SUPPLEMENT OF ENTERPRISE CHANNELS MEA

BUSINESS TRANSFORMATION

AUGUST 2019

THE CHANGE TO FUTURISTIC BUSINESS

biznesstransform.com

SPECIAL ISSUE

STRATEGY

CYBERSECURITY INTEGRAL PART OF TRANSFORMATION

No successful transformation can be rolled out if cyber security strategy is added as an afterthought.

(Left to right) Ammar Enaya, Vectra; Fabio Picoli, Trend Micro; Jay Townsend, Booz Allen Hamilton; John Hathaway, BeyondTrust; Mohammad Jamal Tabbara, Infoblox; Nasser Bostan, BT; Nicolai Solling, Help AG; Rajesh Ganesan, ManageEngine; Sheikh Shadab, KPMG; Tarek Kuzbari, Bitdefender.

Shaikh Khalifa, Bahrain Bourse

BAHRAIN BOURSE SELECTS AWS AS PARTNER TO DRIVE AGILITY

Bas Burger, Global BT

BT TO PROVIDE INTELLIGENT GLOBAL NETWORK FOR SCHINDLER

Leon Smith, DEX

DEX APPROVED TO OPERATE AS CRYPTO EXCHANGE BY ABU DHABI GLOBAL MARKET

Ali Mohd Al Jassim, Etihad ESCO

HOW ETIHAD ESCO IS TRANSFORMING RETROFITTING OF ENERGY SERVICES

George Bou Mitri, Honeywell

HONEYWELL SURVEY SHOWS LACK OF DIGITAL CULTURE, SKILLS LIMITING IIOT ADOPTION

CONTENTS

JUNE 2019

SUCCESSFUL TRANSFORMATION ENABLED BY CYBERSECURITY
Key vendor executives share their point of view.

Ammar Enaya, Fabio Picoli, Jay Townsend, John Hathaway, Mohammad Jamal Tabbara, Nasser Bostan, Nicolai Solling, Rajesh Ganesan, Sheikh Shadab, Tarek Kuzbari.

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

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

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

Business continuity has been a management subject for decades now. After the development of modern datacentres and the increasing role of technology in critical national infrastructure, the concept of disaster recovery sites took mainstream attention. Now, with the increasing maturity of cybersecurity technologies, malware, and state actors, the offensive role of cybersecurity in collapsing a nation's digital economy has now begun to attract attention. The integration of business continuity, disaster recovery, and cybersecurity risk assessment are becoming a key focus area. It is not only acts of nature and force majeure that can paralyse a city or a nation. Cybersecurity and the lack of its integration with the rest of a business or a city or a nation's continuity framework systems may in the future prove to be a costly oversight.

Booz Allen Hamilton in a recent document develops the concept of The Resilience Equation. The Resilience Equation concept relies on three practices: risk assessment, continuity, and testing and exercise. By including cyber security risk assessment, recovery and contingency planning, repeated testing and improvement, businesses can improve their preparedness towards reducing the impact of cyber security threats and losses.

The report points out that while digital transformation and interconnectivity are valuable, they also intensify the frequency and severity of cyber-attacks. This is costing the global economy $600 billion annually, with an average loss of $3.86 million per breach.

While technology and transformation will ultimately take businesses to the next level of large scale customer engagement, the pace of change in laws, regulations, standards, and new technologies has resulted in an increasing number of errors as people struggle to keep up. Dizzying complexities are costing organisations an alarming, 10%+ of their annual profits on average.

In this special issue of Business Transformation, we continue the focus on cybersecurity and present the viewpoints of top vendor executives on the role of an effective cybersecurity strategy and successful business transformation. We also bring in expert comments from Haider Pasha, Palo Alto Networks; Juan Manuel Harán, ESET; Maher Jadallah, Tenable; Roberta Witty, Gartner; Arafat Yousef, Nexans Solutions; on how cyber security is impacting the transformation of regional enterprises.

Our star Editor's Pick in this issue is the deep dive with Etihad ESCO's CEO, Ali Mohd Al Jassim, who explains how the complex interplay of innovative energy services if retrofitted with legacy operational processes, can lead to substantial energy savings, sustainability and modernisation of the building asset. Such an interplay occurs through a fascinating understanding and competence over scores of OEM solutions, working with multiple suppliers, energy and engineering processes, and end of life switch-overs.

This issue is packed with so many must-reads!

Happy readings and happy learnings.

Arun Shankar
arun@gecmediagroup.com

TIME FOR REGIONAL FASHION TO EMBRACE SUSTAINABILITY

Every item in fashion has a sustainable alternative provided manufacturers are compelled to shift, argues Alana Sorokin at Joseph & Alexander.

ALANA SOROKIN, Founder of Joseph & Alexander.

KEY TAKEAWAYS

- A YouGov survey in UAE highlighted that today's consumer wants to shop sustainably but the price is a major motivational factor.
- 75% consider sustainability when buying fashion items but it does remain behind other factors.
- Fitting, material quality, design and price were documented as being more important when deciding what to buy.
- Making sure pieces are developed in a sustainable manner is considered time-consuming and costly.
- As designers and producers, we must sit up, take action and answer consumer needs.
- Every part of the fashion process has a sustainable alternative and this can be done cost-effectively.

Sustainability in retail is no longer a choice. With the volume of noise increasing around fast fashion's jaw-dropping impact on the environment, many people are still shocked to learn that the fashion industry is the second largest polluter on earth, only after oil.

We know that the rise of fast fashion is fueled by the disposable nature of consumers. This has a direct impact on how quickly brands turn around new products in order to keep up with demand. However, with the need to keep costs low, these brands, of course, seek out shortcuts to reduce processes, meaning suppliers or manufacturers may not be up to standard, which in turn creates a negative social and environmental impact on our planet.

Unfortunately, the number of sustainable retailers in the region and the world is worryingly low, which is why businesses must step up their game to go in the same direction as other industries leading the way in this initiative.

The fashion industry is a complicated business, there are many different suppliers and manufacturers within the process and with all these middlemen, making sure the pieces are developed in a sustainable manner is considered both time-consuming and costly. However, it is a process that fashion companies must start integrating into their long-term plans, with both high street to designer brands responsible for the movement to provide a positive impact on the environment.

Almost every part of the fashion process has a more sustainable alternative and this can be done cost-effectively. Instead of using plastic buttons, organic corozo - derived from the Tagua tree - is not only biodegradable but is also durable and scratch resistant. Choosing wooden hangers over plastic as well as a biodegradable garment or retail bags are also just a few small steps that can improve environmental impact.

When it comes to textiles and the materials used for clothing, organic and recycled cotton, as well as Tencel, coming from the pulp of the eucalyptus tree, are comfortable, cool and light alternatives over the standard materials used in the industry.

Furthermore, a UAE focused YouGov survey highlighted that consumers are more inclined to purchase sustainably if brands pushed their messaging a bit harder. Just under half say they would buy sustainable fashion if the brand shared information on the benefits and impact of sustainability 47% or set out their sustainability credentials more clearly on their labels 46%. Furthermore, a third 34% would purchase if they promoted sustainability in their communications.

With the growing demand and expectations from customers, the fashion industry is increasingly under pressure to make a difference in its practices. It is, therefore, the responsibility of the consumer to continue this pressure to ensure more sustainable approaches are made within the fashion industry and for brands as a whole to react accordingly. ■

#REVOLVESENTINELS

CYBER SENTINELS
PRESENTS

GEC SECURITY SYMPOSIUM AND CISO AWARDS 2019

04 SEPTEMBER 2019
DUBAI, UNITED ARAB EMIRATES

11 SEPTEMBER 2019
KSA, RIYADH, KINGDOM OF SAUDI ARABIA

ARE YOUR CYBER SENTINELS ARMED?

BROUGHT BY

GEC MEDIA

OFFICIAL MEDIA PARTNER

Enterprise CHANNELS MEA

BT BUSINESS TRANSFORMATION

FOR MORE VISIT: gecmediagroup.com
CONTACT: arun@gecmediagroup.com, anushree@gecmediagroup.com,
divsha@gecmediagroup.com, ronak@gecmediagroup.com,

FOLLOW US: You Tube www.youtube.com/channel/UCbR-mbzVb6RThghxHg_HxRg

TRANSFORMATION IN ACCOUNTING BOOSTING ENTREPRENEURSHIP

Automation and analytics in accounting are helping businesses to grow more efficiently explains Vikas Panchal at Tally Solutions.

VIKAS PANCHAL,
Business Head,
Tally Solutions Middle East.

In today's 21st century, enterprise companies have been among the first to embark on digitalisation journey to improve operational efficiency and, more importantly, remain relevant and competitive.

The use of digital technologies in the enterprise sector is now the norm in an era where customers are becoming more and more tech-savvy and connected. Not only that, several young aspiring entrepreneurs with creative and innovative minds and a knack for digital tools and services are becoming active and determined to make it big and successful in the business realm.

Tools such as artificial intelligence, 3D printing, Internet of Things, robotics, big data analytics, cloud, and drones, among others, have changed the face of entrepreneurship. One way or another, almost all industries have been looking into optimising game-changing technologies to deliver outstanding customer experience, create and add value, and be ahead of the market competition.

Businesses, for instance, are using technology solutions to know their customers more, allowing them to go deeper when meeting their unique needs and anticipating their future demands. These solutions enable business organizations to engage with customers faster, thereby further enhancing their experience.

Furthermore, many business firms have shifted to digitally driven and automated business management software solutions for efficient processes and procedures. These business management software aid in increased organisational productivity, profitability, and acquiring a 360-degree view of the business to take critical decisions.

Sorting this data out and turning them into a comprehensive industry analysis give entrepreneurs a chance to take relevant and impactful decisions, provide better services and have valuable marketing techniques.

Cost-effective and end-to-end business management software with advanced features are an investment towards the business growth and help in the long run. These are used to ease account maintenance, automate accounting processes, have a better view of the inventory management, minimise human error, smoothen transaction entry, come up with analysis-based decisions, and many more.

Digitalisation has paved the way for a modern business approach that focuses more on innovation and creativity. This leads to products and services that fit today's customers. However, despite many advantages of automation, resistance towards adoption can be seen. Which is why, entrepreneurs must understand that it is for the betterment and growth of the overall business. A careful approach most suited for the company, its vision and mission, and values and culture will assist in this transformation.

Digital revolution has taken the world by storm, most especially the business sector. It is more than achieving business efficiency. It is at the core of a business organisation's survival, expansion, and eventual success in this day and age. ■

KEY TAKEAWAYS

- Sorting data out and turning them into industry analysis give entrepreneurs a chance to take impactful decisions.
- Cost-effective business management software with advanced features are an investment towards business growth and help in the long run.
- A careful approach suited for the company, its vision and mission, and values and culture will assist in transformation.

HOW FIBRE NETWORKS CAN BOOST DIGITAL TRANSFORMATION

Fibre architectures are best suited for scale, agility, use cases of digital enterprises, explains Arafat Yousef at Nexans Cabling Solutions.

ARAFAT YOUSEF, Managing Director Middle East and Africa, Nexans Cabling Solutions.

With the arrival of 5G, smart cities, connected cars - large scale, intelligent networks promise to dominate country, regional, and global landscapes over the next ten years. Wireless and wired networks are growing tremendously with intelligent and semi intelligent-sensors distributed at the edge, relaying trends and insights, downstream to decision makers.

Sustainability, innovation, efficiency, and citizenship promise to be in-country hallmarks for the UAE with the appointment of Minister of Climate Change and Environment, Advanced Sciences, Artificial Intelligence, and Happiness and Wellbeing. Along with smart production, distribution, consumption - conservation of energy will increasingly become an integral part of the UAE's or for that matter any nation's most valued system.

A study published by the European Commission points out that the global ICT industry generates up to 2% of all global CO2 emissions. Networking components and cabling, computing and data centres, connected devices and sensors, all consume energy and are responsible for generating heat and emitting CO2 into the environment. As the digital economy grows exponentially, so will consumption of energy and production of heat and CO2.

Similar to all aspects of the ICT industry, digital transformation has triggered a wave of efficiency standards into networking and connectivity infrastructure. In the past, while twisted pair copper cabling may have been sufficient to meet all the requirements of enterprises, going forward additional efficiency metrics and architectures will be required. Increasingly, the advantages of the role of Fibre To The Office, FTTO are getting highlighted, as being beneficial over traditional LAN.

FTTO is a hybrid network consisting of fibre optic and twisted pair copper patch cords with connectors. In an FTTO network environment, fibre is laid from the central distribution switch right into the office floor, where it ends in active FTTO switches within the workplace. The last leg of 3 to 5M is connected through standard twisted pair patch cords.

The advantages and disadvantages of FTTO over traditional LAN is quite stark. Fibre optic cabling used in FTTO, as a medium is a dielectric and does not allow the flow of current. Hence, it does not generate heating and electromagnetic wave inductions. It also does not require thick insulation covers, which reduces the bulk and has almost no practical limits to a single length of cabling.

Twisted pair cabling has a core length of copper metal and no matter how pure, the cable does generate heat, as well as electromagnetic wave inductions, whenever there are fluctuations in the current strength. Because of these limitations, there is a maximum length that the copper cable can be used for.

In general, with an FTTO architecture, energy bills can be 70% lower, total cost of ownership is reduced by 40%, and installation time is reduced by 60%. FTTO networks work best when the scale is large, with a huge number of ports and over long distances. ■

GEC AWARDS 2019

HONORING THE BEST

GLORY AWAITS THE CHAMPIONS

1ST OCTOBER 2019

FOR MORE VISIT
GECMEDIAGROUP.COM

GENDER DIVERSE SECURITY TEAMS OUTPERFORM OTHERS

While building gender diversity in security teams is a favourable practice, organizations need to be proactive, argues Roberta Witty at Gartner.

ROBERTA WITTY,
VP Analyst, Gartner.

Diverse teams provide an immediate and long-lasting solution to the global shortage of security talent. For every 100 security and risk management, SRM executives, only about a quarter of them are women. The good news is that as the benefits of diversity are more widely realised, that number will increase by nearly 15% by 2020.

While this makes for pretty sober reading, the good news is that the general workforce pipeline has a more balanced male-to-female ratio, meaning that over time, it is likely that there will be more female leaders in the discipline.

The Gartner Gender Diversity in Security and Risk Management Survey explored how gender diversity impacts the ability of an organisation to manage its security and risk management objectives.

Gender-diverse and inclusive teams outperform gender-homogeneous, less-inclusive teams by an average of 50%. Recent Gartner research found that managers of inclusive technology teams were more likely to say their teams outperformed non-inclusive teams in all seven measures studied, including implementing new ideas and making timely decisions.

Early exposure to security and risk management disciplines develops more qualified candidates and provides professional support for gender parity. Gartner recommends that companies target women while they are still in school to sell them on a career in security and risk management.

Grow the general workforce pipeline for security and risk management by partnering with primary, secondary and higher educational institutions to introduce young women to the security and risk management professions. Do not focus only on technical educational programs; approach liberal arts and communications academic programs to ensure that females understand the value of a security and risk management career choice.

Women find security and risk management professions to be excellent career paths, according to the survey. However, concerted efforts must be taken to retain them; otherwise, women may leave their positions to find a transparent and supportive work environment elsewhere.

Respondents believe sponsoring and mentoring high-potential women will improve the recruitment and retention of women in security and risk management. Diversity task forces are extremely important, but mandatory diversity training, job tests and grievance systems are not perceived as beneficial for organisational diversity.

Implement gender-blind recruiting practices and training to mitigate gender discrimination, and use retention practices that promote women to top leadership and executive positions. Providing work-life balance practices such as flexible work hours is a competitive differentiator in the labor market that can improve the retention and recruitment of women.

