on the new generation of workplace technologies will limit employee results and lose their competitive advantage.

As organisations increasingly communicate and do business through digital channels, the nature of work is diversifying. Today's digital workplace is moving beyond a traditional office environment with technology bolted on, to one in which the entire infrastructure and physical space are designed around, and optimised through, digital tools.

People are looking for a digitally-powered working environment that makes everything – from controlling office climate to booking a meeting room – more efficient. As ever more advanced consumer technologies, such as home automation products, become a feature of most employees' personal lives, they will expect the same benefits in their place of work.

> Workplace technology has the opportunity to be the leading force for wellbeing at work.

Aruba's study revealed not only high adoption of standard technologies, from Wi-Fi supplied by 82% of organisations surveyed to cyber security 67% and cloud applications 43%, but traction with a new generation of technologies.

Blurring the lines between facilities- and IT- managed functions, these IoT-driven technologies automate temperature controls and lighting 24%, voice-activated and wireless conference room AV technology 23%, and bespoke corporate mobile apps 23% offering location-based information.

The consumerisation of technology is reflected by a clear appetite from employees for a workplace that is digital by default. Almost two-thirds

The companies that thrive as digital workplaces will be those that start to see technology less as a series of tools and more as fundamental ambient infrastructure.

of employees in Aruba's study 64% said that they thought their organisation risked falling behind if new workplace technology wasn't integrated.

In addition, 71% said they think the workplace of the future should be fully automated, with 72% stating that the workplace should become a completely interactive environment that automatically updates and adjusts itself, while 61% called for virtual and augmented reality to play a stronger role.

ADOPTERS AND LAGGARDS

As workplace technology becomes more prevalent, the modern workplace is dividing into those who are seizing the benefits of digital technologies and those who are falling behind. Attitudes toward technology in the workplace and its adoption vary among employees and across different organisations.

In Aruba's study, they identified two distinct groups within today's workforce: The Digital Revolutionaries, employees that work in fully-enabled digital workplaces where new workplace technologies are in widespread use; and the Digital Laggards, employees who reported their working environments lack digital tools.

Workplace technology is often associated with efficiency and productivity, but that is just one level of benefits unlocked by implementing a digital workplace. Aruba discovered that there are significant personal satisfaction and wellbeing advantages for Digital Revolutionaries as a result of working in more digitally-enabled workplaces.

When implemented correctly, Aruba's research reveals the significant dividend that well-designed and well-implemented technology can deliver for today's companies, by not only helping people to do their jobs better, but to be happier and more fulfilled at work.

Technology does not have to limit or undermine the role of people; in fact, it can support and enhance it. Recent advances in technology provide a catalyst for organisations to jump-start a more productive relationship between people and technology in the workplace and elsewhere.

Workplace technology has the opportunity to be the leading force for wellbeing at work. The study found that 80% of all workers say personal wellbeing and job satisfaction is important to them; addressing this need should already be one of the most pressing concerns for any organisation.

Given the premium that most employers now place on employee wellbeing and job satisfaction in a highly competitive labor market, the need to invest in creating the connected, digitally-enabled workplaces that can enable those things becomes essential.

AUTOMATING THE WORKPLACE

Automation, enhanced with machine learning, has the opportunity to significantly improve workplace productivity and enable employees to expand into more strategic roles. Aruba's research found that there was almost a unanimous belief among all employees 93%, both Revolutionaries and Laggards, that increased use of digital technology will lead to improvements in the workplace.

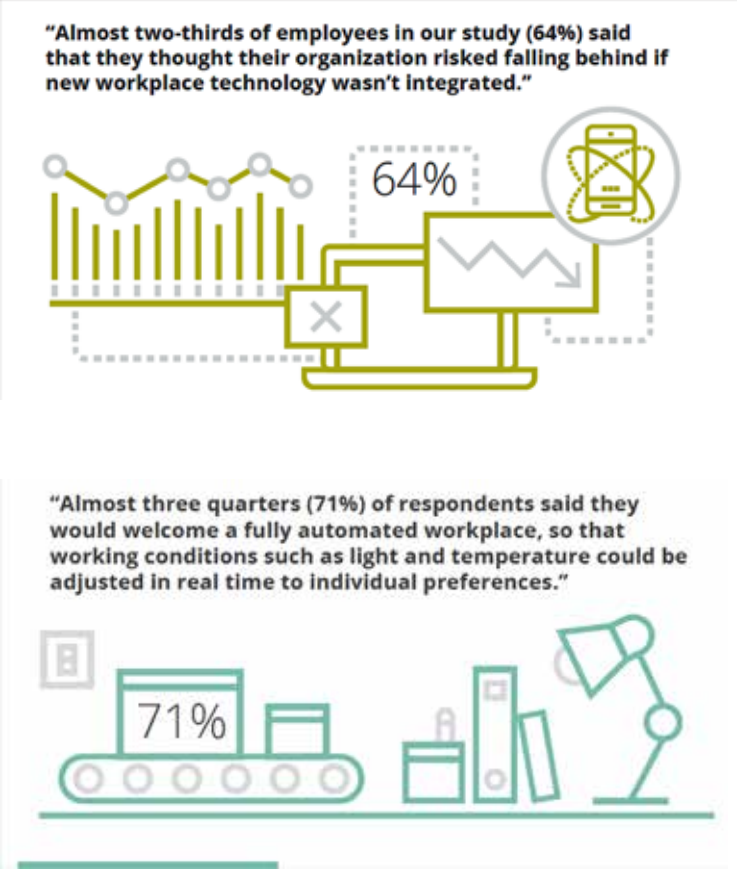
A large number of respondents believe that the future workplace will be more efficient 56% and more collaborative 52% and create a more appealing work environment 47%, while a majority 57% said they would be happy to share more personal data in return

for more personalised tools and experiences.

This general optimism towards technology and the workplace it can create extends to the topic of automation. Almost three quarters 71% of respondents said they would welcome a fully automated workplace, so that working conditions such as light and temperature could be adjusted in real time to individual preferences.

Similarly, 72% thought all office equipment such as the height of desks should be automatically adjustable, and 71% say that biometric data should replace passwords. Considering the repetitive, uninteresting, manual or semi-automated tasks in many of today's organisational workflows, it is not difficult to see why Digital Revolutionaries envision automation as an opportunity to learn new skills and move into more strategic roles.

Automation can also play a significant role in balancing the need for productive employee experiences and risk-taking, by proactively combatting unknown security threats as they appear. Approaches such as User and Entity Behavior Analytics can scan continuously for threats or risks on an individual profile basis, detecting anomalies in the network and taking preventative action before the risk spreads, and before human IT teams become aware.



SECURING THE WORKPLACE

A more connected workplace is inherently more vulnerable to cyber- attacks, a risk that is compounded by the behavior of employees. Although the digital workplace brings clear benefits to both companies and their employees, it also introduces new challenges. A more connected organisation that runs on digital platforms and applications is also more open to security breaches.

