It’s the Year 2021...How’s your Cybersecurity?
by Malcolm Chan, Managing Director, Asia Pacific, BICS
Delivering high quality premium content with expanded capacity at 25.5°/26°E

Es’hailSat’s high powered satellites provide the key infrastructure to media networks and broadcasters to distribute services such as linear TV, video on demand, high definition TV and 4k TV across the region.
# CONTENTS

All articles are available for download at www.connect-world.com

## Beating Cyber Criminals and Terrorists

Beating cyber criminals calls for constant vigilance  
**by Mike McNally, Global Commercial Director, GTMaritime**  
Data protection as a means to safeguard cultural values  
**Helga Tarku, Data Protection and Privacy Consultant, HewardMills**

## Security Predictions

Predictions for 2020  
**by Jackson Lee, Vice President of Corporate Development, Colt DCS**  
The future of the Internet: what will 2020 and beyond bring?  
**by Angelique Medina, Product Marketing Director, ThousandEyes**

## 5G and Security

5G, IPX security, and how operators can take gold this summer  
**by Malcolm Chan, Managing Director, Asia Pacific, BICS**

## Critical Alerts and Communication

A smarter approach to critical alerts and communication  
**by Klaus Allion, Managing Director, ANT Telecom**

## Security and Digital Transformation

Security and the Digital Transformation Age  
**by Cherif Sleiman, SVP, International Business, Infoblox**  
Automation: The new frontier in cyber security  
**by Mike O’Malley, Vice President of Carrier Strategy and Business Development, Radware**  
Encryption is a crucial privacy and security tool for the Asia-Pacific region  
**by Rajnesh Singh, Regional Vice-President, Asia-Pacific, Internet Society**

## Small Enterprise Technology Issues

MSPs offering virtual CIO services could be the answer to small enterprise technology woes  
**by Ryan Weeks, CISO, Datto**

Up-levelling smaller businesses with multi-cloud  
**by Hiren Parekh, VP – Sales & Marketing, Northern Europe, OVHcloud**

## Managed Security Services

How digital businesses can face off evolving cyber threats with managed security services  
**by Wai Kit Cheah, Director, Product Management (Security), CenturyLink Asia Pacific**

Implementing a successful security-as-a-service offering for mobile customers  
**by Hagay Katz, VP Cybersecurity, Allot**
Imagine that hackers have become so successful that the public’s default expectation about Internet transactions flips from “we are basically safe” to “we are going to have our data stolen.” Or, if predictive algorithms improve to be able to predict individual behaviour, all sorts of new attacks might occur. The adoption of Internet of Things (IoT) may make governments both more effective and more vulnerable as a result. Whether for blackmail, “revenge porn” or other motives, cybercriminals and hostile governments in this world would find new ways to exploit data about emotion. The terms of cybersecurity would be redefined, as it became more important for people to manage and protect how their emotions and mindsets appeared to the monitors.

The world in 2020 could look very different from today. The above scenarios may serve to start a conversation and debate, among academic researchers, industry practitioners, and government policymakers.
RED BEE MEDIA EXTENDS AND EXPANDS BROADCASTING CONTRACT WITH FOX IN THE MIDDLE EAST – ADDING GLOBAL DISTRIBUTION SERVICES THROUGH SECURE INTERNET DELIVERY

Red Bee Media has extended its contract with FOX Networks Group Middle East, with a renewal of Playout and Media Management services for channels FOX, FOXMOVIES, STARMOVIES and STARWORLD. For two of the channels, FOX and FOXMOVIES, Red Bee Media will also be providing cost-effective global distribution services through the Red Bee Media Channel Store with secure internet delivery, replacing costly satellite connections and adding new content delivery options. Red Bee Media is now providing managed services for 10 FOX owned channels in the Middle East.

Red Bee Media has a long-standing relationship with FOX Networks Group Middle East. In addition to continuing to benefit from managed services within Playout and Media Management, FOX will leverage the advantages of Red Bee Media’s global distribution service Channel Store for two of their channels. Replacing costly satellite and fiber connections with this secure and highly reliable internet-based signal transport solution, FOX will be able to achieve broadcast-grade distribution while significantly reducing cost and setup time.

“Red Bee Media has been our trusted service provider for a long time and we are happy to continue and expand this relationship for the years to come. Leveraging their global distribution offering, we are now also able to distribute channels globally in a more cost-effective and flexible way”, says Sanjay Reina, General Manager and Senior Vice President, FOX Networks Group Middle East.

By adding their channels to the Red Bee Media Channel Store, FOX will now be able to quickly and cost-effectively distribute their channels onto multiple international affiliates outside of the Middle East, including BeIN, MyHD and ETISALAT.

“We are proud to have renewed and expanded our relationship with FOX and it is a clear confirmation of the value we bring by delivering our managed services. Doing so, we are providing FOX with the ability to focus on content development, production and increased viewer satisfaction, driving business growth in their markets.”, says Houssam Al-Khaled, Head of Market Area Middle East, Red Bee Media.

Red Bee Media is delivering its services to FOX, through their Middle East Hub in Abu Dhabi, United Arab Emirates, servicing 10 channels and affiliate broadcasts, including FOX, FOXMOVIES, STARMOVIES, STARWORLD, FOXCRIME, FOXLIFE, FX, FOX FAMILY MOVIES, FOX ACTION MOVIES and FOX REWAYAT.

The Red Bee Media Channel Store

Aimed at content owners and distributors, the Red Bee Media Channel Store creates the ability to sell and deliver content at any time, anywhere, in any format. Live content from multiple sources is easily aggregated over Red Bee Media’s global network including internal and external Playout sources, fixed-line fiber connections, web streams, internet delivery and satellite down-link via in-house and partner teleport facilities. Channel Store delivers live video and audio in multiple formats; DVB multicast streams, internet CDN, satellite up-link, point-to-point secure internet delivery, and streaming to AWS and Google Cloud applications.

https://www.redbeemedia.com
Beating cyber criminals calls for constant vigilance

by Mike McNally, Global Commercial Director, GTMaritime

As cyber-criminals look to exploit weaknesses in human behaviour using spoof emails, the technological solutions tackling cyber risks must be backed up by crew vigilance, advises Mike McNally from GTMaritime.

Mike McNally, Global Commercial Director, GTMaritime

Mike has more than 25 years’ experience working in the maritime industry both at sea and in senior maritime communications management positions. He began his career at sea, working on offshore workboats, commercial fishing vessels and global product tankers.