People want to work where they know they will be accepted and respected for their unique background, skills and knowledge. It is a win-win situation for all parties. These efforts will contribute to the vast majority of organisations that will exceed their financial targets through 2022 by equipping frontline decision-making teams with a diverse and inclusive culture. ■

Swing Local - Connect Global

GEC OPEN

DUBAI CORPORATE GOLF WORLD CUP

AMATEUR SERIES

2019-20

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

40
PARTICIPATING COUNTRIES

60
QUALIFYING ROUNDS

4500
C-LEVEL EXECUTIVES

FOR MORE VISIT:
www.gecopen.com

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

REMOVING THE DISCONNECT BETWEEN BOARD AND SECURITY

Overloading the board with jargon and complex charts does not help make the case for the security department, explains Maher Jadallah at Tenable.

MAHER JADALLAH, Regional Director, Tenable Middle East.

As technology moves to the centre of most organisational processes across the GCC, CIOs are communicating with the board more often, whether to discuss budget requirements or strategic cybersecurity defenses. Although more people are becoming familiar with IT terms, geek speak can leave many feeling dazed and confused. Talking about Remote Code Execution RCEs, Internet Protocol Security IPSEC, Cross-site Scripting, and Cross-site Request Forgery, for example, can leave listeners baffled and waste valuable board face-time.

Other terms often mean one thing in daily parlance but something else entirely to IT specialists. For instance, a watering hole is neither a gathering place for Oryx nor a venue to unwind after work; whaling does not include a net; a firewall involves neither fire nor a wall; and the sort of container most frequently referred to does not specifically concern maritime trade.

Security is a serious topic that senior executives are particularly alert to, so it is important that there are no misunderstandings. IT and security teams must replace the jargon with language their listeners will understand, if they want to win support for their projects.

In general, upper management finds comfort in metrics. When talking to sales, for example, they seek to understand conversion and close rates. With marketing, it is all about cost per lead. Security must, likewise, focus on quantitative assessments to compare and track performance. The most effective IT and Security pros will be those that can translate the technology and correlate security controls to a metrics-driven conversation. Metrics are the Rosetta Stone of cross-functional conversation.

Here are four key pointers to keep in mind when deciding which metrics to use and how to present them in a way that wins and retains the boards attention:

QUANTIFIABLE DATA

Information that can be monitored and analysed over business cycles serves to inform and educate non-IT audiences. For example, when a big vulnerability like BlueKeep hits - a security vulnerability that was discovered in Microsoft's Remote Desktop Protocol that has the potential to spread in a worm-like fashion and replicate without requiring user-interaction.

A demonstrable metric would be the estimated time required to patch against it. This will highlight how

THE BEST BOARD-LEVEL PRESENTATIONS ONLY SHOW A HANDFUL OF METRICS.

long the company is exposed and at risk. Is it 15 days, 30 days or longer? How can downtime be reduced and, if investment is needed, what will the return be?

LUCID GRAPHICS

When presenting to management, it is important to reduce complex graphs and analytical tables into simple indicators. List the things you want to talk about to keep the conversation focused on your goals. A good question to ask yourself is, what is the intended outcome of showing this piece of data? What do I want the board to do? If you cannot answer that, or have included the slide to fill time, delete it.

The best board-level presentations only show a handful of metrics, each selected to steer the conversation towards new investment or perceptible improvements.

RIVETING PRESENTATION

The best route to winning buy-in for your proposals is a professional presentation with simple and precise information. Think about how you are sharing this data. Spreadsheets, though easy to create for many, may not be the right format as endless columns of numbers can be hard to navigate. And no one likes death by PowerPoint.

To avoid these traps, consider a format that clearly underscores the point you are conveying, and makes it compelling and eye catching – such as an infographic.

Rehearse your presentation and put yourself in the audience's shoes: What terms are unclear? What graphics are hard to read? Modify or get rid of them and tweak your work so it attracts the attention of everyone.

COMPREHENSIVE IDEAS

Not everyone around the table will be a security expert, so avoid terms only the security or IT teams will understand – you are not trying to teach them to speak geek. Instead of playing IT teacher, consider how to make your point simply and effectively, while presenting new ideas in bite-sized morsels that will give your listeners something to chew on. As mentioned earlier, you do not want to risk someone in the room thinking you are talking about port storage solutions when you are actually discussing a development platform.

Instead, focus on making sure everyone can understand what is being discussed and all are in alignment of next steps. With understanding comes the opportunity for actual communication between the board and security experts – and with that comes buy-in.

To sum up, talk to the board in simple, easy-to-understand metrics presented in an attention-grabbing manner. Focus on measurable data and do not overdo the geek speak. The board does not need to be security experts – that is your role. But you do need to make sure they understand what you require and why, as well as what it will deliver for the organisation. ■

KEY TAKEAWAYS

- People are becoming familiar with terms, but geek speak can leave many feeling confused.
- With understanding comes opportunity for communication between board and security and with that comes buy-in.
- Talk to the board in simple, easy metrics presented in attention-grabbing manner.
- Focus on measurable data and do not overdo geek speak.
- The board does not need to be security experts, that is your role.

SKYHAWK
SURVEILLANCE
The Best Comes From Within
Rely on 14TB
for superior surveillance.
SEAGATE
SKYHAWK
14TB
SkyHawk
ASBIS®
Phone: +971 4 8863850
E-mail: info@asbisme.ae
www.asbisme.ae
SEAGATE

WELLNESS TRANSFORMING MILLENNIAL LIFESTYLE PATTERNS

Millennials are ready to adjust their lifestyles to accommodate attributes of top wellness brands writes Krishan Kumar Chutani at Dabur.

KRISHAN KUMAR CHUTANI, CEO Dabur International.

Globally, millennials are often recognised as the key generation driving the $4.2 trillion global wellness market. Their thirst for holistic wellbeing is unparalleled when compared to previous generations. In the US alone, the millennial cohort has grown to value health as the second most valued aspect of their lives.

Armed with their love for health-centric pursuits and interests like yoga, kombucha, and meditation to name but a few, wellness as a whole has bloomed into a way of life instead of something they do on the side. Because this generation harnesses wellbeing methods and products on a daily basis, they have collectively expanded the definition of healthy to encompass a daily commitment to eating right, exercising regularly, and using products and services that support their wellness journeys and objectives.

Nearly everything consumers do is governed by lifestyle approaches that demand a more rounded view of wellbeing. This has forced all sectors to reinvent their approach to meeting the wellbeing needs of consumers. Whether it is the clothing industry creating athleisure apparel enhanced with nutrient-rich materials like sea kelp and bamboo, or the aerospace industry innovating advanced sleeping and exercising wellbeing pods for the future of flight, no industry has been left untouched by the sheer scale of wellbeing's potential.

Because of this, the need to remain authentic amidst the cross-synergetic democratisation of the wellness segment has forced brands to rethink their approach to product innovation.

For the personal care industry, the go green, natural and organic space has become clouded with brands vying for market share. We only have to look at the value of this sector to understand its attraction.

Representing $1,083 billion of the wellness economy pie, personal care and beauty is one of the world's largest and fastest growing industries.

With a plethora of wellness products flooding the industry, it can oft be difficult for consumers to navigate the greenwashing and hype that various products seek to deliver.

The upshot for brands is they have an opportunity to be authentic in their approach to succeeding in this industry. Millennials are also some of the most shopping-savvy consumers out there. In short, this population segment does not suffer fools. Younger populations are increasingly searching for quality as much as value. And they

YOUNGER POPULATIONS ARE INCREASINGLY SEARCHING FOR QUALITY AS MUCH AS VALUE.

are not afraid to shop around for the best brand to deliver the ideal combination of each.

In the purchase journey, a strong brand is not enough to lock in a sale. Instead, the factors that make them loyal to a brand are ones that supplement their busy lifestyles with real and authentic value propositions.

For the personal care sector, realising how consumers purchase cleaner, greener products go deeper. The wellness landscape is vast and filters across all industries. This means that consumers lives do not just hinge on one or two personal care products in their daily routines. From the moment they wake up until the moment they go to sleep, wellness decision making is with them every step of the way.

Ayurveda-based formulations that omit fluorides and harmful chemicals in the oral care segment are striking a positive note with consumers in the Middle East. The same can be said for our dedication to ensuring kids products do not contain known nasties like parabens and mineral oil.

This is invaluable in the Middle East. Consumers in this region exhibit attitudes and preferences that are different to other generations. In the Arab world, millennials in general demonstrate more brand loyalty than their peers in the US, the UK, Japan or Australia. With the MENA region being one of the worlds most saturated regions when it comes to smartphone penetration, they also discover, buy, support or brush-off brands based on the experiences and the level of personalisation they receive.

With regards to wellness, they perceive quality through the genuineness of brand interactions. What this means is that we have to continue delivering quality products that add true value to their lives and complement the wellness synergies they are seeking across all lifestyle facets.

Wellness is not a fad; it is a way of life that stems from deep within a brand. For industry players to successfully engage and influence brand adoption for modern-day consumers in the vast wellness economy, it is time they begin innovating with an emphasis towards being authentic and delivering quality innovations that truly complement consumers overarching wellness journeys.

- In the purchase journey, a strong brand is not enough to lock in a sale.
- Factors that make them loyal are ones that supplement their lifestyles with real and authentic propositions.
- Consumers lives do not hinge on one or two personal care products in daily routines.
- Consumers in this region exhibit attitudes and preferences that are different to others.
- With regards to wellness, they perceive quality through the genuineness of brand interactions.
- Wellness is not a fad; it is a way of life that stems from deep within a brand.
- Consumers lives do not just hinge on one or two personal care products in daily routines.
- Representing the wellness pie, personal care and beauty is one of the largest and fastest growing industries. ■

APTEC
an INGRAM MICRO company

DELL EMC
PARTNER
AUTHORIZED
DISTRIBUTOR

PowerEdge Servers: The foundation of the modern hybrid data center.

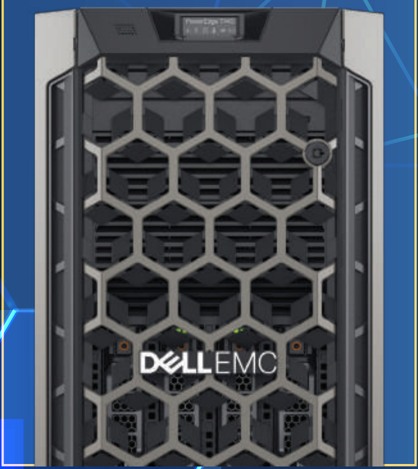
Modernizing with the industry's #1 servers is your starting point for the performance, security and cost advantages of a hybrid infrastructure — including up to 40% less unplanned downtime and up to 30% fewer application errors.

Ready Nodes

Modular Infrastructure

Rack Servers

Tower Servers



Modernize IT with server innovation.

Get in touch with us to know more

Arjun Singh
DELL EMC Technical
Consultant - UAE & Bahrain
Mobile: **+971 58 819 8945**
arjun.singh@ingrammicro.com

Sibin T Mandambeth
Dell EMC Technical
Consultant - Qatar & Oman
Mobile: **+971 58 826 8151**
Sibin.Mandambeth@ingrammicro.com

Zaid Bin Ghayas
Dell EMC Technical PreSales
Consultant - UAE & Kuwait
Mobile: **+971 58 819 9154**
zaid.ghayas@ingrammicro.com

Aptec - an Ingram Micro Company
P.O.BOX: 33550 | Dubai Internet City - UAE
Tel: +9714 3697111 | Fax: +9714 3697110
Website: ae.ingrammicro.com

www.ingramdellemc.com

TAKING OVER A BUILDING SYSTEM THROUGH SIEGEWARE

Unprotected building systems can be tracked through tools like Shodan opening them for Siegeware, explains Tony Anscombe, Juan Manuel Harán, at ESET.

JUAN MANUEL HARÁN, Security Editor ESET.

In countries like the United States, the growth of smart buildings is estimated to reach 16.6% by 2020 compared to 2014, although this expansion is not limited to the US but rather is taking place on a global scale. This growth is largely due to the fact we live in a world increasingly permeated by technology, in which process automation and the search for energy efficiency contribute not only to sustainability, but also to cost reduction. This is a goal pursued in all industries, public and private sector alike. Naturally, the construction industry is no exception.

Smart buildings use technology to control a wide range of variables within their respective environments with the aim of providing more comfort and contributing to the health and productivity of the people inside them. To do so, they use so-called Building Automation Systems With the arrival of the Internet of Things, smart buildings have redefined themselves.

With the information they obtain from smart sensors, their technological equipment is used to analyse, predict, diagnose and maintain the various environments within them, as well as to automate processes and monitor numerous operational variables in real time. Ambient temperature, lighting, security cameras, elevators, parking and water management are just some of the automatable services currently supported by the technology.

To put the possibilities of this smart infrastructure into perspective, taking the example of a hotel in Las Vegas where, two years ago, they decided to install a sophisticated automation system to control the use of the air conditioning keeping in mind that Las Vegas has a hot desert climate and very little rain. So, it is turned on only when there are people present.

This decision led to savings of $2 million during the first year after the smart system was installed, due to the reduction in energy consumption achieved by automating the process. Marriott Hotels implemented a similar system across the entire chain that is expected to generate an estimated $9.9 million in energy savings.

At first glance, we may not see any security risk in these smart buildings. It is likely, however, that at some point the entire smart network is connected to a single database, and that is where the risk is. Particularly if we consider that many IoT devices are manufactured by different suppliers, who may not have paid attention to security considerations during their design and manufacturing process.

The risk of a security incident taking place in an intelligent

THERE ARE TOOLS SUCH AS SHODAN THAT ALLOW ANYBODY TO DISCOVER UNSECURED IOT DEVICES.

building is linked to the motivations of cybercriminals, who mainly seek to achieve economic gain through their actions, as well as make an impact and spread fear.

There are already some tools such as Shodan that allow anybody to discover vulnerable and unsecured IoT devices connected publicly to the Internet. If you run a search using this tool, you can find thousands of building automation systems in its lists, complete with information that could be used by an attacker to compromise a device. In February 2019, around 35,000 building automation systems worldwide appeared in Shodan within public reach via the Internet.

This means that someone could take control of a building automation system after finding it through a search. If, for example, a criminal uses Shodan to search for building automation systems to attack, they will find IP addresses.

If they copy those IP addresses into the address bar of a web browser, in many cases this will bring up an interface for gaining access, where they need to enter a username and password. If the password is a default password or if it can be cracked easily through a brute force attack, the attacker will gain access to the system monitoring panel, which contains information similar to the details visible to the companies located in the smart building.

Once they have control, they could alter the building's heating or air conditioning systems, or adjust the way any of the other automated systems operate, and then demand payment of a ransom in using a system that allows them to remain anonymous, such as cryptocurrency, in exchange for not shutting the building down.

This kind of attack is not an isolated event. In other words, cybercriminals are already carrying out such attacks when they have the opportunity. This is a kind of Siegeware, or the code-enabled ability to make a credible extortion demand based on digitally impaired building functionality.

In conclusion, the low cost of IoT devices for buildings and the advances in technology for building automation systems is leading to changes with an impact on security. This drive toward automation and the use of smart devices to gather data – in order to give a building's users more comfort and to make more efficient use of resources such as energy – is also leading to increased security risks. As a result, the possibility of a cybercriminal launching a ransomware attack on a smart building is already a reality. ■

KEY TAKEAWAYS

- In February 2019, around 35,000 building automation systems worldwide appeared in Shodan.
- Someone could take control of a building automation system after finding it through a search.
- If, a criminal uses Shodan to search for building automation systems to attack, they will find IP addresses.
- Siegeware is the code-enabled ability to make an extortion demand on digitally impaired buildings.