As companies invest in greater digital and connected physical infrastructures, they must also do more to ensure compliance around information security and data privacy. Employers need to understand the mindset of the employees who are driving change towards more technological workplaces.

Aruba's research found that the approach of employees can be problematic for employers who are looking to limit their cyber security liability. These behaviors occurred despite the fact that 92% of employees said they are aware of the potential impact of a company data breach, while 77% said they consider cyber security to be very or extremely important.

The gap between thought and action on cyber issues becomes even more apparent when you consider that just 53% said they use the cyber security software provided to them by their employer.

Given the significant cost that comes with any kind of cyber security breach, companies need to address the problem of employees who are lax in their everyday security behavior than their stated attitudes would suggest.

It is not enough for organisations to invest in secure networks and cyber software; they also need to acknowledge the risks posed by human error, and to understand the irony that it may be the more digitally inclined employee who poses a greater risk than the one who knows and cares less about the cyber threat. ■

Excerpted from the Aruba HPE report: The Right Technologies Unlock the Potential of the Digital Workplace.

HOW WORKPLACE ROLES AND PROCESSES ARE TRANSFORMING

Workplace job roles, asset usage, processes, are all being transformed by digital technologies according to Mahmoud AlYahya at Xerox, Osama AlHaj-Issa at HPE Aruba and Andy Brocklehurst at Cisco.

By Arun Shankar

While cloud, mobility, social collaboration technologies are boosting the emergence of the digital workplace, the key underlying pain point that continues forward is - meeting misery. The reason for this according to Andy Brocklehurst, Collaboration leader for Cisco in EMEAR, is that, "The way in which people work is not intuitive. This creates a challenge. It is complex, so they go and seek another way in which to do things, they go and add another application."

Since people work in ways that best suit them, they keep adopting new ways and new solutions to do things. In essence, what people want to do in the workplace can be captured by one, two, or three kinds of applications, built around workflow and processes, and this represents a simplification of sorts.

"What is the fundamental issue that business is facing and it is meeting misery. Meetings start late, technical issues, no thread or common flow to it, and it stifles decision making," explains Brocklehurst. As organisations implement new systems like virtual meeting rooms, to boost remote working and home working, the best way to make it a success is to make it as simple as possible to use.

Workers will attempt to get to know an application one to two times before they give up. "The best remote control is no control only voice, where the meeting is already ready, and you take the meeting with you," says Brocklehurst.

The growing volumes of data generated within businesses either unstructured or structured data is creating a challenge of management. One such job role to manage data is the analytics specialist. The growing proliferation of cloud applications and platforms within a digital organisation is creating a role of a policy specialist, also referred to as cloud access security broker.

This is someone who decides who in the company can access which cloud resources. This is a new kind of job role generated by the multi-cloud environment that organisations are now living in.

Another challenge for the workplace is the huge difference in speeds between the ability to access or reach the right information internally versus the speed at which technology is progressing externally. In order to boost internal collaboration around information sharing within an organisation, it is imperative to reduce the hierarchal structure of an organisation, in other words flatten the structure.

Using the power of teams built on specialist knowledge rather than on other norms of organisational position, helps to boost creative thinking and innovation. Such types of team structures reduce go to market times, encourage creative and out of the box thinking, and help workers to think about: How will I not make myself a bottleneck and sharing is caring.

Brocklehurst points out, by default organisations are built using a command and control structure, and need to move to a matrix type structure.

EARLY ADOPTERS

According to Osama AlHaj-Issa, Regional Channel Director, Middle East, Turkey and Africa at HPE Aruba, Aruba is a core component of any regional digital transformation initiative, and is usually a preferred platform for early adopters. "If you look at different customers that we deal with, some of them are more advanced on the digital transformation journey and some are more conservative. We are with the

(Left to right) Mahmoud AlYahya, Head of Production Technology Business, Xerox Middle East Operations; Osama AlHaj-Issa, Regional Channel Director, Middle East, Turkey and Africa at HPE Aruba; Andy Brocklehurst, Collaboration leader, Cisco EMEAR.

more advanced pioneers than with the conservatives. Our solutions are playing in an area of future strategy and if you look at some of the biggest organisations in the region, our customers are pioneering in digital transformation."

For the early adopters of transformation in the region, transforming the workplace means a lot for them. Such organisations want to have an open environment with smart meeting rooms, mobile workers, mobile printing, easily locatable workers. Since digital transformation also involves changing the people and processes of an organisation, the way people think and plan, not all organisations are ready for such changes.

Cloud and security are very important components of this journey. "These are objectives of organisations that are going through the journey of digital transformation and we are making this happen for them," says AlHaj-Issa.

AlHaj-Issa explains that Aruba is usually not more than 5% to 10% of an organisation's digital strategy. "But these are very important, and you cannot do a transformation plan without having the right components of security, mobility, workplace, machine learning, intelligent edge. These are all part of a digital transformation, but it takes processes, people, and applications."

PAPERLESS OFFICE

Organisations that begin their digital transformation journey need to start by taking a hard look at where they are today, their processes now and in the future, before they even begin this journey. As an end to end vendor, Xerox enables this with its customers by starting with an assessment, designing the solution, implementing the solution, and then managing the solution.

Says Mahmoud AlYahya, Head of Production Technology Business, Xerox Middle East Operations, "A lot of companies unfortunately miss out that step. They want to jump into digitisation before understanding where they are right now and what are the opportunities that they have to digitise. Going through the step of assessment and assessing what are the areas and processes that could be transformed from document intense area to paperless areas is absolutely key. That is something that we help with massively in terms of understanding their processes their workflows."

Is this an established professional practice within Xerox? "It is not a formal process, it is the way business is done in Xerox, and it is now like a common practice. We all speak the same language in the organisation," explains AlYahya.

For Xerox, digital transformation in the workplace is a four-step process. It starts with organisational assessment, followed by design of a solution, then implementation, and finally management of the solution. Xerox follows the same practice for its managed print services and for any other customer facing services as well.

Xerox's vision for the digital workplace is to develop solutions that makes life easier for its workers, while enabling businesses to reduce cost and increase efficiency. Another part of the vision is to recognise a document in all its digital formats as a normal standard. To assist remote working and work from home, another part of the Xerox vision is mobile printing.

"One of the things we are enabling our clients to do is to be more mobile. Being able to print from anywhere, anytime using our solutions is one of the keys. Making work simple sounds like a very bold headline, but it is a bit more challenging than it sounds," reflects AlYahya. ■

HOW TECHNOLOGY IS REDEFINING THE MEANING OF HUMAN BEING

Recent developments are triggering a wave of interest in how human beings can be rebuilt presenting Neil Harbisson, Amal Graafstra, and Viktoria Modesta.

From tribal piercings to the figurative tattoos of prehistory, humans have been modifying their bodies for millennia. But advances in prosthetics, implants and bioengineering are allowing us to alter ourselves in new and unprecedented ways not only to beautify or overcome deficiencies, but to enhance and exceed our current capabilities.