After coming ashore, he joined Globe Wireless, a major global maritime satellite service reseller. During two decades at the company, he oversaw the successful introduction of several new technologies including VSAT, Iridium and Fleet-Broadband solutions into its range of services. He moved to Inmarsat to manage maritime distribution partners for its next-generation Global Xpress satellite broadband service, ultimately rising to vice president sales for the Americas.

Following a brief stint at Telemar USA, overseeing its successful merger into Marlink, he joined GTMaritime in 2018 to head up sales and marketing activities. Recently appointed as Global Commercial Director, Mike is currently leveraging his expertise in technology management in delivering secure and reliable maritime IT connectivity solutions to the world fleet.

Fraudulent emails designed to make their recipients hand over sensitive information, extort money or trigger the installation of malware on shore-based or vessel IT networks remain one of the biggest day-to-day cyber threats facing the marine industry.

Technical solutions such as the Advanced Threat Protection deep content inspection offered by GTMaritime offer a robust first-line defence by preventing deceptive messages from ever reaching staff inboxes but the cyber-criminals are continually experimenting with new techniques to evade detection.

Recent studies suggest criminals are researching their targets and tailoring emails for staff in specific roles. Another tactic is to spoof emails from the CEO or other high-ranking colleagues in the hope staff lower down the chain will drop their guard and follow the request unquestioningly. Worryingly, maritime-specific examples are beginning to surface. A recent incident in the Gulf of Guinea saw cyber-criminals send spoof emails requesting a cargo manifest, with a view to possibly attacking the vessel and targeting the containers with highest-value contents. The more convincing an email appears, the greater the chance employees will fall for the scam.

To address this residual risk, software-based protection should be treated as one constituent of a wider strategy that also encompasses the human-element as well as organisational workflows and procedures. It is imperative to make crew aware that they are under attack; to bring to their attention the very real-world consequences of a moment’s carelessness or inattention; to reveal the techniques and tricks fraudsters will utilise to manipulate them; to deliver practically-focused guidance on how to spot a potential phishing attempt; and to embed a sense of duty to protect themselves, their colleagues and their ship.

Familiarising staff with the various strategies fraudsters employ to deceive them and sharing practical advice for distinguishing dishonest messages from legitimate ones can make an enormous difference. Real-life examples will help impress upon staff the importance of taking the threat seriously, particularly if they are drawn from a maritime setting.

To maximise its effectiveness, formal training should be reinforced by periodic refresher courses. Putting up posters in high footfall areas or notices near PC terminals act as constant reminders to crews not to let their guards down and stay vigilant.
Checklists are a simple but good way of instilling new behaviours and preventing carelessness as long as they are not perceived as perfunctory, annoying or unnecessary. Giving crew a say in what items goes on a list or letting them adjust it according to their needs or work style can engender a greater sense of ownership.

A selection of basic advice is offered below as a foundation for developing a list that reflects the way emails are used in different shipping segments - the inbox of staff working on a regional shortsea ferry, for instance, will differ to that on, say, a bulk carrier steaming from Australia to China.

- **Question unusual requests**: Be alert to suspicious instructions from high level executives - especially those involving financial transfers. If in any doubt, it best to contact them and verify the request. Don’t just hit reply but start a new email chain.

- **Don’t follow suspect links**: There is no foolproof way to tell whether or not an email is genuine, so if you have any grounds for thinking that an email is fraudulent, it is better to err on the side of caution and not click on any links.

- **Check the email sender and URL**: Check whether the sender’s domain (detailed after the @ sign in the email address) matches the claimed source of the email. Remember fraudsters deliberately use incorrect spellings of legitimate domains in the hope of evading detection.

- **Check that links lead to where they are supposed to**: Hovering a mouse over a link will reveal its destination URL. If the link bears no relation to the claimed destination, do not click.

- **Check for a personal salutation**: Legitimate senders will usually address their customer by name, while phishing attempts will likely to use a generic greeting, such as ‘Dear Customer’. Bear in mind your email address does not count as a personal salutation as the sender already has that info.

- **Take time to review the email**: To encourage a hasty response, phishing emails often include time sensitive requests. Make sure you take the time to review all emails to ensure they are genuine before acting on any request.

- **Don’t give out personal or sensitive information**: Be wary of emails requesting account details or other sensitive information. Contact the sender in another way to confirm the legitimacy of their request.

- **Check the design and quality**: Phishing emails often contain poor spelling and grammar, or incorrectly reproduce graphics stolen from the claimed source. Ask yourself if the quality is what you would expect from an authentic email.

- **Ask for help**: If you receive a suspected phishing email, forward to your IT department.

With cyber-security now coming under the remit of the ISM Code, many shipping companies are already in the midst of assessing their exposure to risk and developing IT policies for inclusion in their Safety Management Systems aimed at mitigating it. So now is a perfect opportunity to reflect on how phishing attempts might target and manipulate staff and to devise formal procedures for handling suspect phishing messages or next steps if staff are a victim of an attack.

A copy of the policy – written in plain language - should be disseminated to crew, explaining what to do and who to contact if they receive an unusual or suspect request. Make sure staff have the confidence to question emails, even if they appear to come from someone important within the organisation. Punishing staff if they are caught out is generally considered counterproductive. Phishing emails are increasingly hard to spot, and penalties will discourage them from reporting an incident and delay interventions to reduce the aftereffects. It may make them so fearful they spend too much time and energy scrutinising every email they receive.

On the technical side, admins can configure user accounts to limit the impact of messages containing malicious code. The rule of thumb here is to provide staff with the lowest level of user rights possible whilst still allowing them to perform their roles. At the very minimum, they should not be accessing the web or checking emails from an account with administrator privileges.

A good way of assessing how big a threat phishing poses to an organisation is to create and send a phony scam email and see how staff respond. Do they click a link right away? Do they recognise that it’s a scam and delete it? Do they contact a senior colleague to warn them? The results will help guide where security measures are needed and act as a reference point when it comes to staff awareness training.

GTMaritime is carrying out such exercises with several customers to gauge how staff across their shoreside and fleet operations react to phishing attacks. Maintaining a high level of vigilance is vital because no matter how many phishing attempts are thwarted by filters and other technological safeguards, the possibility of one slipping through the net always remains. In short, there is no room for complacency.
From thought leadership to social media to the connected world, Connect-World understands the importance of Connected. To assist in running your organization, read for FREE our authors’ thoughts on how the changing digital and technological landscape could impact your business – www.connect-world.com.