DEX APPROVED TO OPERATE AS CRYPTO EXCHANGE, CUSTODIAN BY ABU DHABI GLOBAL MARKET

DEX has secured an in-principle approval from the Financial Services Regulatory Authority, as a regulated Digital Asset Exchange and Digital Asset Custodian based in the Abu Dhabi Global Market in Abu Dhabi, United Arab Emirates. DEX will provide a platform for both retail and institutional grade investors to invest through a fully regulated exchange into digital assets in a highly regulated financial eco system.

DEX will operate as a regulated Digital Asset Exchange and Digital Asset Custodian under the Operating a Crypto Asset Business framework structured by the Financial Services Regulatory Authority that oversees all crypto asset and financial services activities in the Abu Dhabi Global Market. The exchange will act as a fiat to crypto exchange with major international currencies being served as well as local currency pairings native to the UAE and GCC markets.

DEX represents a regulated crypto exchange in the UAE that will allow retail and institutional investors from the UAE, GCC and global markets to trade on a regulated exchange as a fiat to crypto centralised exchange. DEX will offer institutional investors, high net worth individuals and crypto funds with the ability to trade on a highly regulated exchange and to hold their crypto assets on their behalf as a regulated crypto asset custodian.

LEON SMITH,
Founder and CEO, DEX.

The compliance, market surveillance and measures taken to regulate the exposure of BTC to nefarious sources traded on the exchange will provide the highest level of regulation available in congruence with the regulatory framework employed by the Financial Services Regulatory Authority. Moreover, with corporate tax currently set at 0% in the UAE, the exchange will benefit from reduced taxation as well as potentially attracting institutional investors whose profits may benefit from the same tax regime.

Leading financial jurisdictions such as the United States as regulated by the Securities Exchange Commission have provided guidance as to how digital assets in the form of coins, tokens or other digital assets may be treated. However, as no statutory laws have been enacted by the US Congress as federal law it has left many primary stakeholders within the digital asset eco system conducting business in the United States with little to no surety as to how the financial regulatory authorities will regulate the digital asset eco system.

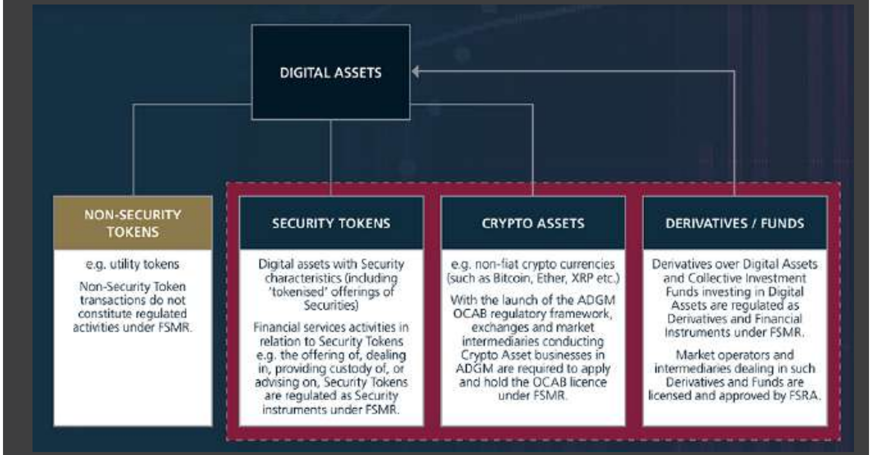
The Operating a Crypto Asset Business framework backed onto the market infrastructure rules in the Abu Dhabi Global Market provides clear guidance as to how crypto assets are treated and represents an attractive regulatory framework for financial institutions to participate in that is congruent with regulatory principles that govern traditional financial markets and products.

DEX embodies first in class operational capabilities, regulatory mechanisms and is positioned to be a regulated Crypto Asset Exchange attracting both local and global institutional investment into crypto assets. Subject to regulatory approval, DEX expects to provide full operational trading services to clients in 2019 in the UAE, GCC markets and globally.

“The GCC has the potential to become a leading financial hub for crypto trading and digital assets. Regulations are being implemented. In June 2018, Abu Dhabi Global Market has launched a framework to regulate spot crypto asset activities undertaken by exchanges, custodians and other ADGM intermediaries,” says Leon Smith, Founder and CEO, DEX.

“The regulatory framework that has been enacted by the Financial Services Regulatory Authority of Abu Dhabi Global Market sets a new benchmark for the regulation of digital and crypto assets on a global scale. DEX will provide a secure platform for our clients to trade crypto assets securely in a regulated environment.” ■

Regulations on operating a crypto asset business


DIGITAL ASSETS
NON-SECURITY TOKENS
e.g. utility tokens
Non-Security Token transactions do not constitute regulated activities under FSMR.
SECURITY TOKENS
Digital assets with Security characteristics (including 'tokenised' offerings of Securities)
Financial services activities in relation to Security Tokens e.g. the offering of, dealing in, providing custody of, or advising on, Security Tokens are regulated as Security instruments under FSMR.
CRYPTO ASSETS
e.g. non-fiat crypto currencies (such as Bitcoin, Ether, XRP etc.)
With the launch of the ADGM OCAB regulatory framework, exchanges and market intermediaries conducting Crypto Asset businesses in ADGM are required to apply and hold the OCAB licence under FSMR.
DERIVATIVES / FUNDS
Derivatives over Digital Assets and Collective Investment Funds investing in Digital Assets are regulated as Derivatives and Financial Instruments under FSMR.
Market operators and intermediaries dealing in such Derivatives and Funds are licensed and approved by FSRA.

The universe of digital assets regulated by the Financial Services Regulatory Authority of Abu Dhabi Global Market includes security tokens, crypto assets and derivatives funds.

To address the global demand from industry players, the Financial Services Regulatory Authority of Abu Dhabi Global Market launched a comprehensive and regulatory framework in June 2018 for the regulation of exchanges, custodians and other intermediaries engaged in crypto asset activities. The framework sets a high watermark catering to participants who are committed to conducting their crypto asset businesses in a safe and trusted environment.

It is designed to address the full range of risks associated with crypto asset activities, including risks relating to money laundering and financial crime, consumer protection, technology governance, custody and exchange operations.

Crypto Asset means a digital representation of value that can be digitally traded and functions as: medium of exchange, unit of account, store of value, but does not have legal tender status in any jurisdiction. A Crypto Asset is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and distinguished from fiat currency and E-money.

Financial Services Regulatory Authority will only allow Operating a Crypto Asset Business licence holders to use accepted crypto assets within the Abu Dhabi Global Market. Financial Services Regulatory Authority has a general power to determine each Accepted Crypto Asset that will be permitted in relation to Operating a Crypto Asset Business activities within the Abu Dhabi Global Market.

For the purposes of determining whether a Crypto Asset meets the requirements of being an Accepted Crypto Asset, Financial Services Regulatory Authority will consider: maturity market capitalisation threshold at the time of an application; other factors that in the opinion of Financial Services Regulatory Authority, need to be taken into account in determining whether or not a particular Crypto Asset meets the requirements to be considered an accepted Crypto Asset, including:

- Security
- Traceability, monitoring
- Exchange connectivity
- Market demand, volatility
- Type of Distributed Ledger
- Innovation, efficiency
- Practical application, functionality

Business distinguishes the regulation of Crypto Asset activities from the regulation of financial instrument, specified investment related activities under the Financial Services Regulatory Authority's existing regulatory framework. Operating a Crypto Asset Business licence holders will be issued with a single financial services permission for the purposes of Operating a Crypto Asset Business irrespective of the Crypto Asset activity that they are conducting. Two key specific activities attract higher regulatory requirements, namely:

- Operating a Crypto Asset Exchange
- Operating as a Crypto Asset Custodian

AWS Bahrain region to offer triple availability option for regional users

Amazon Web Services, announced opening of the AWS Middle East Bahrain Region. With this launch, AWS now spans 69 Availability Zones within 22 geographic regions around the world, and has announced plans for nine more Availability Zones across three more AWS Regions in Indonesia, Italy, and South Africa. Developers, startups, and enterprises, as well as government, education, and non-profit organisations can run their applications and serve end-users from data centres located in the Middle East, as well as leverage advanced technologies from the world's leading cloud, to drive innovation.

The new AWS Middle East Bahrain Region offers three Availability Zones. AWS Regions are composed of Availability Zones, which each comprise at least one data centre and are located in separate and distinct geographic locations with enough distance to significantly reduce the risk of a single event impacting business continuity, yet near enough to provide low latency for high availability applications.

Each Availability Zone has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple Availability Zones to achieve even greater fault-tolerance. AWS infrastructure regions meet the highest levels of security, compliance, and data protection.

ANDY JASSY,
CEO Amazon Web Services.

Enterprises across the region are moving to AWS to become more agile and innovate, and include Al Jouf Cement, Al Tayer Group, Arab Banking Corporation Bank, Aramex, Bahrain Bourse, Bank Al-Etihad, Batelco, Emirates NBD, Flydubai, Gulf News, Hassan Allam, Lulu International Exchange, MBC Group, OSN, Seera Group, Union Insurance, Virgin Middle East, and many more.

Public sector organisations, including Government of Bahrain's Ministries, such as the Ministry of Education, Ministry of Finance, Ministry of Information Affairs, Ministry of Labor and Social Development, and Bahrain iGA, as well as other public sector organisations such as Bahrain Polytechnic, Communications and Information Technology Regulatory Authority of Kuwait CITRA, Mumtalakat, Paris Sorbonne AD, Tamkeen, University of Bahrain, and many more are also using AWS to drive cost savings, accelerate innovation, and better serve the citizens of the region.

"The cloud has the chance to unlock digital transformation in the Middle East," said Andy Jassy, CEO, Amazon Web Services. "We are launching advanced and secure technology infrastructure that matches the scale of our other AWS Regions around the world and are already seeing strong demand in the Middle East for AWS technologies like artificial intelligence and machine learning, data analytics, IoT, and much more. We are excited to see how our cloud technology will provide new ways for governments to better engage with citizens, for enterprises to innovate for their next phase of growth, and for entrepreneurs to build businesses and compete on a global scale." ■

Honeywell survey shows lack of digital culture, skills limiting IIoT adoption

More than 70% of medium-to-large organisations in the buildings and cities sector in the UAE and Saudi Arabia expect to increase spending on digitalisation and Industrial Internet of Things technologies in the next five years, according to a new survey by global technology vendor Honeywell. Findings from the IIoT Market Spotlight – UAE and Saudi Arabia report, which Honeywell has launched in partnership with YouGov and IDC, also reveal that senior decision-makers in the buildings and cities sector are looking to IIoT technologies to capture key benefits including improved operational efficiencies 53%, time savings 50% and increased revenues 26%.

The growing appetite for investment in digital transformation comes as regional governments push forward with the implementation of smart city initiatives. Research by IDC shows spending on smart city technologies in the Middle East and Africa is expected to increase to $2.7 billion by 2022, up from $1.3 billion in 2018. Experts attribute the positive forecast to the acceleration of digitalisation within urban ecosystems as environmental and economic benefits become clear.

Even with increased spending and appetite for digital transformation there remains challenges for the buildings and cities sector to overcome to realise the benefits of digitalisation. Almost half 43% of surveyed executives highlight a lack of digital culture and a lack of qualified staff and training in their organisation as a key hurdle to the adoption of IIoT technologies. More than a third 37% of respondents said data protection issues are a key concern, and 34% cite budgetary pressures as presenting a key obstacle.

GEORGE BOU MITRI, Vice President and General Manager, Honeywell Building Technologies, Middle East, Turkey and Africa.

The Honeywell Masdar Innovation Centre in Abu Dhabi and the Honeywell Technology Experience Centre in Dubai are designed to encourage collaboration and engagement between stakeholders and facilitate the co-creation of industry-specific solutions through the adoption of IIoT technology. Together, the centres demonstrate solutions for a range of sectors including smart buildings and cities.

Honeywell created the Honeywell IIoT Market Spotlight report to gauge the level of understanding and readiness to adopt IIoT technology, among senior decision-makers in medium-to-large enterprises in the UAE and Saudi Arabia. Honeywell commissioned YouGov, a leading market research agency, to interview senior leaders from the buildings and cities, transportation and logistics and industrial verticals to document both the actual and perceived benefits of the technology, as well as the investment outlook for these technologies both today and in the next five years.

A total of 248 interviews were conducted in the UAE 120 and Saudi Arabia 128, with respondents who hold leadership roles, ranging from presidents, vice-presidents and general managers to C-Suite and director-level leaders and department heads. The results were then analysed and compiled by IDC, a leading global IoT analyst house. ■

UAE now ranks #22 in KPMG's latest Growth Promise Indicators survey

UAE ranked as high as 22nd from among 180 countries overall, and ahead of other Middle Eastern countries. The nation's macroeconomic stability, openness, quality of institutions and infrastructure, and human development informed the overall score, earning it recognition in KPMG's 2019 Growth Promise Indicators GPI report.

The UAE has moved up three places in the rankings since last year, largely due to advances in infrastructure development, particularly in transport. The nation's Vision 2021 programme has been a key driver of growth, as it supports development of reliable, sustainable and resilient infrastructure - including regional and transborder - to support economic and social development.

The Growth Promise Indicators report ranks the quality of a country's transport infrastructure as a crucial factor for economic competitiveness. However, the report also clarifies that, while the ability of people and goods to move freely is a fundamental determinant of growth, maintaining and improving transport infrastructure requires significant investment from the public and private sector.

The Growth Promise Indicators report also indicates that an economy equipped with a strong workforce has the potential to grow more quickly. The UAE performs well against this pillar as well, having access to the labor required to power the economy as it expands, and being equipped with the right skills and knowledge to accelerate growth.

VIKAS PAPRIWAL,
Head of Advisory, KPMG Lower Gulf.

KEY TAKEAWAYS

- UAE scores higher than Norway and Sweden according to levels of national debt, budget deficit, public finances.
- The report indicates an economy equipped with strong workforce has the potential to grow more quickly.
- UAE was ranked as high as 22nd from among 180 countries overall, ahead of other Middle Eastern countries.
- The nation's stability, openness, quality of institutions, human development influenced the overall score.

The UAE also scores higher than countries like Norway and Sweden on the macroeconomic stability pillar which assesses countries' progress according to their levels of national debt and budget deficit, and how successfully governments manage public finances.

The Growth Promise Indicator report was first developed in 2014. The Growth Promise Indicators report comprises 26 individual series selected to assess countries' productivity potential, based on relevant academic studies and business survey results. KPMG have covered 180 countries and tracked their performance since 1997. The data indicators are grouped into five key GPIs: macroeconomic stability; openness to catch-up; quality of infrastructure; human development; and quality of institutions.

Vikas Papriwal, Head of Advisory at KPMG Lower Gulf, said: "KPMG's Growth Promise Indicators report offers an unbiased view of a country's true potential, based on factors that go far beyond GDP. It is encouraging that the UAE scores well on pillars like infrastructure development, macroeconomic stability and openness, indicating its potential for businesses and investors. Equally, it speaks to the nation's commitment to large-scale sustainable growth, technology and innovation, and social development programmes." ■

Gant, La Senza, Aspinal in GCC switch to Coniq loyalty management system

Coniq has been selected by Liwa Trading Enterprises to create an innovative new loyalty programme across their retail portfolio in the GCC. The scheme is being called USRA, which means family in Arabic, demonstrating the importance placed on ensuring loyalty customers feel valued and engaged.