All three defy categorisation and eschew the widely-used term body-hacker. But whatever the title: bio-hackers, neuro-hackers, futurists or otherwise, this ever-growing community is challenging the very notion of what it means to be human.

NEIL HARBISSON

Cyborg and designer of artificial senses

Neil Harbisson is the world's first legally recognised cyborg. He has an antenna implanted in his skull which transposes colors into audible vibrations. Since 2010, Harbisson has run Cyborg Foundation, an online platform dedicated to researching and developing artificial senses, promoting cyborg art and defending cyborg rights.

I define what I do as neuro-hacking rather than biohacking or bodyhacking because my ultimate aim is to change the mind. But, in order to do so, I have to change my body.

During my studies at art college, I became interested in sensing things that I could not otherwise sense, which meant color, I was diagnosed with achromatopsia, or complete color-blindness, as a child.

Using technology, I co-created an antenna, that I have implanted to this day which allows me to perceive colors. The antenna senses color frequencies, which reach me as different audible vibrations. It was chaotic at first because, as an artificial sense, it took longer for my brain to process. I could not tell the colors apart, and it took me many months and a lot of memorisation to actually understand and name the colors.

But slowly, after many months, the process became automatic. My brain began to transform sensory input into perception. My sense of what is beautiful has changed too. Now, experiences that I normally would not have found stimulating like walking down a supermarket aisle are. In an aisle, there are lots of different vibrations of colors that, to me, are very flattering.

This project is artistic in intent. Because art has no rules, laws or boundaries, I feel like there is a lot of freedom when you contextualise a project in art. It allows me to think freely about what I want and how I want it. In this case, I am not trying to solve a problem, I am trying to explore alternate realities and solve my curiosity towards color.

The purpose of the Cyborg Foundation, which I co-founded in 2010, is to create senses and organs that are not traditionally human. Whereas the medical

I define what I do as neuro-hacking rather than biohacking or bodyhacking because my ultimate aim is to change the mind. But, in order to do so, I have to change my body.

field usually focuses on creating recreating pre-existing senses and body parts, the foundation focuses on innovating new ones. For example, my fellow co-founder, Moon Ribas, has implanted seismic sensors in her feet so that whenever there is an earthquake in the world or a moonquake on the Moon, she feels it in her body.

Another artist, Manel Muñoz, has biometric ears that can perceive changes in weather. And then there is Kai Landre, who is developing a sensor that allows him to feel cosmic rays. By adding these new senses, we can reveal realities that already exist in nature, but that the human body or brain cannot yet perceive. The teams working on these projects all come from different backgrounds. There are artists, designers, doctors, computer scientists, multiple fields collaborating to create new senses.

Most people think these creations are not necessary for us to function. That is because for thousands of years we, as a species, have been changing the planet rather than our bodies in order to survive. But I think that is the wrong approach.

People might say they do not need more senses, but at night they turn on the lights. But if humans actually had night vision, we would not have to create artificial light. Instead of using air conditioning when it is hot, or heaters when it is cold, could not we just adjust the temperature of our bodies? We should look to designing and changing ourselves.

AMAL GRAAFSTRA

Invisible bio-hacker

Since 2005, Amal Graafstra has had multiple chips, RFID tags and even a magnet implanted into his hands, arms and upper body. He is the founder of Dangerous Things, a bio-hacking firm, and VivoKey, a digital identity platform aiming to make secure implants accessible to everyday consumers.

I have always been fascinated by technology. When I started doing IT for a medical clinic, I began to see the healthcare system's inner workings how doctors are just mechanics, and in terms of how we diagnose, treat and fix it, the body is just a machine.

This experience removed the mystique of medicine. It also eroded the idea that the skin was some sort of sacred barrier. Even though chip implants are safer than ear piercings, people tend to have an – ick - reaction to them, while tooth fillings and breast implants are totally acceptable. The difference has nothing to do with the device or implant procedure, it is applications that drive adoption.

For thousands of years we as a species have been changing the planet rather than our bodies in order to survive.

Bio-hacking is an umbrella term meaning anything from DNA hacking to bionics to simple lifestyle changes. The term hack has a negative connotation, but it is powerful when you understand that it really means an unconventional approach or solution. All good, efficient hacks become mundane they are no longer a hack, they are just how things are done.

If an implant is designed well in other words, it is frictionless, management-less and you give it as much thought as you do your kidneys.in other words, none at all, then it is part of you. It is not a tool that you have picked up like a smartphone, it is actually changing your capabilities as a human. That is philosophically, fundamentally and, as I am sure we are destined to see, legally different from any tool.

When we are literally able to digitally expand our minds we will begin transcending the human condition.

Fear of technology is rampant. The fact that my augmentations are internal they are not visible definitely helps in terms of my daily interactions. I do not typically have to worry about stigma or prejudice from the un-augmented. The typical visual cues that would normally betray the fact I am different are just not there. Most bio-hackers can choose to disclose their augmentations or decide to keep them private.

I think a synaptic brain-computer interface is kind of the holy grail. Imagine we had synthetic synapses that could dock and exchange neurotransmitter molecules with organic synapses. We could pay a digital neural service to fire up a hundred billion extra neurons to think through problems, then shut them down once we're done. It would intellectually free us, as a species, from the confines of biology.

The constant struggle to enhance our capabilities is the very definition of humanity. When we are literally able to digitally expand our minds, we will begin transcending the human condition.

VIKTORIA MODESTA

Bionic pop artist
Futurist

Viktoria Modesta is a bionic artist whose work explores the intersection of art, science, music, technology and design. She is a fellow at MIT Media Lab and has performed at museums, festivals, fashion weeks and the London Paralympic Games. Her work, which includes the viral hit Prototype, challenges our notions of ability and identity.

When I underwent a voluntary leg amputation at the age of 20, I was shocked to learn that doctors felt it was more acceptable for me to be in constant pain and for my whole body to suffer, than it was to have my damaged leg removed and replaced with an artificial one. That process highlighted an unhealthy obsession with how we value the biological body.

We identify with our bodies as what defines who we are. But going through the decision to amputate gave me a deeper sense of self. It made me curious about how we can transcend this rigid view, to approach the body in a creative way and take more care with the things we create.

My main motivation has always been about raising the bar on standards and expectations, which I have always found offensively low for women, especially those with disabilities. As a kid, adults looked at me as if I was destined for nothing, which I found really puzzling. I felt strong and imaginative, and I never identified with that image of being incapable.

My view of prosthetics has undergone an evolution. At one point, I saw it as a form of salvation, and a form of feminism, to be able to take charge of my body and choose what my leg looks like. After my first few prosthetics, it became all about how they can be an art form and a statement of expression and fashion.

Most of the artificial art limbs I own result from a collaboration with the Alternative Limb Project. Crystal, a prosthetic encrusted with Swarovski crystals, was created for the Paralympic Games' closing ceremony.