- Leading discussion forum for ICT leaders
- Established over 25 Years
- Expert analysis and trends from ICT decision makers

Get Connected

sales@connect-world.com
+44 20 7537 9255
www.connect-world.com
https://www.facebook.com/connectworld.ict/
https://twitter.com/ConnectWorldICT
https://www.linkedin.com/company/connectworldict
The destruction of cultural assets as an act of war is not new. History is peppered with examples of cultural property being used to either break the other or enact revenge on a given population. For example, in 1914 German soldiers set the Leuven library in Belgium alight as a retaliation for civilian resistance against the German invasion. The building and its unique collection of books were destroyed. During the siege of Sarajevo in 1992, the Serbian forces deliberately attacked the National Library, burning it to the ground, thus destroying three million books, countless artifacts and an important symbol of multiculturalism. In 2012, after extremists seized the ancient city of Timbuktu, Mali – also known as the ‘City of 333 Saints’ – they began a campaign of destruction and terror. In addition to banning sports, dancing, and singing, the extremists destroyed mausoleums and ancient manuscripts. More recently, various extremist groups have used similar techniques by attacking religious and archeological sites, museums, and libraries in Egypt, Libya, Tunisia, and Yemen.

With the rise of ISIS in 2014, the world watched in dismay as the terrorist organization destroyed invaluable cultural heritage sites in Iraq and Syria including the World Heritage sites like Hatra and Palmyra. Sensationalist use of cultural heritage as a target and means of war has become a key feature of terrorists in their fight against western ideas and culture. Sadly, the destruction of these buildings and landmarks was not a byproduct of military combat but rather a systematic approach to wiping out a people’s heritage.

The destruction and theft of cultural sites not only has repercussions for the history/identity of a nation but can also help fund terrorist cells through the trafficking of antiquities. Extremists in Syria, Iraq, and beyond are known to have claimed protection fees from people who transport illegally obtained antiquities across borders toward western markets. Indeed, sometime between 2014-2015, ISIS began to issue licenses to explore new archeological sites and sell looted antiquities. A report by The Wall Street Journal stated that in 2015 trafficking in antiquities was ISIS’ “second-largest source of finance after oil”[1].

As Turkey steps up its efforts to fight trafficking of antiquities from Syria and Iraq, traffickers are shifting their focus towards Southeast Asia, Thailand, and Russia. Unfortunately, organised crime is highly adaptive and the collectors’ desire for such treasures helps fund these illegal activities.

In light of such events, the US and its allies have become acutely aware that protection of cultural property is one of the key elements of a global anti-terrorist campaign. This is why President Trump’s controversial tweets about targeting Iranian cultural sites resulted in global shockwaves.
As US-Iran events unfold, it is important to remember that cultural heritage can be tangible and intangible. If a western democracy threatens to commit a possible war crime against Iran’s cultural heritage, retaliation could come in ways many countries aren’t able to mitigate.

The fundamental ingredients of a healthy western democracy, and key aspects of our intangible culture, include freedom, independence, privacy, freedom of speech, freedom of choice, equality and free market economy. These cultural/social values do not exist in a vacuum but are carefully curated through complex social, institutional and legal webs. It is for this reason that we need to think and be prepared for the possibility that future attacks could target our intangible culture to instill fear and distrust.

Intangible cultural attacks could take many forms such as cyber-attacks, misinformation campaigns, infrastructural sabotage, surveillance of group behavior, and critical infrastructure targeting. Given the severity of the perceived threat, on January 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), which operates under the US Department of Homeland Security issued a warning to the cybersecurity community to be vigilant against potential attacks from Iran.

It is important to remember that these attacks can be executed anywhere in the world by someone who sympathizes with an anti-western mindset and possesses the technical know-how. Furthermore, we should be prepared to see state sponsored cyber-attacks from North Korea, China, Iran and Russia. The Centre for Strategic and International Incidents has highlighted over 100 significant cyber incidents in 2019. Notable mentions among these incidents include:

• A head of the historic summit in Hanoi with Kim Jong Un and President Trump, North Korean hackers engaged in an 18-month long cyberwarfare against American and European organisations. The sustained attacks targeted banks, utilities, and oil and gas companies. Many of the attacks focused on engineers and executives with broad access to their companies’ computer system and intellectual property.

• Suspected North Korean hackers sought to steal credentials from people working on North-Korea related discussions at the UN.

• During 2010 - 2015, Chinese hackers focused on acquiring intellectual property from aviation companies around the globe to bridge China’s technological gap in the aerospace industry. These systematic attacks were part of a plan to support Chinese state-owned aerospace manufacturer, Comac, as it was building its C919 airplane.

• During 2013-2017, Iranian hackers targeted over 170 universities worldwide, stealing $3.4 billion worth of intellectual property.

• In October 2019, Iranian hackers attacked the Trump campaign, US government officials and journalists.

In response to such state sponsored attacks, the US is taking legal action. On Feb. 10, 2020, the US government charged four members of the Chinese military with hacking into Equifax, one of the country’s largest credit reporting agencies. During this state sponsored attack, the hackers were able to steal trade secrets and personal data of about 145 million Americans. The indictment suggests that the cyberattack was part of a concerted effort by the People’s Liberation Army and the Chinese agencies to better target American officials. Having access to their financial status, and other sensitive information would allow a hacker to identify opportunities for blackmail or bribery.

Although the US is taking legal action against some of these attacks, the issue will not go away any time soon. Governments and private organizations alike should be prepared for asymmetric tactics that threaten our cultural values and weaken our democracies. The concept of war in the digital age needs to be re-assessed, in that indiscriminate attacks on civilian and commercial infrastructure are easy to achieve and yield immediate/tangible results on the adversary. Organizations should take a systemic approach to their security, which includes a robust security plan, training staff on secure use of technology, identifying possible gaps, and imbedding a corporate culture that values privacy and data protection.
Security Predictions

Predictions for 2020

by Jackson Lee, Vice President of Corporate Development, Colt DCS

This year sparked off many a conversation around AI and its use cases across various industries. Within the data centre sector, conversations centred around how providers can support businesses in undertaking this technology and in terms of how data centre facilities themselves are employing AI to elevate their operations.