Liwa Stores manages 20 international brands, including Gant, La Senza and Aspinal of London. They have partnered with leading loyalty and CRM provider Coniq to design a programme which will operate in many of Liwa Stores' 250 shops across the GCC.

One of the most innovative elements of this programme is that the Coniq technology has been integrated directly into Liwa Stores' Point of Sale System. Customers can register for the programme at any till point, and enjoy a seamless experience when subsequently earning points or redeeming them for exclusive offers. A second innovation is that customers pay a fee to join the loyalty scheme in return for access to exclusive welcome offers.

The loyalty programme run by Coniq is a paid for scheme - people who wish to sign up for the USRA loyalty scheme pay an amount in order to become a member and receive welcome offers that they can redeem against future purchases. As all stores in the scheme are Liwa Stores, they all use the same Point of Sales technology and therefore Coniq have integrated their software into the system - meaning that when people who have signed up to the system make purchases they can very easily earn and redeem points, rather than needing a separate system.

JUSTIN CAGWIN,
GM Middle East and EVP Strategic Growth for Coniq.

Data from the POS system feeds directly into IQ - Coniq's market-leading loyalty platform, allowing Liwa Stores to segment and target their consumers with the most relevant offers and discounts. With guidance from the customer success team, this will lead to increased average transaction value and lifetime spend.

Justin Cagwin, GM Middle East and EVP Strategic Growth for Coniq commented, "With the retail industry in the UAE projected to grow by an estimated 16%, Liwa Stores are excellently placed to capture the thriving store-based market. Loyalty programmes provide a huge amount of insight into shopper behaviour that can be leveraged with Coniq's technology to reap huge rewards."

IQ - Coniq's customer engagement and data platform allows a shopping centre, business district or retailer to launch a loyalty programme which gathers data they have never seen before – for the first time they can match spend in store to an actual consumer. $7 trillion is spent worldwide in shopping centres, identify who is spending it, where, when and why. ■

KEY TAKEAWAYS

- $7 trillion is spent worldwide in shopping centres, identify who is spending it, where, when and why.
- Coniq is a CRM and loyalty provider for retail, providing mobile-enabled programmes for 1,500+ retail brands.
- Coniq has been integrated directly into Liwa Stores' Point of Sale System.

Emaar transforming residential estate with 3D printed unit in Arabian Ranches

Emaar awarded the contract to global 3D printing company and UAE based contractor.

Setting a new milestone in residential property development, global real estate developer Emaar Properties announced plans to build its first 3D printed home in Dubai. This is the first step towards Emaar's ambition to be a leading adopter of advanced construction technologies.

Following a global competition, in which the world's leading 3D printing technology providers participated, Emaar has awarded the contract to 3D print a model home in Arabian Ranches III. The construction will be facilitated using a local contractor with the goal of building in-country competencies in 3D printing for the property sector.

Building the first 3D printed model home underlines Emaar's commitment to adopt innovative construction methods to build faster and at a lower cost while achieving higher design and architectural flexibility. Emaar's use of 3D printing technology will also promote the sustainable use of resources by reducing waste of construction materials and noise pollution.

Upon completion, the 3D printed model home will serve as a reference point for investors to further understand the concept and appreciate the value add that advanced technology brings to the real estate sector.

With this pioneering initiative, Emaar aims to set the region's benchmark in construction best practices as 3D printed homes bring several benefits including accelerated delivery of homes and more flexibility in design. 3D printing is also environment-friendly, with sustainable home construction techniques significantly lowering waste and noise pollution during wall construction. 3D printed homes will contribute to lower cooling costs as customers can choose the thickness and type of insulation that goes into the walls; the thicker the insulation used, the lower the cooling costs.

By embracing 3D printing, Emaar's goal is to create a real estate landscape in the future where customers can design, download and print their homes in the future across Emaar's diverse portfolio of master-planned developments.

As the developer of integrated lifestyle destinations, Emaar has delivered world-class communities such as Downtown Dubai, Dubai Marina, Arabian Ranches and Emirates Living and is also shaping the future of the city with projects such as Dubai Creek Harbour, Dubai Hills Estate, Emaar South, Emaar Beachfront, Arabian Ranches III and the recently unveiled Mina Rashid.

Arabian Ranches III, which was launched last year, has already gained overwhelming response for its residential communities that are defined by lifestyle amenities such as a central park, 4 km long boulevard, lazy river and wide choice of outdoor sports facilities.

Mohamed Alabbar, Chairman of Emaar Properties, said: "As the pioneer of integrated communities in Dubai and the trend-setter in the region's property sector, our plans to embrace 3D printing of homes is an integral part of our digital-first and customer-first strategy." ■

Collinson targets India for expansion of airport experiences and loyalty programme

Collinson, a global vendor in customer benefits and loyalty, announced a multi-million-dollar investment into India to fuel additional growth of Priority Pass, its airport experiences programme. Priority Pass will double its lounge portfolio in India over the next three years, building on its suite of 45 airport lounges in 20 Indian cities and global network of more than 1,200 lounges and airport experiences.

Collinson's wholly-owned and operated airport infrastructure business, Airport Lounge Development ALD, is also working with airports across India to identify opportunities to open its own exclusive lounges and airport amenities to meet the growing demand of domestic and international travellers. ALD is an established leader in the airport lounge space in the US and Europe and is now bringing its successful business model to the Indian market.

As a privately-owned, $1bn company, Collinson has more than 30 years' experience delivering customer benefits and loyalty to some of the world's leading brands within the financial services and travel sectors, including American Express, Mastercard and Visa. Its investment in Indian airport experiences is part of a global vision to enhance its offering to more than 30 financial services clients in India and more than 1,400 banks globally – all of whom rely on Collinson products to acquire and retain the most lucrative of customers – the high spending traveller.

DAVID EVANS,
Joint CEO of Collinson.

KEY TAKEAWAYS

- Priority Pass will double its lounge portfolio in India over the next three years.
- Priority Pass has suite of 45 airport lounges in 20 Indian cities and global network of more than 1,200 lounges.
- Collinson is in discussions with Indian technology service providers for bespoke solutions in India.

Collinson is also in partnership discussions with several innovative Indian technology service providers to ensure it can deliver bespoke solutions in India.

David Evans, Joint CEO of Collinson said: "India is a vital market and one we see on a par with China in terms of growth potential. With 1.7 billion domestic passengers having flown in 2017 and outbound travellers expected to reach 50 million by 2020, the influence of the Indian traveller is only going to increase.

"Having had success with emerging markets such as China, Russia and Brazil, and a presence in India for 15 years, working with 42 clients, it is exciting to triple our investment in India. We look forward to building out our lounge inventory and our own airport infrastructure, creating more locally relevant propositions and further strengthening our team on the ground with additional skilled local resource, and partnering with Indian businesses to redefine the airport experience for the benefit of domestic and international travellers." ■

Bahrain Bourse selects AWS as partner to drive agility and transformation

SHAIKH KHALIFA,
Chief Executive Officer, Bahrain Bourse.

Bahrain Bourse has started migrating to AWS due to increased availability and security while reducing operational costs.

Bahrain Bourse announced it has started migrating to Amazon Web Services, AWS due to the increased availability and security it will get and to increase its application speed and performance, while reducing operational costs. The first phase of the migration includes moving backup and disaster recovery solutions to the cloud, with plans to adopt advanced data analytics services to build smart and innovative trading services.

Using AWS, Bahrain Bourse will take advantage of a range of security tools, including encryption, DDoS Mitigation, and monitoring and logging to ensure they continue to maintain the highest levels of security for their customers. Bahrain Bourse will also be able to retrieve archived data within minutes, enabling it to be more responsive in delivering critical and timely data to customers and to more rapidly meet any regulatory requirements.

As it expands its AWS adoption, Bahrain Bourse will continue to explore new ways to support customers with more advanced trading tools by leveraging data lake tools such as Amazon Simple Storage Service Glacier and AWS Glue, as well as data analytics services such as Amazon Redshift, Amazon Kinesis Data Analytics and Amazon QuickSight.

Bahrain Bourse is a self-regulated multi-asset marketplace operator established since 1987. Bahrain Bourse aims to offer to its investors, issuers, and intermediaries a comprehensive suite of exchange-related facilities including offering listing, trading, settlement, and depositary services for various financial instruments.

Shaikh Khalifa, Chief Executive Officer of Bahrain Bourse, commented, “We have adopted AWS as part of our digital transformation efforts and for its ability to provide us with even higher levels of security and performance. We will continue migrating Bahrain Bourse’s technology infrastructure to AWS in order to increase the innovation we can provide customers and in line with the Government of Bahrain’s Cloud First Policy.”

“With AWS, the ability to store and share data at significantly higher speeds will enable us to deliver our services more efficiently to all of our stakeholders. We are excited to continue exploring more advanced cloud solutions that will enhance our service delivery significantly and enable us to be more competitive at a global level.”

Vinod Krishnan, Head of MENA, AWS, said, “It is exciting to see ambitious financial institutions like Bahrain Bourse transform the way they innovate and serve their customers through cloud technology. With AWS, Bahrain Bourse is now able to increase its performance, while improving security and lowering costs. We look forward to continuing to support Bahrain Bourse in its digital transformation journey.” ■

Schneider Electric transforming energy transmission in Nigeria through microgrids

Lagos Solar
EM-ONE provided design consultancy, project management, and test & commissioning services. The project comprised of 213 off-grid solar systems with integrated backup battery banks and remote monitoring systems installed at 11 Primary Health Centres and 175 secondary schools across 10 Local Government Areas.
LSEB
LAGOS SOLAR
www.lagossolar.com

EM-ONE Energy Solutions has won a contract for 30 mini-grids in Nigeria to power hospitals in Kaduna State.

Africa is still facing a serious problem of energy access. Schneider Electric, a vendor for digital transformation of energy management and automation, has taken the first step in creating an African mini-grid industry involving decentralised electricity generation and distribution networks based on renewable energy. It has signed a memorandum of understanding with EM-ONE Energy Solutions, a Nigerian sustainable energy engineering company.

On the African continent, many cities remain off-grid. With a population of more than 200 million, Nigeria is a country comprising 36 states, only one of which has an electricity network. According to the International Renewable Energy Agency IRENA, West Africa's energy consumption could quadruple by 2030 to reach 219 TWh a year, less than half of the 478 TWh already consumed in France in 2018.

Part of the solution will come from mini-grids, decentralised networks powered by photovoltaic energy. Demand is high: an estimated 200,000 mini-grids are required to power the continent and reach the United Nations Sustainable Development Goal. Schneider Electric, which produces mini-grids at its factory in Kenya, has decided to take its efforts to the next level.

In the past 10 years, the Group has already installed 700 mini-grids in Africa, mainly for rural electrification, through its Access to Energy programme. This has largely been achieved with donations to NGOs and equipment often produced in Europe.

For 18 months, led by its sustainability department, the Group has been working to set up an industry based on mini-grids built or operated by local stakeholders. This has led to a first MoU with EM-ONE Energy Solutions, a Nigerian company that also operates in Canada.

With 12 sales representatives spread out over 12 countries Chad, Senegal, Côte d'Ivoire, Tanzania, and others, Schneider Electric is seeking engineering procurement and construction companies to locally produce its solutions - example Villaya Community, a mini-grid designed for rural electrification, providing 7-63 kW of power. Schneider Electric will provide them with advice on setting up an industrial plant and testing.

The Group is also working with public and private funding bodies. It intends to cover the full range of needs with capacities up to 500 kW enough to power a city of 10,000 inhabitants in Africa through its standardised solutions, and from 500 kW to 20 MW through specific architectures for cities of several hundred thousand inhabitants that are without an electricity grid.

The potential for electrification is enormous, not only in rural areas but also for companies who would like their own reliable electricity grid, including banks and their network of agencies and cash dispensers, food and beverage manufacturers, data centres and even electricity providers that currently use power generators and need to switch to hybrid energy production with mini-grids. ■

Signify partners with Diamond Developers for transformation of Sustainable City

(Left to right) Goktug Gur President and CEO of Signify Middle East, Turkey and Pakistan; and Faris Saeed, CEO of Diamond Developers.

Signify Euronext, global vendor in lighting, and Diamond Developers, the real estate developers of fully sustainable communities, have signed a memorandum of understanding as part of their mutual commitment to utilise creative and innovative technologies and solutions designed to promote sustainability. The signing took place at Sustainable City, a Diamond Developers project and the first fully sustainable community of its kind, modeled to become an international showcase for high quality sustainable living. The agreement is a testament to a collaborative approach that seeks to accelerate innovation in sustainable energy and vertical farming.

The agreement is built on two pillars of collaboration; the first pillar is centered around providing the latest advanced lighting solutions and innovations that contribute to the city's green branding and drive its overall sustainability. As the lighting company for the Internet of Things, Signify aims to utilise its IoT platform, Interact, to deliver new data-enabled services to expand its value from lighting products to systems and services, offering new capabilities to unlock the extraordinary potential of light within sustainable cities.

The second pillar focuses on horticulture solutions, in which Signify distinguishes itself through a customer-centric approach, where a plant specialist and application engineer work together to offer the grower a business case, financial services, plant growth expertise, installation expertise, LED systems and community networking.

Innovative farming technologies, such as LED lighting, now make it possible to grow plants in indoor environments without sunlight. Vertical farming is a reply to the environmental problem that exists today in horticulture, how to provide fresh food to urban environments in a way that's efficient and sustainable. Using lighting provided by Signify, customers can grow and process consistent, high-quality produce in one location in a vertical farm that can be close to retailers and consumers. The idea is to push boundaries to deliver quality products to consumers in a sustainable way.

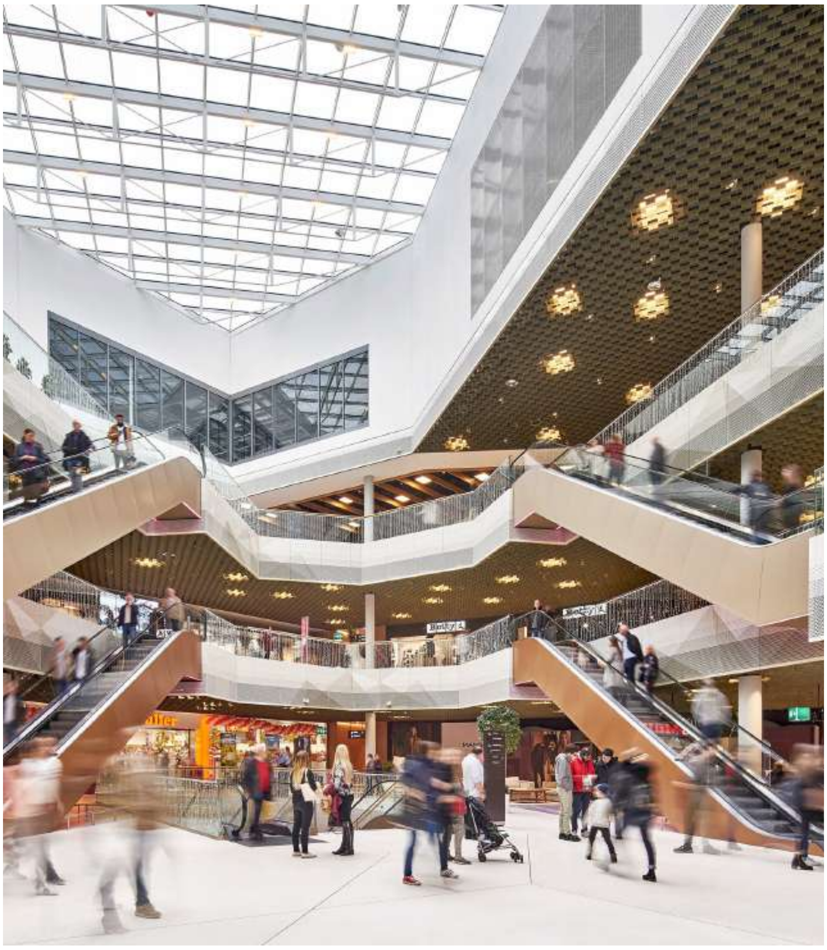
The Sustainable City in Dubai is born from a vision to accelerate the transition towards sustainable development. The Sustainable City demonstrates the living, working proof of this future ready concept and acts as a benchmark for sustainable living. Located in Dubailand, the mixed-use development spans some 46 hectares and provides an array of green residential facilities and amenities with no negative impact on the environment.