Spike, a black lacquered, geometric prosthetic; and Light which contains LEDs, both featured in my viral music video Prototype. By working with tech-facing artists and designers, I am now developing many conceptual projects fusing prosthetics, fashion, musical instruments and emerging technologies.

Nowadays it seems that the prosthetics space is changing from a basic medical industry to a consumer one, and it is being infiltrated by designers and engineers from other fields.

Medical assistive devices are becoming more like any other aesthetic and technological features found in our lives. From the things I have seen in development, it may be increasingly common to have internal sensors that can project data from inside the body, uniting all forms of tech wearables.

Whether it is clothing that monitors your health, bionic limbs controlled by the power of thought, or robotic attire that responds to the environment, we are heading for a neuro-connected, expressive future where technology will be an intimate extension of our selves.

We are all interfacing with technology. It might be for different purposes like medicine, lifestyle, art or simply a manifesto, but this segregation is just one of those human illusions.

It does not matter whether you identify as a cyborg or transhumanist, or if you are an amputee, gamer, or older person kitted out with medical tech inside your body. Technologically advanced human bodies are the future, and the future is already here. For me, fusing my body with technology feels like a philosophical exploration of humanity. It is art. ■

KEY TAKEAWAY

THE PURPOSE OF THE CYBORG FOUNDATION IS TO CREATE SENSES AND ORGANS THAT ARE NOT TRADITIONALLY HUMAN.

Content courtesy CNN Style. Photography by Lars Norgaard. Images courtesy of Neil Harbisson.

IS TRANSFORMATION BOOSTING THE VALUATION OF PRIVATE EQUITY

A survey by PwC throws up pros and cons in a real-life manner on whether digital transformation is boosting the valuation of private equity in the region.

As a region, the Middle East has embraced the digital revolution. Now more than ever before, PwC are seeing an increased comfort in going digital unsurprisingly given the region's young demographics and good quality infrastructure. Certainly, at a consumer level there is a high level of technology adoption: Bahrain, Kuwait and the UAE are among the most penetrated countries in the world with a mobile subscriber rate of over 90%.

Although, with that said, most Middle Eastern companies are still in the process of adoption stage in comparison to the West when it comes to digitisation.

What do we mean by digitisation? We mean transforming analogue and manual processes, functions and tasks into digital throughout a company. Digitisation encompasses digitising product and service offerings as well as expanding the business model and customer access by offering disruptive digital solutions.

At a corporate level, digital has disrupted almost every industry sector, and will continue to do so. As the digital landscape evolves, there is a pressing need for private equity houses in the Middle East to keep up with these rapid changes, or risk being left behind. The private equity investment horizon means that the digital transformation of a portfolio company is being assessed and planned even before private equity houses even think about investing in any new company.

Digitising a company does not need to be expensive, and digital can create value throughout the private equity holding period: new customers can be found online; costs can be optimised through more efficient purchasing and operational management; cash flow can be improved and the wealth of data now being generated by connected devices and customers can inform everything from product design to customer interaction and marketing.

Private equity firms in Middle East have considered the extent to which they should increase their investment in digital beyond traditional domains.

THE SURVEY

PwC Middle East surveyed a number of leading private equity firms in the region to find out what digitisation means to them and how it is impacting their investment decisions. The survey focuses on the private equity life cycle from the time of investment, holding period right through to exit and highlights the maturity of digital developments facing the region.

At the initial investment stage, private equity houses usually focus on two main areas when they are thinking about going digital:

- PE houses identify and plan how the potential impact of digital will have on the companies they are investing in, whether this be the threat of disruptive competition or the opportunity for new sales and service provision
- PE houses assess the extent of digitisation within a company, and how digital can be used to optimise cost and revenues.

Such things can fundamentally change a company's business model, and therefore the digital investment of portfolio companies should be at the forefront of management and board thinking.

PwC survey shows that private equity houses believe that going digital is a necessity. It features heavily in the investment decision process and value creation plans of all the private equity firms surveyed in the Middle East region. Notably, 80% of private equity houses said that digitisation is critical for making their companies future ready.

These findings are even stronger than in Europe, where digitisation is more advanced. A comparable PwC Private Equity and Digital Transformation survey, led by European team, found that less than two-thirds 62% of private equity firms thought that digital could deliver sustainable value for a company, although it was considered the single most important trend influencing investment decisions.

Almost three quarters said that they are now focused on the level of maturity of a company's digitisation during the

due diligence stage of an acquisition. When PwC maps this to the recent deal activity happening in the region, they are seeing industries such as Financial Services, Healthcare, Retail and Consumer as investable sectors all focused on enhancing their digital footprint.

From the survey findings, it is clear that digitisation means different things to different private equity houses. Some see it as an enabler to maximise revenues within a fairly short timeframe. Others see it as a way to improve management reporting, with better- quality data feeding better informed decision making. There is a general consensus over the need for better information systems including real time information.

REAL LIFE SCENARIOS

That said, for all of the recognition of digital's importance, private equity companies are cautious about their initial investment decisions and they are unlikely to be early adopters of the latest technologies. Given capital constraints and holding periods, with typical investors looking to sell assets after 3-5 years, private equity houses will adopt a very pragmatic approach to digitisation.

Private equity houses will carefully consider the solutions to be rolled out, ensuring they have been tested before committing to them.

The risk and costs of testing a very innovative solution will probably exceed the expected return in their typical time horizon. Digitisation is not something

What do we mean by digitisation? Transforming analogue and manual processes, functions and tasks into digital throughout a company.

75%

OF PE HOUSES ARE NOW FOCUSED ON THE DIGITAL MATURITY OF A COMPANY AT DUE DILIGENCE STAGE OF THEIR ACQUISITION

that can simply be imposed by private equity investors.

Rather, digitally enhancing portfolio companies depends on the actions and attitudes of wider stakeholders including the Board and Management, and on how easy it is to change customers' mind set. Overall, the survey suggests that private equity houses recognise that they are at a crossroads here. They must balance the risks of adopting new technology against the opportunities it offers and the danger of failing to build the exit equity story.

There is also increasing awareness of how digital is disrupting the business model. For example, PwC are already seeing Procurement 4.0 and how digital innovation is disrupting the entire procurement value process. The market is seeing some innovative examples of how digital is rapidly transforming supply chain and logistics, such as, efficient inventory management and transport tracking systems.

Some 79% of respondents in the Middle East say that such production and procurement savings are some of the most important impacts of digitisation on portfolio companies. In fact, there is no single right way to embrace digital or to adopt new technologies: the extent of digitising portfolios must be based on the current needs of the company and on global industry standards.

Private equity firms need a strong management team on the ground who truly understand the specific companies' digital needs and the extent to which these technologies can be implemented. Private equity houses have also found ways to access global knowledge through experts and advisors.

Hiring external expertise allows them to manage the skills gap in their own management teams and at Board level in the region. They consider the digital agenda to be a Board discussion topic and the focus should often be given to Board members who have led such transformation projects either inside or outside of the region.