Jackson Lee is an accomplished strategy and finance professional with extensive background in sourcing and structuring deals within the data center industry. In his current position at Colt Data Center Services, a global data center developer, Jackson is the VP of Corporate Development, providing recommendations into market expansion (in Europe and Asia) through M&A, new builds and partnership opportunities, competitive positioning and product differentiation. Prior to this role, Jackson was a Director within Fidelity Investments private equity group, where he provided portfolio management oversight, acquisition/divestiture capabilities and financial restructuring expertise to the firm’s telecom, data center and real estate assets in Europe and Japan. Over the course of his career, Jackson was involved in nearly $3 billion worth of transactions, covering M&A, liquidity events and debt restructuring.

Prior to joining Fidelity, Jackson spent five years in the Retail Apparel industry at J.Jill and TJX, where he served in key positions in FP&A and corporate strategy. Jackson began his career at Societe Generale as an Investment Banking Analyst in their Leveraged Finance Group.

Jackson Lee holds a BSBA, Finance & Economics degree, from Questrom School of Business, Boston University.

As we stand just months away from the new decade, we are presented with the opportunity to look back on the year that was and gaze ahead at what’s to come in the year ahead.

2019 was a year of new technology trends promising to alter our business landscape as we know it. Safe to say not all these trends came fully to fruition but they did lay the groundwork for the coming years and we are excited to see where this takes us.

Bigger the better – hyperscale is here to stay

2019 saw an uptick of smaller data centre facilities. Designed for smaller workloads, the demand for decentralised micro data centres grew, raising questions around the need for hyperscale data centres in years to come.

But hyperscale is here to stay. In fact, the demand for these large-scaled centralised data centres is set to reach new heights in 2020, with bigger than ever data centres entering the scene.

As digital companies expand into new markets, Asia and Europe will take the lead in terms of new hyperscale builds. Smaller facilities are not commonplace in these regions where regulations and barriers surrounding news builds have limited the number of facilities providers can enact.

On the flipside, U.S, a more mature market where the data centre new build market is much easier to navigate, will see a slowdown in hyperscale facilities in 2020.

Sustainability is the name of the game

The ball will drop in 2020 when legislators realise that the climate crisis is a real issue.

We will see legislations that require data centre new builds fulfil a green power quota coming into play. In fact, we can expect some regulators holding back permits for new data centre builds as a result of limited power supply.

There is a likelihood that some governments will limit data centre operations in order to fulfil power needs of both the public and corporations alike.

Adding 5G into the mix in 2020 can only mean there is less power to go around. Unable to travel the distance like its far-reaching predecessor 4G, 5G will need more wireless receivers to create substantial aggregation points. This will inevitably grow the power supplies needed to keep the network working to effectively.

We already saw this within the Dutch municipalities of Amsterdam and Haarlemmermeer, which called for an immediate stop to the construction of data centres in the region to ensure public reliance on the power grid would not be impacted as a result of power-hungry data centre facilities.
Security Predictions

A1 will be limited in its capabilities

This year sparked off many a conversation around AI and its use cases across various industries. Within the data centre sector, conversations centred around how providers can support businesses in undertaking this technology and in terms of how data centre facilities themselves are employing AI to elevate their operations.

The tail-end of the year saw many coming to the stark realisation that AI can be limiting in the benefits it can bring. Within the data centre industry for example, AI was pipped to be a fantastic replacement for building management systems. It was believed that AI could take over the role engineers played in carrying out the manual facility management processes. Yet, that simply has not and will not happen given the need for engineers on-site to make specific judgement calls.

2020 will be the year where the industry realises that while AI can be a fantastic extension to enhancing human capabilities, it cannot work independently or replace human roles within facility management. Instead, skilled engineers will be more in demand to ensure AI can effectively be incorporated into any data centre facilities to drive higher value for end customers.

Change will be slow to come

The data centre industry has historically been known to be resistant to change.

For instance, we saw a new cooling technology come into play over a decade ago which involved placing servers in water to help regulate the temperature. Both cost-effective and power-efficient, it took off significantly in some regions like the US, yet even after a decade later, the widespread roll-out of that has yet to come.

In 2020, what needs to change the most is the mindset of data centre providers. "Why change something that isn’t broken" can be a safe option but it will inevitably leave providers lagging behind other industries in harnessing the benefits of fast-moving technology solutions.

Whether it’s integrating a new technology or implementing a new design, providers need to be thinking about offering the best possible solution for their customers. And often times, this will involve changes to current ways of operating.

2020 will hopefully be the year that providers embrace change the way they should be.

Data centre industry growth will reach new heights... and new locations

2020 will see more and more businesses recognising the data centre sector as a lucrative business opportunity. Hoteliers and real estate companies alike will start branching out into data centre new builds.

We’ll also see more non-data centre establishments investing big money into the industry. One way this will occur is through acquisitions of smaller data centre operators looking to scale up.

As a result, the already competitive data centre market will only become even more so.

We’ll also see regions that have not historically been associated with data centre builds cropping up with new facilities. Data centre hubs like the US and Europe will start reaching saturation point, forcing providers to extend their builds into newer areas.

Major cities with large population and heavy digital reliance will require a high bandwidth of connectivity, making them the new target markets in years to come. Southeast Asian countries like Vietnam, Thailand, Indonesia and even Malaysia will become new regions to watch for providers.

These emerging markets will allow providers an easier inroad due to lesser restrictions from regulations such as GDPR. Providers will also find themselves facing better cost-saving opportunities as they can serve these markets through on-site facilities rather than having to do it remotely from the nearest country for instance.
MWC Shanghai is where the mobile industry’s influencers gather, CEOs meet, and innovators get a glimpse of the future.

In 3 days, you will be able to:

● Network with key decision makers from our industry
● Develop new business opportunities
● Advance your business strategy with insights from top thought leaders

This is the place to do business, connect with leaders, and harness the power of connectivity to help the world thrive.

This is Connected Impact, MWC Shanghai, 2021.

#MWC21
So, what does the future of the web look like? Will we see global Internet use continue to increase, whilst at the same time witnessing a growth in Internet censorship? And will there be a tipping point with new technologies like cloud gaming, 5G, the Internet of Things and artificial intelligence? Here are five top Internet trends that will be prominent for enterprises, ISPs and cloud providers alike over the next few years.

The Internet will become more important than ever before

This may seem like a no-brainer, but as the cloud has become the new data center and the Internet is the new network, the number of enterprises that rely on the cloud increases every year, so does the reliance by the world’s biggest brands to keep their businesses online and keep the revenue chugging in.