A unique concept which redefines sustainable living; offering energy efficient housing, with net zero energy impact, zero maintenance and low service fees, green education and health care and a host of indoor and outdoor leisure and wellness activities, an urban farm, green mosque and innovation center.

The partnership is in line with Signify's strategy and purpose to unlock the extraordinary potential of light for brighter lives and a better world and its commitment for sustainable revenues and operations across the globe. ■

BT to provide intelligent global network for Schindler using IP Connect

BAS BURGER, CEO Global BT.



BT will provide Schindler with a reliable and secure network and voice solution connecting about 500 sites worldwide.

BT announced it has signed a contract with Schindler, a global provider of elevators, escalators and moving walkways, as well as maintenance and modernisation services. BT will provide Schindler with a reliable and secure network and voice solution connecting about 500 sites worldwide.

BT will deploy and manage a consolidated global network infrastructure for Schindler, connecting their data centres, offices, factories and contact centres globally. BT will use IP Connect, its secure network service and a global Internet solution. This will remove the complexity of dealing with a multitude of network operators. It will offer Schindler better visibility of cost and performance as well as improved end-to-end service quality.

Matteo Attrovio, Chief Information Officer, Schindler Group, said, “A global, secure, integrated network is a crucial element of our digital strategy. It will allow us to move from a fragmented network of suppliers to a global provider who can offer a fully managed, high quality end-to-end network service.”

Bas Burger, CEO of Global BT, said, “We are proud to have been chosen by Schindler as a trusted advisor on their digital transformation journey. Schindler is a fast-growing, global company, and we are happy to support them with our services and expertise all around the globe. Schindler moves more than one billion people every day, and it is fantastic that we can support them in providing a safe and secure service.” ■

Etisalat Digital, FAB, Avanza, spearhead blockchain to detect UAE finance fraud

EEtisalat Digital, in partnership with First Abu Dhabi Bank and Avanza Innovations, have developed UAE Trade Connect UTC, a new nationwide platform that will use the latest disruptive technologies to digitise trade in the UAE. The initial phase will focus on addressing the risks of double financing and invoice fraud before turning to other key areas of trade finance.

UTC is aimed at driving digital transformation of trade in the UAE by enabling banks, enterprises and governments to collectively benefit from innovations such as blockchain, artificial intelligence, machine learning and robotics. Seven major UAE banks, in addition to FAB, have joined the nationwide platform.

The agreement to develop the solution was signed by:

- Salvador Anglada, Group Chief Business Officer, Etisalat
- Manoj Menon, Head of Global Transaction Banking, First Abu Dhabi Bank FAB
- Sumit Aggarwal, Executive Vice President and Group Head, Transaction Banking Services, Emirates NBD
- Hassan Al Redha, General Manager, Institutional and Transaction Banking, Commercial Bank of Dubai
- Ahmed Abdelaal, Executive Vice President, Mashreq
- Devid Jegerson, Head of Customer Experience and Platform Development, National Bank of Fujairah
- Peter England, CEO of RAKBANK
- Haytham Elmaayergi, Global Head of Transaction Banking, Abu Dhabi Islamic Bank
- James Greenwood, Chief Operations Officer, Commercial Bank International

Etisalat Digital along with the eight banks will form a working group to further develop and extend the solution to other areas of trade. This nationwide platform, which is open for all UAE banks to join, will safeguard banks from potential fraud losses through advanced detection tools, allowing them to extend additional financing to their corporate clients. ■

Restructuring veteran Othman Al Ali joins Emirates Water Electricity as CEO

Othman Al Ali has been appointed Chief Executive Officer of the Emirates Water and Electricity Company, a leading company in the coordination of planning, purchasing and providing of power and water across the UAE. Othman joins from the Federal Electricity and Water Authority FEWA, where he was Chief Financial Officer. He has almost two decades of experience in both the private and public sectors, having held various positions in the utilities and banking industries across a number of federal government entities.

Consensys Capital founder Andrew Keys joins DARMA Capital as Managing Partner

Andrew Keys has joined DARMA Capital as Managing Partner. Prior to DARMA Capital, Andrew co-founded ConsenSys Capital. He also served as Head of Global Business Development for ConsenSys, the largest Ethereum software engineering company in the world. During Andrew's tenure at ConsenSys, his responsibilities included teaching central banks and Fortune 500's the importance of blockchain technology in digitising the global economy. Andrew also co-created the first Ethereum Blockchain-as-a-Service offering with Microsoft and helped start the Enterprise Ethereum Alliance EEA.

Julie Sweet to lead Accenture as CEO driving innovation, inclusion, diversity

Accenture's board of directors announced that Julie Sweet has been appointed Chief Executive Officer. David Rowland, currently interim Chief Executive Officer, has been appointed Executive Chairman. Marge Magner, currently non-executive chair of the board, will resume her role as lead independent director. Julie Sweet, 51, is currently Chief Executive Officer of Accenture in North America, the company's largest geographic market, representing almost 50% of Accenture's global revenues. As a member of Accenture's Global Management Committee for nearly a decade, Sweet has played an integral role in the company's business and investment strategy.

Phil Brace moves to Veritas from Seagate to drive software defined storage

Veritas Technologies, a global vendor in enterprise data protection and software-defined storage, announced the appointment of Phil Brace as Executive Vice President. Brace will lead Veritas' Appliances and Software-defined Storage business. Brace is an accomplished technology leader with more than 25 years of experience in engineering, product, and general management roles. He comes to Veritas from Seagate Technologies, where he served most recently as President of the Cloud Systems and Silicon Group responsible for the Storage Systems Business and solid-state drive product divisions.

SUCCESSFUL TRANSFORMATION ENABLED BY CYBERSECURITY

While CISOs face technology, cultural, operational challenges inside their business, no successful transformation strategy can be rolled out if the cyber security strategy is added as an afterthought.

(Left to right) Ammar Enaya, Regional Director, Middle East and Turkey, Vectra; Fabio Picoli, Managing Director, Gulf Cooperation Council, Trend Micro; Jay Townsend, Principal Booz Allen Hamilton; John Hathaway, Regional Vice President, Middle East and India, BeyondTrust; Mohammad Jamal Tabbara, Senior Technical Sales at Infoblox; Nasser Bostan, Head of IT Security Practice, Middle East, Africa and India, BT; Nicolai Solling, CTO, Help AG; Rajesh Ganesan, Vice President, ManageEngine; Sheikh Shadab, Associate Director Cyber Security, KPMG; Tarek Kuzbari Regional Director Middle East, Bitdefender.

AMMAR ENAYA,
Regional Director,
Middle East and Turkey, Vectra.

SECURITY IS A SHARED ISSUE ACROSS THE ENTERPRISE

Digital transformation demands a grass roots review and analysis of what new risks transformation will create.

Technology, particularly around mobility and communications, has moved IT beyond a simple utility service, to becoming a source of strategic value creation, sustainable competitive advantage, and a contributor to the management of risk. Technology is a prime enabler of business agility and provides the opportunity to innovate, and delight customers, stakeholders, and citizen by enabling new ways to work, interact, and live.

Digital transformation is where an organisation implements strategic change through the adoption of new technologies, organisational structures, and operations. It is often driven by the need to adapt to new operating environmental norms.

An organisation's digital transformation drives security transformation too. New ways of organising, working, new systems, and particularly new equipment all bring changes that can include new vulnerabilities and an extended attack surface.

KEY TAKEAWAYS

- An organisation's digital transformation drives security transformation too.
- New ways of organising systems and equipment bring changes that can include new vulnerabilities and an extended attack surface.
- Digital transformation invariably demands a grass roots review and analysis of what new risks transformation will create.
- Security should be an integral element of the transformation project planning, not a consequence of it.

> AN ORGANISATION'S SECURITY POSTURE IS NOT A STATIC THING AND GROWS AS IT DEALS WITH INTERNAL, EXTERNAL CHANGES.

With an influx of IoT and mobile devices, CISOs need to ensure they can exert appropriate controls, based on their policies, on these devices wherever possible. And, as devices often get deployed without announcement to security teams, as minimum they need to be able to identify and monitor them for suspect and malicious behavior.

CISO's should also be mindful of the increased value their organisation will be placing on data, and so its management, use and storage will almost certainly have compliance requirements to consider.

Too often security is seen as inhibitive by their internal stakeholders. CISOs need to be trusted advisors that partner with the lines of business, having shared discussions about risk, and being part of the solution that appropriately secures new business initiatives.

In progressive organisations, cybersecurity is not just seen as a technology and policy issue. Security has to be a shared issue across the enterprise. This changing of organisational mindset is not easy, takes time, and requires an adept CISO who can move, influence and carry respect in both the business and security and risk domains.

Digital transformation invariably demands a grass roots review and analysis of what new risks the digital transformation will create, the organisation's risk appetite for them, and the identification of acceptable risk management approaches.

In fact, security should be an integral element of the transformation project planning itself, not as a consequence of it. New security capabilities may often be needed and require resourcing. An organisation's security posture is not a static thing, it needs to adapt and grow with the organisation as it deals with both internal changes and shifts in the external environment.

Finally, end customers want solutions that work, deliver on their promises, and make work easier. ■

FABIO PICOLI,
Managing Director GCC,
Trend Micro

WHY CISOs CONTINUE TO FACE INCREASING PRESSURE

Managing the complexity and volume of disparate security solutions that do not integrate can become a daunting task.

Government-led digital transformation initiatives are catalysing the adoption of cybersecurity in both public and private sectors. While GCC boardrooms are knowledgeable about cybersecurity, the cyber skills gap is holding them back.

Numerous organisations from the public and private sectors are digitally transforming. For example, organisations are increasingly moving to the cloud to optimise IT costs, maintain business continuity, scale up as their business grows, and foster new levels of collaboration and communication. However, moving to the cloud presents its own set of cybersecurity challenges, which require cloud-based security solutions.

Few GCC organisations know how to protect their cloud infrastructure, which is different from securing physical servers. Regional organisations are increasingly moving to hybrid cloud environments, which requires that they protect both on-premise and cloud infrastructures simultaneously. Securing data migration can be a complicated process. Researchers predict that cloud misconfiguration in data migration could lead to more data breaches in 2019.

Digital transformation comes down to three key factors: security efficacy, operational efficiency, and business enablement.

CISOs need to monitor and communicate cyber risks and implement technical controls and countermeasures. CISOs also need to put together the right personnel, skills, and processes. Organisations should eliminate process bottlenecks and ensure they can operate at peak performance. Organisations often connect their IT systems with third party systems to boost productivity. CISOs need real-time visibility to monitor business complexity and mitigate risk.

In discussions with CISOs, their biggest challenges include: empowering staff while mitigating risk; automating security processes to enhance incident response; increased regulatory pressure; an endless shortage of cybersecurity skillsets; technology vendor consolidation; and the rise in shadow IT expanding the threat landscape.

CISOs need to set the cybersecurity strategy for the organisation. While some tasks can be offloaded to an external cybersecurity vendor, such as detection and response responsibilities, CISOs do need to understand the latest threats and trends out there, and also keep themselves updated on the newest technologies and how to integrate them into the existing IT infrastructure. The most pressing cyber threat challenges require a deep understanding of the issues.

As the IT environment becomes more complex, an organisation's security stash can grow bloated. A typical organisation has an average of 15-20 cybersecurity solutions in place, and many of them are from different vendors. This has led to issues like visibility and management nightmare. Today, we are already seeing a bevy of organisations starting to request for integration – for these solutions to talk to each other and exchange threat information. In the near future, we will continue to see this happen not only in UAE, but also globally.

GCC organisations are looking for a different security approach that encompasses endpoint, network, and hybrid cloud security. ■

KEY TAKEAWAYS

- A typical organisation has an average of 15-20 cybersecurity solutions in place, many from different vendors.
- Organisations should focus on hiring CISOs who can stop cybercriminals by closing gaps in IT infrastructure.
- Digital transformation comes down to three factors: security efficacy, operational efficiency, business enablement.
- Managing the complexity of disparate security solutions that do not integrate can become a daunting task.

JOHN HATHAWAY,
Regional Vice President,
Middle East and India,
BeyondTrust.

TRANSFORMATION IS COMPLICATING SECURITY POSTURE

The challenge is to enable and not restrict the productivity of the businesses that are being protected.

With the rapid increase in the attack surface, CISOs are left with the almost impossible task of manually managing privileged accounts and assets. For some organizations, digital transformation might mean embracing cloud technology, for others it may be the need to develop strong DevOps capabilities, and for still others it may be the need to plan for a wide adoption of IoT devices.

It is likely however, most CISOs will have to plan for a combination of all of these things. If you stand still, then this new digital world will consume you.

The role of CISOs has often come up in the boardroom. Their influence in this environment and the rest of the organisation is now critical to ensure security policies are adopted and followed. The best CISOs have a plan and are not afraid to make decisions that will ensure they are not the subject of a costly and embarrassing breach.

KEY TAKEAWAYS

- The challenge is to enable and not restrict the productivity of the businesses that is being protected.
- Top CISOs are not afraid to make decisions that will ensure they are not the subject of an embarrassing breach.

SOLUTIONS THAT HAVE BEEN MADE TO LOOK MODERN BUT BUILT ON A BACKBONE THAT DATES BACK 15 YEARS, WILL STRUGGLE.

It is easy to point fingers when things go wrong but, in the world, we live in today, it is more complex than ever before. Take a DevOps environment. The development team will typically use high powered credentials, architecting business critical applications and processes in a cloud-based environment and sometimes production environments as well. The challenges this present to a CISO are enormous.

How do they balance the productivity of the business with the controls they require to deliver security? The huge increase in wearables, mobile and intelligent devices present an equally large problem. How do you control what is brought into the corporate environment, how do you protect it, how do you ensure you are meeting strict compliance mandates?

Digital transformation complicates the security posture. The world that's been protected prior to the transformation was understood and quantifiable. It is now a world where solutions have to be dynamic, flexible and built for huge scale. The strategy, budget and ability to execute has to be right or the organisation will be at risk to attack.

Those solutions that have been made to look modern but built on a backbone that dates back 15 years, will struggle. Innovative products that solve the problem of speed, agility, visibility, control and protection will become those which solve the problems created by the modern world. The challenge is to enable and not restrict the productivity of the businesses that is being protected.

End users have to find a balance in their organisation to protect and not constrict, whilst facing a maelstrom of cyber-attacks. ■

*MOHAMMAD JAMAL TABBARA,
Senior Technical
Sales, Infoblox.*

CISOs FACE CHALLENGES OF BUY-IN, SKILLS INCOMPETENCE

Technology challenges of legacy networks are coupled with human resource challenges in meeting digital demands.

Today the world is getting more connected. Organisations are connecting traditional aspects of their business with the Internet. Trends such as digital transformation, IoT, smart cities, connected OT, BYOD, and more are bringing unprecedented cyber threats.

It is not unusual to deal with prospects that either suffer from lack of skilled personals or lack of budget. Making these limitations, two of the main challenges that could slow the business a little.