EXIT STRATEGIES

The digital revolution is further increasing the focus private equity houses should have on the exit phase before they invest. They must ask questions about how the investment industry will be disrupted and what that will mean for the asset.

Industries from retail to healthcare will be heavily impacted in the near future, so this needs to be a major consideration when looking to exit. That is all the truer for private equity houses looking to sell assets to international buyers, who will expect global standards when it comes to the assets' digital offering and capabilities.

Using digital to increase sales and performance will be seen as central to maximizing value by the time investors decide to exit. Therefore, developing a robust digital strategy that compliments the exit process will be key. 95% of respondents think that digital is important to future exits from their portfolios, and to the returns on investments that can be realised.

E-commerce remains relatively underdeveloped in the Middle East and reportedly accounts for just 2% of retail sales compared to over 17% in the UK. With such high mobile penetration in the region, it is reasonable to expect there will be rapid catch-up growth in this sector.

All of this suggests that digital markets will grow very fast with mobile platforms becoming increasingly important in areas such as healthcare, where apps such as Babylon are even using artificial intelligence AI to answer users' medical queries.

THE REGION IS ALREADY BEING HEAVILY DISRUPTED BY DIGITAL. SOME EXAMPLE INCLUDE:

FINANCIAL SERVICES (FINTECH)

RETAIL (E-COMMERCE)

HEALTHCARE (AI AND ROBOTICS)

FMCG (CUSTOMER DATA CAPTURE))

MANUFACTURING (BSB SUPPLY CHAIN))

79%

BELIEVE PRODUCTION AND PROCUREMENT SAVINGS WOULD BE THE MOST IMPORTANT IMPACTS OF DIGITISATION ON PORTFOLIO COMPANIES

KEY TAKEAWAYS

- Private equity companies are cautious about their initial investment decisions and unlikely to be early adopters of latest technologies.
- With capital constraints and holding periods private equity houses will adopt a very pragmatic approach to digitisation.
- The risk of testing a very innovative solution will probably exceed the expected return in their typical time horizon.
- Digitisation is not something that can simply be imposed by private equity investors.
- Survey suggests that private equity houses recognise they are at a crossroads, balancing risks of adopting new technology against opportunities.

FUTURE OUTLOOK

PwC findings suggest that companies in the Middle East have been cautious over exploiting the potential of such new technology – none of PwC respondents have actually implemented things like AI robotic surgery, for example, although it is interesting to some investors. There was no mention of online monitoring of patients, which has been used successfully in countries such as India and China. More broadly, areas such as AI and smart manufacturing seem to be further down the agenda.

Digital transformation is high on the agenda for Governments across the region, with many national programmes launched to improve and develop the countries' digital infrastructure and economy. In the UAE, PwC have seen the Smart Dubai initiative launch in early 2017 which sets out for the UAE Government to be 100% paperless by 2021. Saudi Arabia views digitisation as a key enabler for its Vision 2030 transformation programme.

Digitisation encompasses digitising product and service offerings as well as expanding the business model and customer access.

Investors are recognising that, as the infrastructure develops and companies join consumers in a rapidly evolving digital landscape, it will become increasingly central to company performance. This should also support the digitisation efforts of the region.

When PwC compare the Middle East landscape to that of Europe or the West, it is clear that all regions are at different stages of digital adoption. Our survey shows that private equity firms here in the Middle East have considered the extent to which they should increase their investment in digital beyond the traditional domains such as enterprise resource planning ERP systems.

The unique and vast opportunities that this presents in the region is exciting. The Middle East can tap into sector knowledge from across the globe, meaning private equity firms can benefit from best practice and lessons learned from the West. Being part of a growing economy means that there are fewer technologies already in place and less need to upgrade legacy systems. Many companies are starting with a blank canvas.

The digital revolution has changed the way products and services are consumed. As the market continues to adapt to consumer demand, private equity firms and portfolio companies must remain relevant by mirroring consumer behaviour.

Having a digital strategy is essential for future proofing a company that wants to retain market share and stay ahead of the competition. Those who are nimble will reap the benefits of the value to be created through digitisation. This mindset

must also be adopted by management teams who can no longer survive without integrating digital capabilities within their teams to complement their traditional skillsets. ■

Excerpted and adapted from PwC Report: Digitisation, The revolution transforming Private Equity by Erwan Colder, Private Equity Leader Middle East; Romil Radia, Middle East Valuations Leader; Maged EzzEldeen, Egypt Deals Leader; Ovais Chhotani, Middle East Deals Director; and Jad Barakat, Middle East Deals Director.

38TH **GITEX** TECHNOLOGY WEEK

14 - 18 OCTOBER 2018

DUBAI WORLD TRADE CENTRE

Experience Future Urbanism

WELCOME TO THE LARGEST TECHNOLOGY EVENT IN THE MIDDLE EAST, AFRICA & SOUTH ASIA

Big on numbers. Bigger on opportunities.

At the centre of the global tech revolution and the region's digital transformation, GITEX Technology Week brings together the most powerful innovations influencing the future – right from AI to Smart Cities to Blockchain.

4,700+ EXHIBITORS	**100,000+** VISITORS	**6,238** MEETINGS SET
80% EXHIBITORS SECURED OVER 2 BUSINESS DEALS	**16,000+** GOVT & CORP BUYERS	**9** VERTICAL CONFERENCES WITH 100+ HOURS OF CONTENT

FOLLOW US

#GITEX2018

CONTACT THE TEAM ON

+971 4 308 6566/6022/4090/6282/6077

gitexsales@dwtc.com

www.gitex.com

Organised by

مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

Co-located with

GITEX FUTURE STARS

HOW VULNERABLE ARE SCADA OPERATIONAL SYSTEMS IN THE GCC

Gulf Business Machines looks at the increasing vulnerability of operational technology systems and the role of artificial intelligence in the Gulf region.

According to 7th Edition of GBM's Annual Cybersecurity Study, conducted across UAE, Bahrain, Oman and Kuwait, 31% have already experienced attacks to their operational technology environments. The survey polled over 600 executives and IT professionals from a range of industries including IT, healthcare, education, oil and gas, hospitality, and many others.

According to Hani Nofal, Vice President, Intelligent Network Solutions, Security and Mobility, Gulf Business Machines, operational technology systems are being challenged because of the integration of SCADA systems with Internet of Things and the Internet.

HANI NOFAL
Vice President, Intelligent Network Solutions, Security and Mobility, Gulf Business Machines.