Fortunately, faster remediation of service outages improves the overall quality and performance of the global Internet, making worldwide connectivity more reliable than ever.

The ‘Splinternet’ will become more splintered

With the growth of technologies such as 5G and edge computing, a dramatic connectivity acceleration is currently underway. However, we’re also experiencing a growing “Splinternet”, where some regions of the globe are experiencing a lack of connectivity as the Internet becomes increasingly fragmented. In 2019, Russia passed its Sovereign Internet’ law to block off its Internet from the rest of the world,
and Iran implemented a near-total Internet shutdown. In 2020, this “Splinternet” trend of a fragmented Internet will accelerate, as more countries will attempt to create restrictions of their Internet using government control overflows of traffic and internet-based services. The most likely candidates to extend these restrictions? Turkey, Turkmenistan, and Saudi Arabia.

**A Chinese ISP will cause major global collateral damage**

The Great Firewall doesn’t just isolate Internet users in China, the way many people think. A major Chinese ISP will demonstrate the impact of Chinese government censorship far beyond its borders, as hundreds of sites and services around the world get knocked offline for a significant period of time as a result of routing policies meant to only impact users within China.

**DNS Snafus will be responsible for the most outages in 2020**

Many things can be responsible for future outages, including natural disasters, attacks or even simple human errors. Attacks are also a major cause of outages. DNS is a fragile infrastructure that is often overlooked and has been a target for major attacks. Past DNS attacks such as Dyn have had a huge blast radius causing widespread outages, creating a devastating impact on businesses. BGP is another weak point in the fabric of the Internet that has been subject to past attacks. User error, such as “fat fingering” can also result in outages, as well as internal misconfigurations or infrastructure failures, with symptoms that manifest themselves on the network layer.

BGP-related outages caused major collateral damage in 2019, leading many ISPs to adopt better Internet routing security measures, which will dramatically decline these issues in 2020. Similarly, DDoS attacks will decline overall, particularly in the US and Europe. Ironically, often overlooked DNS services may be ripe for a major service disruption or compromise that could cause ripple effects across the wider Internet.

Ultimately, the Internet wasn’t designed to manage everything it’s currently being used for. It’s a mass of independent networks and providers which are unpredictable and vulnerable to outages and security threats. With this in mind, we expect 2020 to be another disruptive yet pivotal year for our world wide web.
Malcolm Chan has been the Managing Director of BICS Asia since February 2014 with overall responsibility for BICS’ entire suite of wholesale telecoms solutions. As the leading global provider for highly reliable, secure mobility and voice solutions, BICS acts as the bridge between telecommunications operators and a variety of communications providers in Asia and around the world.

Before joining BICS, Malcolm was part of the start-up team at StarHub Singapore, which won Singapore’s third telecommunications license in 1999. He later assumed the role of Director of International Services, responsible for StarHub’s roaming and international business. Subsequently, he was Principal Deal Architect at Vodafone Global Enterprise, providing telecommunications expense management solutions to Fortune 500 companies in Asia.

Prior to joining the telecommunications industry, Malcolm spent seven years at American International Assurance. Malcolm graduated from the Royal Melbourne Institute of Technology with a Bachelor of Business Administration (Degree with Distinction), with a major in Finance.

Cyberattacks and network security have dogged Olympics organisers in the past. During the opening ceremony of the 2018 Winter Games in Seoul, for instance, 300 computers and routers were hacked, and distributed malware disrupted internet access, WiFi and TV systems. Plans have already been put in place to mitigate hack attempts at this summer’s Games. A utility company in Japan, for example, has signed a deal with the Israel Electric Corporation to help it secure infrastructure against attacks during the event and beyond. Microsoft, meanwhile, has advised national and international sporting and anti-doping bodies to improve IT security practices following reports that they’re once again being attacked.

Alongside the world’s greatest athletes, we’re likely to see another winner take a spot on the Olympics podium this summer: 5G. Come July, viewers’ attention across the world will be focussed firmly on the sporting performances of their nations’ athletes. Those in the technology and communications sector, on the other hand, will be keeping a close eye on the performance and security of existing cellular networks, as well as the promised improvements delivered by new 5G infrastructure.

Following field trials in 2018, Japan’s Ministry of Internal Affairs and Communications (MIC) set 2020 – and the Olympic Games in Tokyo – as a major milestone on its 5G roadmap. In September last year, Intel announced a range of developments to aid and enhance connectivity and the spectator experience at the event. More recently (and at the time of writing), Samsung announced a special edition of one its 5G handsets, available exclusively for 2020 athletes.

So, what can we expect in terms of advancements in connectivity at the event? And – more importantly – how can the industry ensure that developments in infrastructure don’t jeopardise network (and subscriber) security?

A challenge of Olympic proportion?

It’s great to hear stories of 5G trials and roll-outs ahead of the Games, but the telecoms and tech industries must be careful not to get too carried away, at the expense of implementing robust network security.

Cyberattacks and network security have dogged Olympics organisers in the past. During the opening ceremony of the 2018 Winter Games in Seoul, for instance, 300 computers and routers were hacked, and distributed malware disrupted internet access, WiFi and TV systems. Plans have already been put in place to mitigate hack attempts at this summer’s Games. A utility company in Japan, for example, has signed a deal with the Israel Electric Corporation to help it secure infrastructure against attacks during the event and beyond. Microsoft, meanwhile, has advised national and international sporting and anti-doping bodies to improve IT security practices following reports that they’re once again being targeted by hacking collective Fancy Bear.

Adopting security practices and solutions is particularly important during an event like the Olympics, which will see spectators and sporting stars travelling across the globe to Tokyo. When travelling and once they’ve arrived in Japan, the majority of subscribers will expect to be able to use their mobile phone or connected device as they would at home. Roaming traffic in Asia has seen massive growth in the past couple of years – data roaming traffic across Asia surged by 245% in 12 months to June 2019, and events such as the Olympics will contribute to further growth.
As such, the sheer number of subscribers, volume of traffic, and signalling requirements will put pressure on networks, and enlarge an already expansive threat landscape.

In response, we’ve seen moves by carriers to enhance network capacity to support the expected demand for roaming and IP-based services. In addition to reducing latency and improving end-to-end quality for subscribers, moves which keep roaming traffic locally - within Asia Pacific - also minimise the cost for operators as traffic is not routed out of the continent and back in. Most subscribers will be using 3G and 4G services, but, with 5G services (and potentially 5G roaming) also live, are operators doing enough to secure this new infrastructure?