The lack of talented skillsets is usually due to, insufficiency in the number of human resources in the cybersecurity buying centre, or due to a poor buy-in from the C-level executives pertaining to cyber security.

The budget challenge can be either a lack of funding or lack of proper project prioritisation. The organisation might be spending their limited budget on projects that can wait, and putting on hold vital projects that can alleviate many of the unrecognised lurking threats or potential destructive breaches.

Digital transformation is reshaping the business landscape faster than ever before. Organisations that ignore this will struggle and rapidly lose customers and market share. This transformation has introduced many new technologies. All of them have one thing in common, they are network-centric.

Legacy networks are not aligned well with today's business needs. Digital businesses need to ensure network and service availability, manage risk, improve operational efficiencies, by using actionable network intelligence.

A successful digital transformation cannot happen without security. Cyber security is one of the essential aspects of digital transformation. You can transform to digital business only if your network services will allow it. To meet exploding digital demands, your network must be highly available, adaptable, easy to manage, resilient, and secure.

Data theft and malicious infiltration are two challenges for a CISO. Yet the biggest challenge of all time is talent incompetence and lack of awareness. Mainly blind spots in security start when the safety of the existing running services and protocols are taken for granted, or when the cyber security individuals are oblivious from the latest threats or the potential misuse of the available services.

Absence or lack of adherence to a cybersecurity and data governance framework will impose a threat to the organisation as a whole along with its supply chain, customers, partners.

Skilled talents are what industry leaders should prioritise. Today many organisations are acquiring state-of-the-art cyber security solutions that cost massive budget, yet the human resources operating these systems lack the skills and motivation to make the most of these systems, leaving gaps open for malicious vulnerabilities and misuse.

End user organisations are commonly looking for integrated cybersecurity solutions. Channel partners need to identify the current cybersecurity trends and regional initiatives at first, and then offer integrated solutions that form an orchestrated ecosystem to their prospects. ■

KEY TAKEAWAYS

- Legacy networks are not aligned well with today's business needs.
- Digital businesses need to ensure network availability, manage risk, improve efficiency.
- A successful digital transformation cannot happen without security.
- To meet digital demands, networks must be available, adaptable, easy to manage, resilient, secure.
- Data theft and malicious infiltration are two challenges for a CISO.
- Biggest CISO challenges are talent incompetence and lack of awareness.
- Blind spots in security start when safety of existing services and protocols are taken for granted.

NASSER BOSTAN,
Head of IT Security Practice,
Middle East, Africa and India, BT.

IMMENSE PRESSURE TO TRANSFORM AND SECURE AS WELL

End users and channel partners are increasingly managing the complexity of installed cyber security solutions.

Digital technology is moving at a dizzying pace. As users, we have adapted to that pace. And we want to interact with companies and providers via the channel most convenient to us. Businesses need to adapt to this change by embracing digitalization focusing on the things that matter most.

Digital transformation is therefore the change from a traditional legacy business model and technical architecture, processes and systems to a business model and technical architecture that enables evolving business outcomes in a rapid and agile way. Digital transformation is driving business transformation which is driving business growth.

The most important technology elements are security, reliability, integration and cost effectiveness. Agility and scalability come lower on the list, even though the ability to flex, respond and scale rapidly are still core competences of successful digital businesses

The Chief Security Officer must weigh this against the need for security and provide a level of protection and resiliency that corresponds with the need for digital transformation. Combine this with conflicting needs of the CISO versus the CIO and CFO, and the challenge becomes even bigger

Businesses wants to make greater use of the cloud, but each new platform brings more complexity and potentially expands the attack surface. And if the organisation is adopting software defined network in response to greater bandwidth demands, it could inadvertently be creating even more vulnerabilities unless fully thought through. The team may not have all the skills required to protect an expanding hybrid environment.

Increasing and ever-changing regulations and knowing if the organisation is compliant with them is impossible and even basic system hygiene is difficult when the CISO does not know all the devices connected to the network and the cloud.

Signature-based security is no longer sufficient. Not all attacks will be caught at the firewall. The challenge is not just about the cloud and the connection to it. It is about having a comprehensive approach that considers what security is throughout the infrastructure.

As cloud adoption increases, regulations become more stringent, the convergence of IT and OT environments continues and with the rise of the IoT, customers are increasingly having to act as integrators with large in-house security teams to make sense of the vast landscape of vendors and products on the market.

With the exception of a few, most vendors are interested in pitching their product with little thought given to how their solution would affect the customer's overall security posture. However, increasingly vendors understand that working through a partner, with the ability to provide the integration skills and knowledge that customers are looking for, is the way forward. ■

KEY TAKEAWAYS

- Digital transformation is driving business transformation which is driving business growth.
- The most important technology elements are security, reliability, integration and cost effectiveness.
- Knowing if the organisation is compliant is impossible when the CISO does not know the devices connected to the network and the cloud.
- Customers are increasingly having to act as integrators with in-house teams to make sense of the landscape of vendors.

> MOST VENDORS ARE PITCHING PRODUCTS WITH LITTLE THOUGHT ABOUT HOW THEIR SOLUTION WOULD AFFECT THE CUSTOMER'S OVERALL SECURITY POSTURE.

NICOLAI SOLLING,
CTO Help AG.

VENDOR CLUTTER ADDING TO CISO's TRANSFORMATION CHALLENGES

Delayed integration of cyber security strategy and vendor noise are adding to CISO's transformation challenges.

The rapid and exponential growth of the cybersecurity industry has resulted in a crowded playing field. Today, every vendor claims to have the latest and greatest solution and there's plenty of overlap between what different technology providers offer.

This has the potential to overwhelm CISOs and IT decision makers, resulting in long drawn sales cycles and ultimately resulting in investments being made into domains that do not necessarily address the most critical threats businesses actually face.

While from a technology standpoint, undertaking digital transformation is not necessarily challenging, complexity and risk are introduced when cybersecurity is overlooked. The same solutions and processes that facilitate digital transformation can be the root cause of business disruption. There are countless examples of this, with the most recent ones being Capital One, Marriott, and Equifax.

Historically, CISOs have adopted a rigid approach to keeping their organisations and users protected. This has often resulted in cybersecurity technologies and processes becoming a hindrance or burden to businesses.

Today, with tech-savvy employees and customers, this mindset simply does not work. Restrictions will be circumvented as is evident from the ever-present challenge of shadow IT. CISOs must therefore cultivate the ability to really understand the business requirements of the users they serve and then identify how they can facilitate the necessary workflows without impacting security. Ultimately, CISOs must ensure that cybersecurity becomes an enabler, rather than an inhibitor of business.

Vendors that we consider to be leaders are not just those that are identified as such by industry research firms. Rather they are the providers that demonstrate a clear understanding of the market needs and address these with technology roadmaps that also serve to future-proof investments.

A bigger driver is the fact today, more than ever, IT is a fundamental enabler of business. Competitive differentiation in business today is inextricably linked to innovation. For this reason, we see plenty of organisations moving away from legacy models and adopting a digital approach to running their businesses and engaging with their customers. As technology becomes more and more important to deliver the best service, enterprises are slowly moving away from being businesses that operate technology, to technology companies operating businesses.

In short, the decisions you make regarding your IT investments today, will determine whether your business remains successful or not. Unless you work to establish the right technology platforms, you will not be able to rapidly adapt to ever changing customer demands, which will result in them moving away to competitors that have primed themselves for change. ■

RAPID GROWTH OF THE CYBERSECURITY INDUSTRY HAS RESULTED IN A CROWDED PLAYING FIELD.

KEY TAKEAWAYS

- Every vendor claims to have the greatest solution and there is overlap between what technology providers offer.
- The decisions you make regarding IT investments today, will determine whether your business remains successful or not.
- Unless you work to establish the right technology platforms, you will not be able to rapidly adapt to customer demands.
- From a technology standpoint, undertaking digital transformation is not necessarily challenging.
- Complexity and risk are introduced into digital transformation when cybersecurity is overlooked.
- The same solutions that facilitate digital transformation can be the root cause of business disruption.

RAJESH GANESAN,
Vice President,
ManageEngine.

DATA FLOW ENABLING TRANSFORMATION, CHALLENGE FOR CISOs

Transformation must deliver value, decentralisation, customer experience, coupled with the free flow of data.

Technology is bringing about some profound and irreversible changes to how businesses operate. Because of the proliferation of consumer technology, users expect the same experience and ease of use with technology used in the business. This augurs well for the business where adoption of their new solutions becomes easy with less efforts to promote and train users.

Technology also fosters a model where a business can truly operate in a decentralised model, yet not compromising on the centralised spirit and culture, by closing the gaps in communication and collaboration. Technology application has also become inevitable for businesses to respond to external factors like a new law or regulation coming into force and the business mandated to comply. These are factors where technology plays a very strategic role for driving business growth and building differentiation.

Businesses realising the need to go through a transformation often focus on the following three aspects. The first is the value transformation where the business has to invent a completely new business model that offers more value at less cost and is relevant to the current day and age.

KEY TAKEAWAYS

- The downside is making all this work together, so that the sum of the parts is far greater.
- Number of externally originating attacks far outnumber internal incidents.
- The consequences of internal attacks far outweigh the external ones.
- Any business transformation should start at fundamentals and then look at how to leverage current technology.

> THE UPSIDE REALLY IS WITHOUT THE SECURITY SOLUTIONS, IT IS IMPOSSIBLE TO RUN OPERATIONS SECURELY.

The second is the ability to operate in a otally decentralised fashion, yet the overall performance of the business should be optimal and meet the stated objectives. The third would be the unrelenting focus on understanding the changes in customer expectations and doing every bit to enhance it every day.

Any business transformation should start at such fundamentals and then look at how to leverage the best the current technology has to offer to enable the transformation. Blindly falling for the hype of a new technology and trying to force fit it into the business operations is a recipe for disaster.

For CISOs, every day is a new challenge as technology now enables business data flow freely beyond boundaries. Though the business goals demand such availability of data, any mishap could result in a severe consequence for the business.

Though the number of externally originating attacks far outnumber the internal incidents, the consequences of internal attacks far outweigh the external ones. Sophisticated technologies exist to detect and prevent external attacks to a great degree but when privileged insiders having direct access to data and controls, decide to act up, it is hard to address this problem only through technology.

It is imperative for business to collect, store and process personal data of millions of their customers and this is precisely why business data comes under targeted attacks. Individual, societies and countries around the world demonstrate different outlook towards how they see and approach privacy.

With personal data flowing freely around and with new laws coming into force that hand out severe punishments for violations, executing privacy by design and educating about it upto the very last person, is a very important challenge for the business and increasingly, this is falling in the laps of the CISO. ■

SHEIKH SHADAB,
Associate Director
Cyber Security,
KPMG.

SECURING DIGITAL SYSTEMS HERCULEAN TASK FOR CISOs

CISOs are under pressure with data being leveraged across the digital enterprise and stricter regulatory compliances.

Traditionally, data and systems had perimeters and it was easier to manage their security. In the increasingly digital world, systems and data have fewer boundaries. They are accessible from anywhere and everywhere, over cloud, mobile, Internet of Things. Securing systems and data in this extended perimeter is a herculean challenge for most of the CISOs.

The key enablers driving adoption of cyber security are regulatory changes, growing awareness at top management of the threat landscape and increasing adoption of digital transformation as a journey by more and more organizations.

Technology should be an enabler to business capabilities rather than simply a cost center. It should enable businesses to increase connectivity, enhance customer experience, automation and predictive analytics. Digital transformation is a journey which should be measured by the enhanced customer experience and automation.

THE ENABLERS DRIVING ADOPTION OF CYBER SECURITY ARE REGULATORY CHANGES, AWARENESS AT TOP MANAGEMENT, ADOPTION OF DIGITAL TRANSFORMATION.

In today's digital world, key skills expected from every CISO are an understanding of the business and the ability to communicate the cyber security challenges in a business language.

The introduction of a new wave of technologies has created tremendous opportunities for technology, as well as consulting vendors in terms of helping businesses adopt and customize these technologies to their business needs. At the same time, this has created challenges in terms of the security of these technologies, compliance to the regulatory requirements, data privacy, technology awareness of the business users.

The upside would be that cyber security solutions from vendors drastically reduce the implementation timeline. A downside is that every new cyber security solution from vendors may create a new set of challenges for business users to adapt to its functionalities.

A typical product portfolio in cyber security should help businesses better identify cyber risks, implement necessary controls to better manage cyber risks and respond fast to a situation in case of any cyber security incident.

The expectations of channel partners are to be able to address a specific business requirement, provide long term support and maintenance, and deliver technology specific trainings.

The expectations of end customers are to be able to innovate to keep up with the evolving threat landscape and technology changes, provide long term support and maintenance, and deliver technology specific trainings. ■

KEY TAKEAWAYS

- Technology should be an enabler to business capabilities rather than simply a cost center.
- Digital transformation is a journey which should be measured by the enhanced customer experience and automation.
- The expectations of channel partners are to be able to address a specific business requirement.
- The expectations of end customers are to be able to innovate while keeping up with evolving threats.

TAREK KUZBARI,
Regional Director
Middle East,
Bitdefender.

CAN CISOs REDEFINE THEMSELVES IN DIGITAL TRANSFORMATION

There is no doubt that digital transformation is key to future innovation, provided security threats are managed by CISOs.

As the pace, scale, and impact of technological innovation and disruption have exponentially escalated, technology has become a primary influence on business strategy and value-creation models.

CISOs, as technology leaders, have a tremendous opportunity to be relentlessly proactive in identifying how technology can create new value for the business. There is widespread recognition among leaders in most industries that the role of digital technology is rapidly shifting, from being a driver of marginal efficiency to an enabler of fundamental innovation and disruption.

Digital is reimagining the human experience. Most companies recognise that they cannot turn a blind eye to such a powerful force shaping human behavior. What worked yesterday to attract, engage, and retain customers may be fast becoming obsolete.

Digital transformation is the strategic adoption of digital technologies to improve processes and productivity, manage business risk, and improve customer service.

During the last couple of years, most enterprises have been accelerating the pace of their digital transformation, based on the adoption of leading-edge ICT technologies like cloud and edge computing, Big Data and the Internet of Things. At the same time, organisations are still suffering from security attacks, which are amongst the most critical barriers in the implementation of their digital transformation agendas.

As organisations pursue digital transformation and adopt new technologies and business processes, we can expect to see a corresponding increase in security related issues and concerns. New technologies, such as IoT and multi-cloud environments, have dramatically increased the attack surface and the number of entry-ways into a network.

DIGITAL TRANSFORMATION IS THE STRATEGIC ADOPTION OF DIGITAL TECHNOLOGIES TO IMPROVE PROCESSES, PRODUCTIVITY, BUSINESS RISK, CUSTOMER SERVICE.

In speaking with top CISO leaders in the Middle East, the following challenges seem to be top of mind for most: increased surface and sophistication of attacks, skills shortage, government regulations and compliance, budget, resistance to change, amongst others.

As enterprises race towards digital transformation, CISOs must redefine their role in the digital business team. By enabling infrastructure agility and visibility, they can create business value and become a trusted partner. Critical skills would include: communication skills, collaboration and conflict management skills, decision making skills, planning and strategic management skills, incident management, knowledge of regulation and standards compliance, risk assessment and management.

Despite the promise of digital transformation to drive business initiatives, security concerns are a primary worry for technology executives at the helm of these projects.