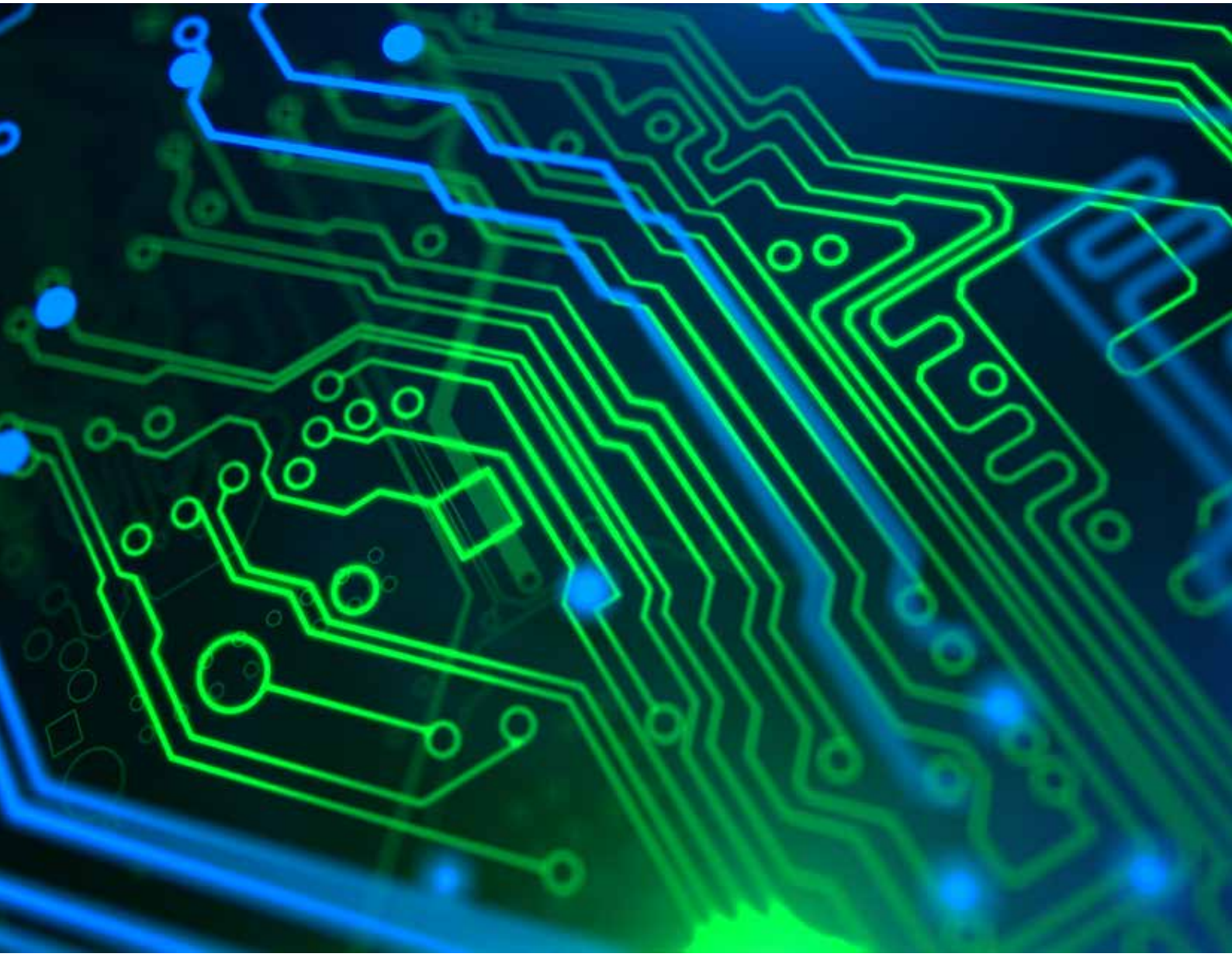
Industrial control systems are the central nerve system for all manufacturing, utilities, oil and gas plants. These are the systems which operate the plants input and output, all of which are designed to work seamlessly to achieve specific measured outputs.

Computer-based supervisory control and data acquisition systems have evolved over the past 40 years from standalone, compartmentalised operations into networked architectures that communicate across large distances. In addition, their implementations have migrated from custom hardware and software to standard hardware and software platforms. However, the security envelope has not evolved with the same pace as SCADA and ICS systems.

SCADA and ICS systems and applications were designed for high resilience but not with the view of cybersecurity. SCADA and critical infrastructure systems run on the same operating platform as corporate servers and desktops. Industrial control systems send data in the clear, without any encryption or authentication.

From a cyber perspective, SCADA systems look similar to business systems like firewalls, switches, Active Directory, file and print servers, Windows Servers and workstations. However, they often lack basic protection. There is near zero visibility in SCADA environments from a threat detection perspective.

31% of organisations have already experienced attacks to their operational technology environments. There is a shift in Gulf organisations that have started taking action by deploying security controls for



operational technology and developing a security strategy for prevention, detection and response.

A few organisations in fact are leading the way in setting up a security operations centre dedicated for SCADA infrastructure and applications isolated from the IT environment.

BLENDING AI AND HUMAN SKILLS

There has been a significant increase in the development and execution of artificial intelligence and machine learning technology over the past few years. We have always talked about how everyone should improve their skills with experience – practice makes perfect – and that is the fundamentals behind machine learning, computer learning and adapting through experience. This is why CISOs have been investigating how to use artificial intelligence to bolster their cybersecurity. Machines and technology can now be taught to teach themselves how to build models or recognise patterns and anomalies without human intervention.

Organisations can use the data from previous cyberattacks to detect and respond to newer and similar attacks their security may experience, while it can also be automated to simply watch over the

31%

HAVE ALREADY EXPERIENCED ATTACKS TO THEIR OPERATIONAL TECHNOLOGY ENVIRONMENTS

network traffic, learn what is normal and use the information gathered to flag any anomalies that it considers suspicious. Detection, response and prediction are driving factors behind an artificial intelligence-based adoption with Gulf organisations.

Organisations in the UAE, Bahrain, Oman and Kuwait have highlighted that a mix of artificial intelligence and human skills is the way forward to best utilise the functions of artificial intelligence or machine learning. There is an ongoing debate between cybersecurity experts on what path to take when considering the protection of their business and it appears the opinion is still split down the middle.

Organisations are now beginning to see the full benefits of utilising artificial intelligence within their cybersecurity practices as 62% of enterprises in the Gulf surveyed said they were likely to utilise artificial intelligence within 3 years, 40% of whom aim to accomplish this within a 1-2-year timespan.

While many organisations wonder if artificial intelligence will eat into the jobs aspect, it seems far-fetched to have the same effect on cyber security. Either artificial intelligence will help in bridging the gap in human skills or create a new skillset requirement which the new generation needs to be ready with. It is unlikely that the shortage of human skills in cybersecurity will fade in the next three years.

SECURITY OPERATIONS AND AI

Another, often overlooked, benefit of artificial intelligence is how much time it will free up for employees tasked with security. For the simpler attacks, the system could be programmed to deal with the situation without any guidance and instead only flag up the more extreme case to the security teams. Taking an assume breach mentality, artificial intelligence can also be programmed to attack or breach your own systems, as any hacker would to discover vulnerabilities, sending the findings to the security team, maybe even with recommendations, so it can be patched up before it is exploited for real.