**Will 5G signal a security upgrade?**

Details of 5G availability remain hazy, but connected services are likely to include 3D athlete tracking, autonomous taxis, robotic meet-and-greets, and facial recognition. If realised, this will all add up to a hyper-connected, data-rich IoT-powered Olympics.

Upgrading the core network to a full 5G environment will require completely new 5G signalling between operators. This will mark a significant change, and mean that end-to-end security must be introduced in the initial design stages of 5G signalling and in the encryption of signalling messages.

Operators will need to set up fully secure relationships between 5G networks and roaming partners on a global scale; a costly and complex task for those working without the support of a third party. To ease costs and complications, IPX providers and specific roaming solutions will be invaluable. These parties and platforms will be able to facilitate 5G signalling, helping operators to establish and secure 5G roaming relationships with all required parties and to enable secure roaming on a global scale.

Alongside developing and deploying 5G, it’s important that operators keep a close eye on ensuring the security of existing 3G and 4G infrastructure. The vast majority of current IoT deployments today - whether that’s connected tracking of athletes and spectator experience applications during the Olympics, or a smart factory in the IoT space - don’t require the speeds and low latency of 5G. Instead they rely on 3G and 4G.

**Laying a foundation for the future**

Unfortunately, much 3G and 4G infrastructure is not fully secured from a network point of view, as end-to-end security was not embedded in 4G specifications. Standardised end-to-end security of 4G networks is currently lacking, and 4G signalling (i.e. the critical information exchanged between different operators and network elements) is not fully secured in many cases. Operators may have secured their own private, domestic infrastructure, but if they want to safely open these up on an international level, they’ll have to deploy a secure IPX. Implementing the right security policies and practices with 3G and 4G now will therefore pave the way for a more secure 5G – and IoT ecosystem - further down the line. So, what should operators be considering?

Enhancing security should be viewed as a three-step process:

1. Assess network and identify weaknesses
2. Monitor the network to identify where attacks are coming from
3. Proactively block network threats and use intelligence to mitigate future threats

**International insight**

What’s needed is a solution that incorporates information from and insight on international network infrastructure and numerous other operators. It must give operators clear insight into the capacity layer, signalling, IPX, and roaming. This will ensure that when connected ‘things’ (or human subscribers) travel from one country to the next, they can expect the same high level of security (and the same low level of threat) when crossing a border as they do within their own home country. This will be crucial in securing connectivity for and between people and things for international events like the Olympics, as well as in the long-term, as the IoT expands to become a truly global ecosystem.

Finally, monitoring must be fully independent from the network and include proactive protection, automatically identifying and stopping attacks before they can cause major damage.

The benefits for operators in terms of network security are clear. And improving network security is ultimately to the benefit of end-users - operators’ subscriber base. Securing the signalling network will help tackle the threat of intrusion by criminals, who would otherwise intercept calls and SMS, siphon funds from mobile accounts, bypass billing, or impact the operation of the mobile network.

These things are crucial year-round and on an ongoing basis, however, events like the upcoming Olympics are particularly important. The world’s top athletes won’t be the only ones under the spotlight in Tokyo this summer. Operators – and their networks – will also be under scrutiny from mobile subscribers, businesses looking to invest in the IoT, and (increasingly) regulators. 5G is gaining a lot of attention currently, but without implementing robust security now – and with threats and hacks gaining media attention – operators are unlikely to realise their 5G goals in the future.

If they want to win big at the Olympics and beyond, the telco community must tighten up security of current network infrastructure on a global scale, and leverage the solutions and relationships required to make this happen.
Critical Alerts & Communication

A smarter approach to critical alerts and communication

by Klaus Allion, Managing Director, ANT Telecom

Choosing a device with smart integrated lone worker functionality means devices can be equipped with panic buttons, tilt and no-motion sensors as well as impact alarms. So for example, when a driver is parked up in a layby or an estate and is more susceptible to an attack or robbery, alarms can be activated, which will then alert the appropriate response teams to provide the necessary support as quickly as possible. These features are crucial within a safety context and can save business vast amounts in costs, both financial and human.

Klaus Allion is Managing Director at ANT Telecom, a bespoke telecommunications provider based in High Wycombe.

Klaus has over 25 years’ experience working in the telecommunications industry, including roles as divisional manager at Bosch Telecom UK and sales and marketing director at ASC.

In his current role, Klaus aims to make ANT’s customers work more effectively and feel safer with ANT’s comprehensive range of telecoms products and services, from telephone systems to wireless technology, such DECT and radio. ANT provides these solutions to businesses that want to improve productivity, service and safety, especially those operating in challenging and risky environments.

In an increasingly interconnected world, businesses from all industries must ensure that cross-team communication is flawless. Not only is it important in order for specific job roles to function effectively, but from a safety perspective as well. From lone workers to those in an ATEX environment, having the right tools to communicate information or critical alerts is absolutely essential, and this means workers must have a dedicated, streamlined and reliable device to hand at all times.

Often, when selecting the right device for these tasks, a smartphone is a common choice. We all use them in our personal lives, not only using them to communicate via phone, but also integrated text messaging, diary alerts, emails and internet access in one device. But businesses need to analyse the numerous options available to suit their unique set of challenges, from operating systems (OS) to format and functionality. It’s definitely not the straightforward buying decision that many managers presume it is. After all, smartphone purchases can often be based on emotion rather than any sort of logical reasoning, because when it comes to the latest technology people frequently go for their preferred personal option, for instance the latest iPhone model. However, when applying this technology to business environments, that’s not necessarily the smartest route to follow. Klaus Allion, ANT Telecom Managing Director, examines what it could cost businesses that fail to give the decision deeper consideration.

Choosing from the crowd

With so much choice in lone working and communications solutions for manufacturing environments, it’s challenging for businesses to identify the most appropriate device for them. The familiarity and perceived low overall cost of smartphones often make them an attractive option for many. But businesses frequently overlook the key functionalities that can take the standard smartphone technology to the next level, and augment it into a multifunctional tool that unites several aspects into a single device to help a business to manage its alarms, communicate with colleagues and crucially, keep them safe. Simply buying the cheapest, most basic tier smartphones could spell disaster, because with unnecessary features still enabled, such as access to social media, or a lack of compatibility with certain safety apps, employers are risking the safety of entire teams and individuals through distraction or a complicated setup.