Digital transformation is altering security needs in some fundamental ways. It is expanding the attack surface, increasing the potential for organisational damage and as a consequence making it imperative for organisations to take a continuous improvement approach to security. Cybersecurity defenses and processes need to be continuously monitored and evolved to adapt to the changing threat landscape. ■

IMPROVING CYBERSECURITY BY USING EQUATION OF RESILIENCY

Using a three-pronged approach of risk management, continuity, testing, businesses can reduce the impact of cyberattacks and incidents.

*JAY TOWNSEND,
Principal, Booz
Allen Hamilton.*

*ROSA DONNO,
Senior Associate,
Booz Allen Hamilton.*

Business leaders have always looked to implement new technologies and innovations to enhance their day-to-day operations and gain competitive advantage. First our phones became smart, then buildings, and now entire cities. Through these technological advancements, our entire world has reached unprecedented levels of connectivity, with systems, people, and processes all intertwined and continuously improving as part of a global feedback loop, which in turn accelerates the next technological leap.

However, while this degree of interconnectivity has enabled great strides in sectors and industries worldwide, it also amplifies an organisation's exposure to risk and the severity of the incidents they face. Cyber risk factors now plaguing our digital age are often conspicuously missing from the top of corporate strategic agendas.

One reason for this is that technological advances have, in some cases, transformed the business landscape so quickly that leaders are yet to develop a deep understanding of precisely how their particular business is exposed to cyber threats and their impact. In other cases, organisations have not yet been stung hard enough by cyber-attacks for resilience to been seen as a strategic priority.

Nevertheless, resilience should be an integral part of the cyber strategy and should permeate day-to-day operations. Organisations need to build awareness of the importance of resilience and the need for it to be integrated seamlessly across all plans, activities, and systems relating to their risk management programmes. As a major denominator in resilience, cyber risk factors need to be integrated within the organisation's risk management, continuity management and testing and exercises programmes and systems.

Where cyber risks are concerned, resilience can be built through a two-way approach: top-down and bottom-up. A top-down-approach integrates cyber risk factors within the Resilience Equation, while a bottom-up approach considers business and corporate resilience through a number of cybersecurity functions.

The top-down approach focuses on integrating cybersecurity factors into the risk management, continuity management, and testing and exercises programmes or systems.

As a first step, the organisation integrates cybersecurity factors within its risk management programmes. It then assesses the potential of various cyber risks on overall business before developing a clear understanding of how particular risk factors would affect specific operations.

The bottom-up approach centres on injecting business resilience requirements through five cybersecurity functions: identify, protect, detect, respond, and recover. IT professionals within the organisation should also apply the resilience guiding principles, redundancy, buffering, and adaptiveness in day-to-day activities.

WHAT IS THE RESILIENCE EQUATION?

No organisation will ever be impervious to risk, but by building resilience it is possible to mitigate the severity of threats and bounce back when a negative event occurs. To become

RESILIENCE EFFORTS SHOULD BE INFORMED THAT NETWORKS ARE COMPRISED OF INDIVIDUAL NODES THAT MAY OPERATE INDEPENDENTLY.

THERE MAY BE MANY PATHS TO FAIL, THERE ARE ALSO MULTIPLE WAYS FOR A NETWORK TO QUICKLY HEAL ITSELF.

resilient, organisations must be aware of their future threats and current weaknesses, and they must take informed strategic and tactical decisions in order to prepare for risks and respond effectively to internal and external events.

Building resilience involves decreasing the likelihood of disruptive events and managing the consequences when such events do occur, as the following equation illustrates:

Resilience = Identifying risks and tackling their likelihood + Managing consequences of disruptive events

Resilience = Risk Management + Continuity Management + Testing and Exercises

By proactively managing risk, the Resilience Equation protects the mission and reputation of an organisation. Furthermore, by establishing an effective continuity system, organisations can ensure that essential functions are restored in time when disruption or disaster strike. Meanwhile, through systematic exercises, strategic options, and tactical plans can be rigorously tested so that any entity–no matter how big or small–can be ready for the unforeseen.

The risk landscape is more complex and dynamic than ever, but it is not insurmountable. For mission success in today's world, organisations must embark on a journey to build their defenses–a journey that begins with the implementation of the Resilience Equation.

Here, risk management looks at how to assess threats, vulnerabilities, and impact in order to prioritise and mitigate risks, while continuity management focuses on mission execution and begins with acceptance that some disruptions will inevitably succeed and some functionality will be lost as a result.

In addition to assessing threats and weaknesses, any resilience building efforts should also be informed by the understanding that networks are comprised of many individual nodes that may operate independently. So, while there may be many paths to expose vulnerability and many ways to fail, there are also multiple ways for a network to quickly heal itself.

Testing and exercises provide continuous review and assurance of the effectiveness of the internal control system as well as an opportunity to practice and evaluate organisational preparedness in a simulated and controlled environment.

Through testing and exercises, eventual gaps or control deficiencies are identified and mitigated; they also provide an opportunity for organisations to practice and evaluate their preparedness in a simulated and controlled environment. The information gathered from these exercises may then be used to further refine resilience, emergency, and continuity plans.

Through a mix of virtual and augmented reality, various scenarios, such as earthquakes, tsunamis, and fires are simulated, and resilience is tested to ensure networks, systems, and staff are responding to stress and disruption as expected. ■

Excerpted from, The Resilience Equation by Booz Allen Hamilton.

KEY TAKEAWAYS

- Cyber risk factors now plaguing our digital age are missing from the top of corporate strategic agendas.
- Leaders are yet to develop an understanding of how their business is exposed to cyber threats and their impact.
- Organisations have not yet been stung hard enough by cyber-attacks for resilience to been seen as a strategic priority.
- Organisations need to build awareness of resilience and the need for it to be integrated across systems.
- Cyber risk factors need to be integrated within the organisation's risk management, continuity management and testing systems.
- Testing and exercises provide review of the effectiveness of the internal control system.
- Testing and exercises provide an opportunity to evaluate preparedness in a controlled environment.

HOW ETIHAD ESCO IS TRANSFORMING RETROFITTING OF ENERGY SERVICES

Versatile solutions, innovative technologies, back to back delivery, competency in energy project management, are boosting Etihad ESCO's role in the energy services retrofitting business.

BY: ARUN SHANKAR

Etihad Energy Services Company or Etihad ESCO was started in 2013. In 2015, Etihad ESCO started its first retrofitting project. In 2016 the first project was executed and completed. And finally, in 2017, projects started rolling. Reflects, Ali Mohd Al Jassim, Chief Executive Officer at Etihad ESCO, "The boost started at the end of 2016 and into 2017. Since then we have had, three flourishing successful years."

Etihad ESCO first started with just three people, and then the next jump was to ten employees. The team strength expanded from ten employees to 30 employees and then from 30 employees to 50 employees. "Each one of them has a specific role in the whole process," says Al Jassim. The Etihad ESCO team today consists of managers, energy engineers, contractual, financial, auditors, inspectors, project managers and support staff.

Today, Etihad ESCO has a proud portfolio of 18 mega retrofitting projects, of which nine have been completed and nine are still on-going. In addition, Etihad ESCO has 18 solar energy fitting projects. Al Jassim points out that such a large number of retrofitting projects is a characteristic and achievement in UAE. "Here we have thousands of buildings being retrofitted, while in the West it is limited to a few hundred at the most."

Etihad ESCO initially targeted the government entities and drew up a list of 61 companies that are high consuming in energy and water and where there was a potential to generate a high value in terms of savings in energy costs. It was not sufficient to just have a respectable percentage of energy savings, but the value of the aggregated savings also needed to be high.

Al Jassim points out that the reason Etihad ESCO approached government organisations in the early stages was that the government has to lead by example in such sustainability initiatives. The private sector was expected to follow the lead of government organisations, once such retrofitting projects were underway.

Once the potential list of government organisations was identified, the next step was to have a detailed energy audit and get the government entities into a build, operate and transfer model for energy sustainability services.

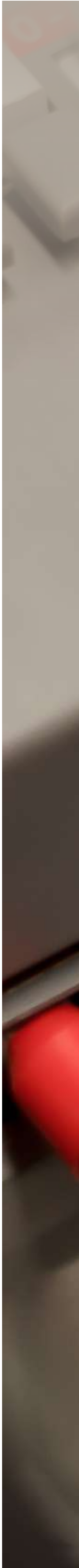
HOW IT WORKS

Before submitting any proposal for retrofitting, Etihad ESCO always undertakes an on-site energy audit that confirms the potential to bring in the latest innovative energy saving technologies in the area of heating, ventilation, air conditioning or HVAC, LED lighting, and water fixtures. The on-site audit usually confirms a number of key factors.

The first is the potential to generate energy savings - typically a thumb suck figure is around 25% to 30% of the total energy cost. The second is the total value of that savings. And the third is the potential to sustain the energy saving for a prolonged period of time, between three to six years.

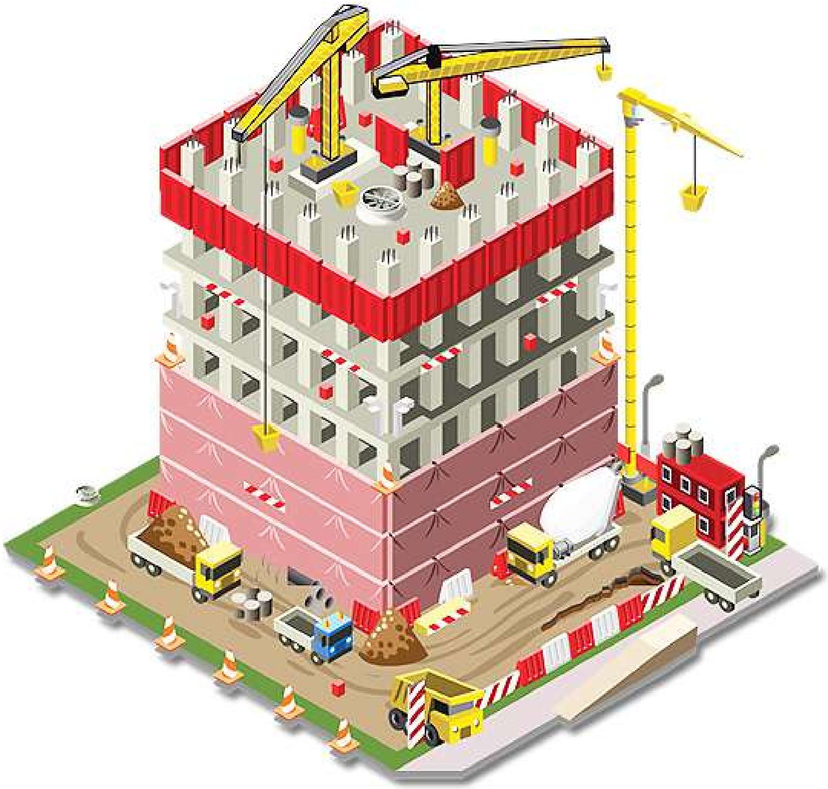
"When I do the detailed audit, I also come to know besides the number of years, what I will change," says Al Jassim. "When you are retrofitting, you know, this is sustainable for so many years."

Today, Etihad ESCO undertakes retrofitting projects across government, commercial, and residential properties. Al Jassim, points out that Etihad ESCO undertakes retrofitting of HVAC, lighting and water solutions, across government and commercial establishments. In residential areas the focus is more on bringing in solar energy and LED lighting,



Ali Mohd Al Jassim,
Chief Executive Officer at Etihad ESCO

A reason for success is a deep knowledge of the products and solutions involved.



The end customer benefits by extending the life cycle of the building premises through investment in sustainable technologies.

since the HVAC solutions in play are more modern than commercial establishments.

To achieve the benefits of energy saving across various types of projects, Etihad ESCO raises requests for quotations across 150 mechanical, electrical, and plumbing, categories, with a portfolio of 23 energy services companies or system integrators specialised in retrofitting. Each of the 23 energy services companies themselves use a myriad of vendors and suppliers with whom they work best, and quote for the cost of supplying equipment and solutions and the percentage of reduction of energy consumption.

A typical retrofitting contract, whether for government, residential, or commercial entities, guarantees a certain percentage of energy savings reflected in a reduction of utility billing. The contract also indicates the length of time that the sustainability is guaranteed through the introduction of the latest innovative energy services technologies and solutions.

Within this contracted period of time, the energy services companies contracted by Etihad ESCO, as well as Etihad ESCO itself, recover the leased

The potential to generate energy savings is around 25% to 30% of the total energy cost.

value of their products and solutions and professional services through savings in the customer's energy and utility billing.

At the end of the contracted period, Etihad ESCO and the contracted energy services companies exit from the contract. The customer is able to continue using the innovative energy services solutions that provide a saving in the energy and utility billing, and enjoy the reduction in the billing, and a revamped energy management environment.

After the exit of Etihad ESCO and the contracted energy services company, typically, a maintenance and support contract come into play assuring the customer of uptime around the energy services solution. This is different from the previous leased contract, whose purpose is to function as a build, operate and transfer model.

GUARANTEEING SUCCESS

What is the role of technology in such energy services solutions? "I choose the best and the latest," says Al Jassim. The catch here is to bring together, the latest technologies and the guarantees of energy savings associated with those technologies. "If the latest technology innovation is not there you cannot get this combination," continues Al Jassim.

How does such a complex interplay of technologies, suppliers, and end customer operations work successfully for such an extended period of time? Al Jassim nails it down to a win-win situation for everyone. The end customer benefits by extending the life cycle of the building premises through investment in sustainable and innovative technologies.

Moreover, the investment is being made through a reduction in operational expenses, over an extended period of time, being reinvested into a leased capital expenditure, rather than a direct capital purchase of an asset.

Equipment vendor and its local channel partners or suppliers benefits through sales of equipment, technology and solutions. The project contractor benefits by construction, implementation, and roll out of the solution. The facilities management partner benefits from the extended support of the solution, from the time of handover to the end of life term. And finally, Etihad ESCO benefits through end to end management of the retrofitting project. "Even the client does not have pay because they are benefiting from this savings," emphasizes Al Jassim.

Another reason for the success of such a complex interplay of industrial operations and financial models at the end customer's premises, is a deep knowledge of the products and solutions involved. There is a long baseline of historical information about the energy consumption performance of the various products and solutions supplied by Etihad ESCO's portfolio of energy services partners.

Today Etihad ESCO continues to make inroads into the world of energy sustainability opportunities by leveraging its multiple strengths. These are around its deep relationships in government and commercial business sectors, the high degree of trust that it enjoys, the strength of its energy savings guarantees, its diverse portfolio of energy services partners, the global brands that it provides through its solutions, and its state-of-the-art technology solutions.