CISOs want to enhance their security, improve their operations and protect their organisation's IT business and artificial intelligence is certainly gaining momentum in providing some much-needed protection against attackers. There are always discussions about artificial intelligence bringing forth mass redundancies, but artificial intelligence needs to be applied to complement the security team and its infrastructure not replace.

The aim of artificial intelligence is to eliminate human error. However, human is the heart of not just functioning security operations centre, but a successful one. The high volume of

SOC integrated with artificial intelligence allows analysts to not be overwhelmed by data and monitor a company's infrastructure.

WHAT DO YOU THINK IS THE DRIVING FACTOR BEHIND AN AI-BASED CYBERSECURITY TECHNOLOGY ADOPTION?

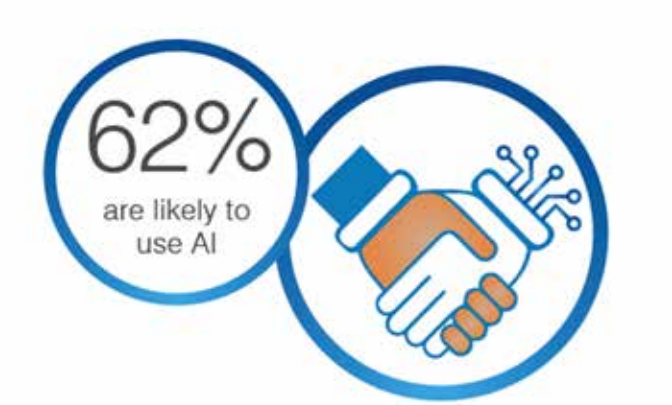
31%

OF ORGANISATIONS HAVE ALREADY EXPERIENCED ATTACKS TO THEIR OPERATIONAL TECHNOLOGY ENVIRONMENTS.

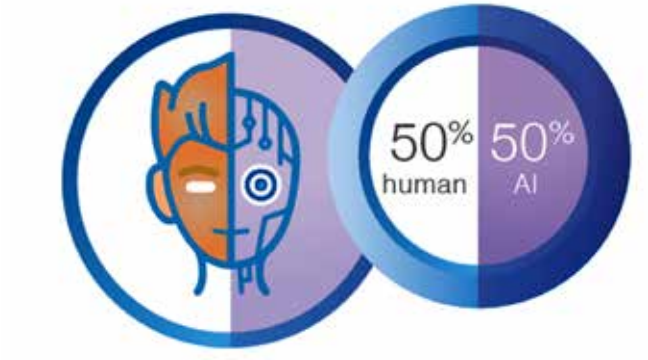
KEY TAKEAWAYS

- A few organisations are leading in setting up a SOC dedicated for SCADA isolated from the IT environment.
- SCADA and ICS systems and applications were designed for high resilience but not with the view of cybersecurity.
- There is near zero visibility in SCADA environments for threat detection.
- The aim of artificial intelligence is to eliminate human error.

HOW LIKELY ARE YOU TO UTILIZE ARTIFICIAL INTELLIGENCE IN SECURING YOUR ORGANIZATION?



WHAT WOULD BE THE MOST CRITICAL RESOURCE THAT COULD HELP YOUR ORGANIZATION PREDICT CYBERATTACKS?



data now being collected and stored by organisations and the sheer weight of attacks they face has made it difficult for one single solution to be the answer.

A security operations centre integrated with artificial intelligence can provide the best of both worlds, allowing a security operations centre analyst to not be overwhelmed by the constant stream of data and also consistently monitor a company's infrastructure, flagging any major security incident that requires human intervention.

For companies uncomfortable with putting the fate of their security in the hands of unmanned machines, it is important to note that artificial intelligence still needs human feedback in order to improve the quality of its decision making. The best solution is an integrated one.

What the survey has discovered is artificial intelligence is as important as human resources in predicting cyberattacks and it is expected that mentality would be repeated in all aspects of cybersecurity. The fact is artificial intelligence and security operations centre is the future of cybersecurity and organisations in the Gulf are quickly coming to the realisation this is the direction needed to fully protect their infrastructure for the ever-increasing threat of cyberattacks.

> Artificial intelligence is as important as human resources in predicting cyberattacks.

A security operations centre is a facility housing an information security team who monitor and analyse an organisation's security on an ongoing basis. By analysing and monitoring an organisation's network, server, data and endpoints 24x7, the security operations centre team can ensure the timely detection and response of any security incidents. ■

HOW ORGANISATIONS CAN USE GATEWAYS TO BRIDGE OT AND IT

Operational and information technology are different worlds and gateways help to bridge information from one to the other, explains Oliver Horn at Red Hat.

OLIVER HORN
Senior Solutions Architect – Alliances, Red Hat.

The Internet of Things, IoT will make operational technology, OT, the hardware and embedded software for monitoring and controlling physical devices, processes, and events – fit for the future. It has the potential to fundamentally transform almost every industry, whether production, energy supply and distribution, transport and haulage, or healthcare. The networked sensors, measuring devices, and actuators monitor and control the status of resources and machines.

Most IT companies still treat IT and OT as separate areas and develop, maintain, and use the two for different purposes:

- The CIO is responsible for general company applications, such as ERP, CRM, and BI solutions.
- The operations or production manager is in charge of production control and other special applications, such as Manufacturing Execution Systems, Energy Management Systems, and Supervisory Control and Data Acquisition Systems.

IT and OT solutions emerge independently of each other over time. They solve different problems and use different system architectures and communication protocols. For example, IT systems were developed to connect applications and enable data sharing, and they generally use an open, standards-based architecture.

Operational control systems, on the other hand, are devised as standalone systems and were not originally designed for connection to the outside world or for external access. OT systems are frequently self-contained and proprietary.

Department managers and IT architects see the IoT as a catalyst for change. They want to deploy standards-based operational control systems as an important component of IoT projects, thereby replacing standalone measuring devices, sensors, and actuators with intelligent, IP-based devices. By interlinking OT and IT solutions on the basis of established protocols and modules, companies can link heterogeneous systems and processes, thereby eliminating redundancies.

When attempting to link OT and IT systems, system architects are faced with a number of functional requirements:

SCALABILITY

Intelligent systems record and analyse large quantities of data from a variety of endpoints and require high-performance computing, storage, and networking capacities to do so.

AVAILABILITY

Many intelligent systems are designed to be deployed in environments where system failure

THE TWO ORGANISATIONAL UNITS HAVE TO COORDINATE THEIR ACTIVITIES IN ORDER TO BENEFIT FROM A CONVERGENT OT AND IT ENVIRONMENT WITH A UNIFORM IOT ARCHITECTURE.

might lead to reduced productivity, unsatisfied customers, or even loss of revenue. In the case of critical applications such as medical applications, monitoring solutions, and smart grid implementations, system failure may even result in severe damage to health or the environment.