Therefore, once a business has determined that a smartphone is the best device to meet their needs, they must then take a detailed look into what they require as an organisation, and any particular ways to integrate it into other areas of the business. For instance, teams operating in ATEX environments require a smartphone that is intrinsically safe and may also need a device that can withstand being dropped, or can be used by multiple shift operatives with a hot swappable battery.

It’s not just about the physical handset either, smartphones can be more than phones, they can be turned into streamlined safety devices as well as primary communication tools. By combining devise functionalities in this way, employers can reduce the number of technology products employees have to learn and carry, and create the most efficient approach to employee wellbeing; offering vast savings in training, technology purchases and maintenance.
Critical Alerts & Communication

Safety built-in

Smartphones that have been adapted and chosen correctly, can also be used as lone worker devices and be optimised to enable features such as push to talk technology. As well as other functions, for instance: being able to help rapid response teams find lone workers through real time maps or easy troubleshooting capabilities for engineers. There are even apps available that disable certain mobile phone functions, to help those long-haul delivery drivers to maintain their focus for instance, or so night-shift workers don't rack up business phone bills - whilst still being an intrinsically safe device. This is particularly important as statistics from the British Security Industry Association cite that the employees facing the greatest levels of risk are delivery and HGV drivers. However, not all these apps are available on Android and IOS, which means that unless businesses do the proper research, they may end up with the wrong device - a costly mistake.

To avoid this, each organisation must be aware that it will have its own unique set of challenges, and while the internet makes it easy to compare the technical specifications of individual smartphones, some key features can easily be overlooked. For example for manufacturing environments or ATEX zones, is the smartphone compliant with regulations and does it offer a button that can be pressed to raise an immediate alert, even if the phone is locked? If not, is that device the right fit for every potential scenario the employees may face? Choosing a device with smart integrated lone worker functionality means devices can be equipped with panic buttons, tilt and no-motion sensors as well as impact alarms. So for example, when a driver is parked up in a layby or an estate and is more susceptible to an attack or robbery, alarms can be activated, which will then alert the appropriate response teams to provide the necessary support as quickly as possible. These features are crucial within a safety context and can save business vast amounts in costs, both financial and human.

Conclusion

With a vastly distributed workforce in constant operation across many industries, smartphones enable organisations to stay in regular contact with their employees, digitise many necessary processes, as well as delivering welcomed health and safety benefits to staff. Integrated smartphone devices combine reliable communication and comprehensive lone worker protection into a single integrated and adaptable device that can be an ideal solution once specifically tailored. By working with an unbiased supplier businesses can work collaboratively to analyse these components and ensure they get it right for employees using it on a day to day basis, to maximise productivity and safety at the same time, and to achieve this level of tailored functionality at ease.
Securing critical national infrastructure: a global priority

by Stuart Reed, VP, Cyber Security, Nominet

Given the importance it has to society’s operations, Critical National Infrastructure (CNI) has become an increasing target for cyber criminals. For the UK, in particular, the National Cyber Security Centre chief has said that it is a question of “when, not if” a major cyber-attack on UK infrastructure will happen - and the same can probably be said of most nations in the world.

Stuart Reed has amassed more than 15 years’ experience in a variety of world-class technology brands— including Sony, Symantec and NTT — with a particular focus on cybersecurity over the last decade. In his role as Vice President at Nominet, leading the research, product and marketing teams, Stuart is responsible for product and go-to-market strategy globally. Adept at understanding how security plays a role within business strategy and wider organisation transformation, Stuart is at the forefront of cyber, identifying innovation and shaping thought leadership across the industry.

Critical National Infrastructure (CNI) is the backbone of what allows our society to operate. It means that energy can be run to our homes and businesses, that we can get money out of ATMs, and that our hospitals can be relied upon for health services.

In fact, its exact definition varies depending on the country and the shape of its society. In India, for example, the National Critical Information Infrastructure Protection Centre was established in 2014 to protect six broad sectors, including Power & Energy, Banking, Financial Services and Insurance, Telecoms, Transport, Government and Strategic & Public Enterprises. By comparison, in the UK there are 13 National Infrastructure Sectors, while in the US there are 16. Despite the differences between countries, the overall concept is consistent; if these services are disrupted it will significantly impact society.

Critical National Infrastructure (CNI) is the backbone of what allows our society to operate. It means that energy can be run to our homes and businesses, that we can get money out of ATMs, and that our hospitals can be relied upon for health services.

In fact, its exact definition varies depending on the country and the shape of its society. In India, for example, the National Critical Information Infrastructure Protection Centre was established in 2014 to protect six broad sectors, including Power & Energy, Banking, Financial Services and Insurance, Telecoms, Transport, Government and Strategic & Public Enterprises. By comparison, in the UK there are 13 National Infrastructure Sectors, while in the US there are 16. Despite the differences between countries, the overall concept is consistent; if these services are disrupted it will significantly impact society.

For example, investigations of the Muddy-Water group - also known as SeedWorm - indicated that telecoms were the most likely group within CNI to be targeted, with Pakistan taking the brunt of attacks. This becomes even more critical when you consider the internet of things and the fact that many devices and machines are also reliant on our communications network to operate.

Often attacks are focused on Industrial Control Systems (ICS), which are used to operate parts of the CNI infrastructure, such as the control centre for flight operations or a metro network, for example. In a recent analysis, 47 percent of computers they protected saw malicious activity targeting ICS. When broken down by country, the highest impacted were Vietnam where 70 percent were infected, compared to only 15 percent in Hong Kong.

Attacks against Critical National Infrastructure

It is hard to predict how badly an attack against CNI could affect a country, as it depends on the type of critical national infrastructure targeted and the type of attack. In the UK, researchers have predicted that an attack on UK electricity networks would cost the country in the region £111 million a day. Of course, financial impact is just one measurement of how detrimental an attack on CNI could be - the true cost of losing access to electricity, even partially, is clearly far higher.

For the telecoms network, which often underpins many of the critical services delivered to society, there is also high risk of potential damage. If a communications network is taken down, it can make it almost impossible for information to be passed between organisations.
Critical Alerts & Communication

Digital transformation heightens concern around CNI security

These global threats need to be considered in the context of digital disruption. In our recent research into digital transformation efforts, all CNI respondents expressed that they were actively engaged in digital transformation. This is understandable, when you consider that a failure to keep pace with technological change could result in a negative impact on a country’s economy. For example, in the case of telecommunications, the race to 5G has become a driving force for change. 5G will significantly transform countries, and all the businesses operating within them to interact and share information.