With the rapid expansion of the urban landscape across the UAE and the national emphasis on sustainability and green energy, the leadership role of Etihad ESCO is just beginning to get underway. ■

SNAPSHOT

ETIHAD ENERGY SERVICES COMPANY

Etihad Energy Services Company or Etihad ESCO is the official Super Energy Services Company established as an initiative by the Dubai Government, under the leadership of the Dubai Supreme Council of Energy, to help foster a performance contracting market in Dubai.
Etihad ESCO was established to support Emirate's vision of cutting down 30% energy demand by 2030.
Etihad ESCO aims to create a viable performance contracting market for energy service companies by auditing and proposing energy conservation measures for major building contractors and developers, bringing Dubai closer to the achievement of its sustainability goals.
Retrofitting is the process of modifying something after it has been manufactured. Retrofitting a building involves changing its systems or structure after its initial construction and occupation. This work can improve amenities for the building's occupants and improve the performance of the building. As technology develops, building retrofits can significantly reduce energy and water usage.
Retrofitting an existing building can often be more cost-effective than building a new facility. Since buildings consume a significant amount of energy, particularly for heating and cooling, and because existing buildings comprise the largest segment of the built environment, it is important to initiate energy conservation retrofits to reduce energy consumption and the cost of heating, cooling, and lighting buildings.
But conserving energy is not the only reason for retrofitting existing buildings. The goal should be to create a high-performance building by applying the integrated, whole-building design process, to the project during the planning and roll out phase that ensures design objectives are met.
When deciding on a retrofit, consider upgrading for accessibility, safety and security at the same time. Designing major renovations and retrofits for existing buildings to include sustainability initiatives will reduce operation costs and environmental impacts, and can increase building adaptability, durability, and resiliency.
An energy audit is the foundation for effective retrofit work. It is an inspection, survey and analysis of energy flows in a building, process or system to reduce the amount of energy input into the system without negatively affecting the output. As a result, it offers at a minimum a description of the building, its characteristics and its envelope, details of its energy and water consumption and costs, and subsequently recommendations for adequate technical and organisational measures to increase the energy efficiency of the audited building.
Use cases

RETROFITTING OF OLD DEWA BUILDINGS

Dubai Electricity and Water Authority, DEWA is the government-owned organisation producing and distributing electricity and water in the Emirate of Dubai. DEWA gave the task to Etihad ESCO to survey its buildings and prepare an energy retrofit project.
Etihad ESCO identified that 7 DEWA buildings could be seriously improved to reduce electricity and water consumptions. The project therefore consisted of improving the energy efficiency for 7 DEWA buildings by installing several energy conservations measures.
As part of the project, the fresh air injection system in the main HQ building was refurbished to provide occupants with a real comfort benefit. Using the Energy Performance Contracting model for a duration of 6 years, DEWA was guaranteed of the results. A six-year comprehensive maintenance contract was included.
Several energy conservation measures including refurbishment of the old and inefficient air-cooled chiller plant in DEWA Main Office by a new high efficiency water-cooled system, removal of split units, replacement of other chillers, implementation of variable frequency drives on motors and pumps, evaporative coolers on chillers, solar films on windows, variable fresh air flow system with CO2 sensors, timers and controllers, occupancy sensors for lights, water efficient fixtures, energy management center, amongst others. The project was completed by 2016.

- 31% reduction of the current energy consumption yielding 5 GWh reduction per year.
- 6-year contract with guaranteed electricity and water savings.
- Production of 2,245 tons of CO2 avoided.
- Replacement of old chiller plant by an efficient new one repaid investment.
- Improvement of DEWA employees comfort levels in the buildings through air balancing, fresh air, better lighting.
- Overall improvement of the building equipment.

RETROFITTING OF LIGHTING AT DEWA POWER STATIONS

The 1st Phase of the project consisted of replacing 8,500 existing light points in the Jebel Ali and Al Awir Power Stations. As part of the project, an equalisation and improvement of the lighting levels is made to improve the occupant's visual comfort and security.
Using the Energy Performance Contracting model, DEWA was guaranteed of the results both in terms of kWh savings but also light levels for the duration of the contract. A comprehensive maintenance contract was also included to take care of any failure.
The energy saving came from new highly efficient LED lights replacing existing indoor, outdoor and street lights. The guarantees were given on the volume of energy saving, kWh and on the light levels during the contract duration. The project execution by the Etihad ESCO took place during 2015. From 2016, DEWA benefited from the new lights and the significant energy savings.

- 68% reduction of the current energy consumption yielding 14 GWh reduction per year
- 6-year contract with guaranteed electricity savings and light levels.
- Production of 6,286 tons of CO2 avoided.
- Replacement of old lighting infrastructure by a new one that saves significant energy
- Better quality lighting through the use of latest LED technology lighting improving the employees working conditions
- Reduction of the lighting maintenance budget with long lasting LEDs that do not need replacement or maintenance. ■

CAN AI BE THE GRAND MASTER OF SECURITY OPERATIONS

Deep Blue beat chess grand master Garry Kasparov, but AI may not be able to repeat this feat with SOCs argues Haider Pasha at Palo Alto Networks.

*HAIDER PASHA,
Regional Chief Security Officer, Emerging Markets, Palo Alto Networks.*

Asrtificial intelligence no longer is the next new thing. Artificial intelligence, machine learning, deep learning and other forms of algorithmic-based, automated processes are now mainstream and, on their way, to being deeply integrated into a wide range of front office, back office and in-the-field operations.

As business leaders, you have given at least some consideration to the notion that artificial intelligence will completely replace soon your security operations center security operations centre. My advice to you is this: Do not rely solely on technology to protect your organisation, but assess instead how artificial intelligence can help to complement your security operations centre.

To help you understand why you will be not able to replace your security operations centre with artificial intelligence, let me give you a real-world lesson from the world of competitive chess.

Most of you know that in 1997, chess grandmaster Garry Kasparov played—and lost to IBM's famous artificial intelligence machine, Deep Blue. What you may not realise is that Kasparov was winning a key game, when Deep Blue made what was then considered an unusual move, confusing Kasparov to the point where he lost his rhythm and, ultimately, the game.

Deep Blue's unorthodox move, however, was not a calculated step to trip up the chess master. Instead, it was later discovered that Deep Blue ran into a bug and made a random, rather than meticulously-thought-out, move.

While Deep Blue's victory was hailed as a milestone in the evolution of artificial intelligence, the bug influencing the outcome of the key game should be a cautionary tale in not putting all our eggs in the artificial intelligence basket.

In fact, sometimes you have to think and to act outside of the box like the error in Deep Blue and not based on predefined rules to win the game. This is true, especially when it comes to cybersecurity.

FAILURE OF AI

Artificial intelligence and machine learning have demonstrated the ability to automate many tasks previously done either by security operations centre personnel or earlier-generation tools. And artificial intelligence is a great way to automate many decision-making processes about cybersecurity.

But artificial intelligence will always be limited in its ability to replace human intelligence in an area that is changing as rapidly and dramatically as cybersecurity threat identification and management.

We often do not know what the

NEW BAD ACTORS DO NOT PLAY BY THE RULES THAT MACHINES HAVE LEARNED AND MASTERED.

KEY TAKEAWAYS

- You can teach a machine how to recognise a chair by showing it billions of pictures.
- The advantage of rapid decisions by artificial intelligence is otherwise useless if you cannot act in an automated way.
- The success of artificial intelligence is defined by the automation and integration level of your security controls.

threat is and what its impact can be until it is actually spotted.

Consequently, often it is not possible to train a machine in advance to recognise completely unknown patterns. Machines, like humans, have found it extremely difficult to sort out the signal from the noise, the real threats from the false positives. Why do you think that we still have so many unfounded intrusions even in an era profoundly influenced by automated and algorithmic tools?

As we continue to compete as cybersecurity grandmasters, we look for ways to get ahead of the threats by tapping into the massive and still-growing public data set coming from threat intelligence services and other surveillance methods.

Analysing recent incidents, participating in cybersecurity discussion groups, setting up honeypots or crafting red-team exercises all help and can become the training set basis for an artificial intelligence-driven defense. But training our machines using this data is very difficult, and far from gap-proof.

TRAINING MACHINES

What machines are great at doing, of course, is recognising patterns based on input and learning from human sources. I can teach a machine how to recognise a chair by showing it billions of pictures of different sizes, shapes and formats. But what happens to our machine learning when someone develops a completely new form of chair, like those ergonomic chairs in the form of a large rubber ball or some product of whimsy like a chair shaped like a farm animal or a piece of sporting apparatus like a baseball glove?

In those cases, the human brain is going to make the connection between this never-before-seen format and the functionality of a chair, while any machine will immediately fail to understand that you can seat on it unless it looks like a chair.

We still need our clever security operations centre analysts to teach the algorithms how to recognise it is a chair—just as they would teach the artificial intelligence system to recognise a new piece of malware for the threat it is.

So, while artificial intelligence and machine learning are not going to replace your security operations centre, those technologies are going to play an increasingly important role in automating decision processes at light-speed in such areas as:

- Network traffic analytics
- File or mail classification
- Endpoint protection
- User behavior analytics
- Source code analysis
- Application or database request analysis
- Process behavior
- Identity theft

ARE YOU AI READY?

Before being able to consume artificial intelligence, organisations often forget to transform both cybersecurity technologies and the security operations centre itself.

> ARTIFICIAL INTELLIGENCE IS GOING TO PLAY AN IMPORTANT ROLE IN AUTOMATING DECISION PROCESSES.

The success of artificial intelligence is defined by the automation and integration level of your security controls.

Technologies and tools designed to block bad network traffic, quarantine a machine, remediate a problem or roll out a patch must be available and implemented beforehand —as an automated application programming interface across an entire enterprise. The advantage of rapid decisions by artificial intelligence is otherwise useless if you cannot act in an automated way.

Artificial intelligence is going to have an important impact on security operations centre analysts—but not the job-killing impact that news reports and pundits would have you believe. Artificial intelligence will actually enrich the role security operations centre analysts play by freeing them up to become data scientists and security architects.

In those roles, they will focus on re-architecting core operational processes, ensuring that the right data is being collected and is of the highest quality and coming up with innovative hunting techniques and creative new ways to spot problems unique to individual industries, organisations or job functions. And the security operations centre analyst will sooner or later evolve into those roles.

So, when business executives and boards start thinking about the role that artificial intelligence plays in supplementing and extending—not replacing—the security operations centre, it is important to understand that artificial intelligence is not only going to reduce risk, but also transform your security operations centre personnel.

Consequently, executives need to focus on artificial intelligence's ability to automate the decision processes when machines are working under the direction of security operations centre personnel to ensure full threat visibility, access to the full range of relevant data and the instrumentation of controls.

Finally, remember that there are new bad actors popping up all the time, and they do not play by the rules the machines have learned and mastered. So, you would better have your own cybersecurity grandmasters at hand to ensure you can thwart the attackers as they invent new rules.

> WHAT HAPPENS TO MACHINE LEARNING WHEN SOMEONE DEVELOPS A COMPLETELY NEW FORM OF CHAIR.

Military precision in Radiomir's wrist watch collection

In the 1940s, Panerai came into prominence as the sole supplier of wristwatches to the Royal Italian Navy. These were timepieces which were specially developed with the essential function of a precision instrument to be used by commandos. Today, in these watches the dense, non-reflective green colour becomes an element that expresses a unique quality, as do the sapphire glass with marked convexity, the beige shade of the luminescence and the Italian tanned natural leather strap. It is water-resistant to a depth of about 100 metres.

Gold and silver-plated USB containing moon dust powder

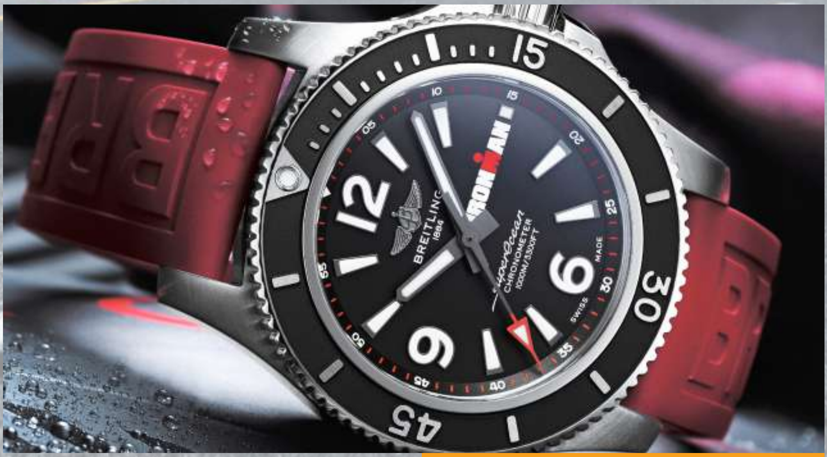
To celebrate 50 years since the NASA Apollo space mission landed the first man on the moon, ST Dupont has created a limited edition, hand-carved Apollo 11 Lunar Module lighter with gold and silver-plated USB key containing moon dust powder. Part of only eight hand-crafted lighters encrusted with diamonds, with a gold and silver finishing, they house a USB containing genuine moon dust powder. Each of the eight pieces takes over 500 hours to handcraft, and will be accompanied by a certificate of erial from the Lunar Highlands.

Taking on high seas with Nomad 75 SUV luxury yatch

Gulf Craft's Nomad 75 SUV luxury yatch, just completed a 3,300 mile journey from Dubai to Cypris in 18 days. The Nomad 75 SUV gives you range and speed. It has 3-decks and is at home on the high seas allowing those on board to enjoy its luxurious features making it a versatile yacht. Lifestyle electronics include Satellite Entertainment TV System TV6 by KVH Tracvision with satellite receivers, 55 inches LED TV 7000 series by Samsung. Advanced electronics include Night vision camera M324S by FLIR, CCTV camera system of three cameras by HIK vision, Thuraya Satellite Phone, Yacht controller for remoter control maneuvering, Twin Gyro Stabilizers SK-16 by Seakeeper, Eight white LED Ultimate 80 LED underwater lights.

Breitling Superocean Ironman Limited Edition

Breitling has partnered with Ironman, in launching the Breitling Superocean Ironman Limited Edition timepiece. The diver's Limited Edition, has a 44-millimeter stainless-steel case and a black dial featuring the Ironman logo. It is presented on a red Diver Pro III rubber strap with a pin buckle. The numerals and hands are coated with Super-LumiNova, a luminescent material that allows readability in any lighting. The certified chronometer has central hour, minute, and second hands. It is water-resistant to 1000 meters. The case back is engraved with the legend one of 300.



GLOBAL GROWTH PROMISE INDICATORS

Switzerland has maintained its place at the top of the GPI 'league table', which is comprised of 180 countries, followed by the Netherlands and Singapore. Elsewhere in the top 10, Luxembourg and Finland have both moved up a single place compared to last year, leapfrogging Norway. This year's ranking has also seen Mauritius, the Bahamas and South Korea make significant ground.

Venezuela

Rapid macro-economic deterioration in Venezuela has prompted a larger fall in its GPI Index score than in any other country.

South Africa

South Africa has slipped six places down the ranking, largely due to lower scores for judiciary independence and business rights.

GLOBAL GROWTH PROMISE INDICATORS

1	–	Switzerland	8.6
2	–	Netherlands	8.5
3	–	Singapore	8.4
4	–	Denmark	8.2
5	▲ 1	Luxembourg	8.2
6	▲ 1	Finland	8.1
7	▼ 2	Norway	8.0
8	–	Sweden	8.0
9	–	New Zealand	7.9
10	–	Canada	7.8
11	▲ 2	Germany	7.7
12	▼ 1	Ireland	7.7
13	▼ 1	United Kingdom	7.7
14	–	Iceland	7.7
15	–	Australia	7.7
16	–	Belgium	7.6
17	–	Japan	7.6
18	–	Estonia	7.5
19	–	Austria	7.4
20	–	United States	7.4

Source: KPMG analysis

Norway

Norway's lower GPI ranking reflects lower scores for its institutional quality in areas such as business rights and transparency of policymaking.

South Korea

South Korean investment in infrastructure – particularly in technology readiness – has paid off, supporting the biggest improvement in its GPI ranking of any developed economy in the Index.

India

India's commitment to greater transparency and improved business rights has helped it rise four places.

United Arab Emirates

The UAE has moved three places up the rankings, largely thanks to advances in its infrastructure, particularly in transport.

KPMG 2019 GROWTH PROMISE INDICATORS REPORT

THE WORLD CIO 200 SUMMIT

SEPTEMBER-DECEMBER, 2019

3
CONTINENTS

14
COUNTRIES

3000+
C-LEVEL EXECUTIVES

BROUGHT BY

GLOBAL CIO FORUM

WWW.GLOBALCIOFORUM.COM