SECURITY

Intelligent systems frequently depend on the publicly accessible Internet or use cloud-based computing and memory resources. To protect against loss or theft of data or a denial of service attack, the new solutions have to be optimally secured and easy to maintain. This means, among other things, that it must be possible to apply security patches quickly. OT is not traditionally configured to support this.

To achieve optimal scalability and reliability, a hierarchical, intelligent system architecture consisting of a device tier, a gateway tier, and a datacentre or cloud tier, is required.

- The device tier includes endpoints such as IP-capable measuring devices, sensors, displays, actuators, medical devices, antennas, machines, and vehicles, where data is collected and then transmitted.
- The datacentre or cloud tier consists of computing or memory capacities, for example, for industrial process monitoring and control. But it also includes integration into the existing IT infrastructure, the deployed ERP systems, and other business-oriented company applications. The connection to the company's value chain is made here.
- The gateway tier serves as an intermediary between the devices and the datacentre or the cloud. It aggregates device data and can buffer it before relaying it to the datacentre. In addition, it transfers controlling information to the device on the basis of open messaging standards. It also serves as a buffer for data that is required for tactical analysis or regulatory requirements.

Furthermore, gateways can facilitate a direct, local reaction, as required – without going through the datacentre. Therefore, the gateways can be situated in the factory hall, a train station, or a hospital wing.

GATEWAYS

IoT gateways are the cornerstones of a convergent OT and IT architecture. They were especially developed to close the gaps between devices in the field, as well as in central economic and industrial applications. IoT gateways optimise the performance of a solution by collecting real-time data from operating procedures at the place of origin and performing initial processing.

In this way, they disburden the applications in the datacentres and the cloud and facilitate efficient development by introducing an abstraction tier between the devices and the application. Furthermore, by separating the devices from the applications, they enable new endpoints to be added more quickly and easily to a configuration.

The Industrial Internet of Things, IIoT area provides a good example in this context: here, gateways are used due to different communication technologies and can deliver value-added services at the intersection of IT and OT. In this use case, data often needs to be converted between fieldbus systems

KEY TAKEAWAYS

- Through a convergence of OT and IT environments, companies can improve their performance and reduce the total cost of ownership.
- Different organisational units have previously been responsible for OT and IT functions – with different targets, budgets, and strategies.
- To achieve scalability and reliability, a hierarchical system architecture consists of device tier, gateway tier, and a cloud tier.
- Most IT companies still treat IT and OT as separate areas and develop, maintain, and use the two for different purposes.
- IoT gateways are the cornerstones of a convergent OT and IT architecture.

– for example the Modbus – and TCP. In doing so, data can also be aggregated and machine conditions for example are only reported when there is a change.

Another example is building services where different communication technologies are used, for example power line communication, different radio frequencies and protocols as well as bus systems. Collected data can be transferred into a unified TCP communication and data can be enriched – for example from which building, which room, and which sensor does the data come from?

Furthermore, data can also be aggregated, the gateway only sends a message when the temperature is changing. Here, reactions might be necessary locally and self-sufficiently in order to stick to required reaction times or to ensure reactions when connectivity to the datacentre is interrupted.

Finally, there are use cases in the transportation sector. It might be necessary to amalgamate data from the tractor, the trailer and the cargo directly at the vehicle – again either to react locally, when having an unstable data connection to the datacentre or because there are heterogeneous technologies for vehicle, trailer and cargo that cannot be controlled by one tool.

The hierarchical architecture addresses the strict requirements regarding IoT scalability, availability, and security. The number of gateways can be increased incrementally, thereby enabling cost-efficient growth. To avoid single points of failure, companies can implement redundant architecture components at every tier.

This ensures service availability, for example, in cases of an individual component malfunction. Specific security measures that cover a comprehensive spectrum of threats and vulnerabilities should be implemented at every tier.

> BY SEPARATING DEVICES FROM APPLICATIONS, THEY ENABLE NEW ENDPOINTS TO BE ADDED MORE QUICKLY AND EASILY TO A CONFIGURATION.

CONVERGENCE

Through a convergence of OT and IT environments, companies can improve their performance and reduce the total cost of ownership. However, detailed preliminary analysis and planning is required to reconcile various departments, disciplines, and business processes optimally with each other. In most companies, different organisational units have previously been responsible for OT and IT functions – with different targets, budgets, and strategies.

The OT department implements and supports highly specialised process control systems that ensure continuous availability of applications. Yet, the IT department implements and supports comprehensive, complex, open systems that depend on standards-based networks and servers running virtualised applications that partly rely on cloud services.

The two organisational units have to coordinate their activities in order to benefit from a convergent OT and IT environment with a uniform IoT architecture.

Unlike traditional, manufacturer-specific control systems, modern OT solutions use standards-based IT infrastructures and communication protocols; as a result, they can achieve greater flexibility and scalability while remaining cost-efficient. Thanks to the convergence of previously separated OT and IT environments, companies might now be in a position to increase performance while reducing complexity and infrastructure costs. ■

GEC OPEN

DUBAI CORPORATE GOLF WORLD CUP

AMATEUR SERIES

AUSTRALIA
AZERBAIJAN
BAHRAIN
BOTSWANA
CANADA
CHINA
EGYPT
FRANCE
GHANA
INDIA
INDONESIA
ITALY
KAZAKHSTAN
KENYA
MALAYSIA
MAURITIUS
NEW ZEALAND
NEPAL
NIGERIA
OMAN
RUSSIA
SAUDI ARABIA
SCOTLAND
SINGAPORE
SRI LANKA
SPAIN
SOUTH AFRICA
SWITZERLAND
THAILAND
TURKEY
UAE
UNITED KINGDOM
US
ZIMBABWE

34
PARTICIPATING COUNTRIES

50
QUALIFYING ROUNDS

3,700
C-LEVEL EXECUTIVES

FOR MORE VISIT:
www.gecopen.com

CONTACT:
ronak@gecmediagroup.com, vineet@gecmediagroup.com, bharat@gecmediagroup.com

A digital performance gap exists

While digital performance is deemed critical, and successful digital strategies can have a meaningful impact on the business, there is a significant digital performance gap that exists today impacting the customer experience, diminishing productivity, and causing deadlines to push.

80%

report that important digital services and applications are failing a few times a month or more

22%

report that important digital services and applications are failing a few times a week or more

When digital performance suffers, business performance is impacted

42% Loss of Sales and Revenue

41% Delayed Product Launches

41% Loss of Customers

41% Loss of Brand Loyalty

40% Loss of Employee Productivity

Source: Riverbed Digital Performance Global Survey 2018

Source: Riverbed Digital Performance Global Survey 2018

MEET THE SERVERS BUILT TO BUILD YOUR BUSINESS

With no-compromise scalability, intelligent automation and integrated security, the latest Dell EMC PowerEdge servers with Intel® Xeon® Platinum processor are your foundation for innovation.

intel XEON PLATINUM inside

DELL EMC

DellEMC.com/servers