CNI organisations are not the only ones pursuing digital transformation. This was reflected across all industries, with 93 percent of respondents currently engaged in or planning to engage in digital transformation. Even in industries with a reputation for being risk averse; such as government and healthcare, the majority were actively working on digital transformation projects (67 percent and 86 percent respectively).

Fifty percent of respondents did also admit that cyber risks were their top concern in their digital transformation projects. For example, digital transformation projects led to an increase in perceived risk around blind spots (64 percent), the sophistication of cyber-criminals (64 percent), the exposure of customer data (64 percent), the exposure created by IoT devices (36 percent) and the growing threat surface (27 percent).

Ultimately, as you make changes as part of digital transformation projects, inevitably there will be a need to integrate new and legacy technologies, there are likely to be new innovations and a move to the cloud will also increase the digital surface area of an attack. It is therefore completely justifiable that these lead to concerns around security and digital transformation projects, and in industries such as CNI this becomes even more important.

Securing CNI

As tensions across the globe grow fiercer, CNI has become a prime target for malicious nation-state activity. New ways to penetrate networks and spread malware are constantly being discovered and the domino effect of disruption to essential public services (gas, water and electricity) could have a detrimental impact on the wider public and exerts significant pressure on economies across the globe.

Protection of CNI therefore has to be a global priority. Both in terms of countries across the world encouraging their CNI organisations to build cyber resilience, and also in terms of working together to defend against cyber-attacks. Just as nations can choose to attack each other, they can also aim to share security knowledge, resources and learnings to ensure the most robust defence possible.

It’s also important that in the race to adopt next generation technology, cyber isn’t deprioritised. In a hyper-connected world where CNI continues to embrace new technologies which redefine how they operate; it is even more integral that innovation and security goes hand in hand.

So what needs to be done? Firstly, CNI firms must ensure they are one step ahead by considering security early on in their digital transformation journeys. Building security into their systems from day one will avoid them having to chase their tails. Secondly, once the technology is in place, CNI firms need to have a holistic overview of their IT infrastructure. Siloed thinking opens organisations to blind spots which if left unchecked has the potential to bring a country to its knees.

To this end, appointing a good network of partners and vendors is critical. Ensuring that they understand the significance of a cyber-attack and the need for the type of caution and provisions required when securing Critical National Infrastructure. There is also a need for stakeholders to understand the geo-political contextual environment, to truly understand the implications of decisions.

By definition, CNI is fundamental to our society and consequently needs the most robust cyber protection possible. The answer is to ensure projects – such as digital transformation - are collaborative and that communication is open to ensure security is considered from the outset, in context of the broader political, social and economic environment we exist in. It’s not an impossible task, just one that CNI and the security industry need to work together on.
Dr. Cherif Sleiman is the Senior Vice President of International Business responsible for driving the overall International go-to-market strategy and growth for Asia Pacific, Europe, the Middle East and Africa.

Prior to joining Infoblox, he worked at Cisco Systems as Managing Director where he led the Enterprise and Advanced Technologies Lines of Business for the MEA region. Dr. Sleiman has also served as Chief Technology Officer of the Enterprise Business Unit at Nortel Networks where he was responsible for R&D strategy for a variety of technology areas including Routing, Switching, Optical, Wireless LAN, IP Telephony, and Security.

The 2020s will be the decade of the digital transformation around the world. Organizations are building their networks in a different way—taking advantage of concepts like multi-cloud and SD-WAN technologies, and leveraging the power of IoT devices and the software-as-a-service revolution—to provide better customer service, empower their employees, and respond more quickly to market opportunities.

One of the privileges of my job is the opportunity to talk to business leaders across Asia about where they see the opportunities and challenges in their fields. And in all these conversations, two issues keep coming up: the digital transformation and cybersecurity.

Many of these leaders talk about these issues as though they are distinct, but after all my years of experience in this industry, I see them as essentially two sides of the same coin. Leaders really cannot consider the digital transformation without considering the broader cybersecurity concerns that come with it. And indeed, companies need to have robust cybersecurity policies in place if they want to take full advantage of the opportunities afforded by this fourth industrial revolution.

I will begin this paper by talking about the challenges and opportunities afforded by the digital transformation, especially as they pertain to security.

Next, I will discuss the implications of big data on security, what this means for companies, and how they can forge a “new social contract” that will address the unique concerns of the data driven economy.

Finally, I will explain why companies seeking to undergo the digital transformation should focus on security first, and provide some advice for how they can integrate security-minded thinking into their digital transformation strategies.

Challenges of the digital transformation

The 2020s will be the decade of the digital transformation around the world.

Organizations are building their networks in a different way—taking advantage of concepts like multi-cloud and SD-WAN technologies, and leveraging the power of IoT devices and the software-as-a-service revolution—to provide better customer service, empower their employees, and respond more quickly to market opportunities.

As businesses invest in these new tools to digitize their operations and move to the cloud so they can better compete, the legacy world of data center and interlocked branches policed centrally is fundamentally changing. The network perimeter that we have been used to is permanently dissolving.

Indeed, as devices proliferate, remote access becomes the norm, and companies increasingly store data and run applications from the cloud, the threat matrix that companies face becomes varied and complex.

Enterprises need to understand that the more they take advantage of the benefits of the digital transformation, the more of their critical applications and data will be stored, accessed and run in the public domain—outside of direct corporate control. And at the same time, the expansion of IoT devices, BYOD policies, and remote access is increasing the surface area through which malicious actors can gain access to the network.

Security is no longer something that can be considered as an add-on to running an enterprise network, it needs to be integrated into how enterprises think about their entire digital transformation strategy.
A new social contract

Ask anyone what the key to digital transformation is and they’ll likely respond with one word: data. Data is what allows companies to allocate resources efficiently, identify new business opportunities, and provide targeted services to customers. But data is also a resource in its own right, and one that is highly sought after by cyber-criminals. Criminals can steal data outright, as they did in the 2017 Equifax breach, or it can be locked down and held for ransom, like in the WannaCry ransomware virus that spread around Asia in 2017.

So the opportunity for business is there, and so too is the risk. The digital transformation gives companies the chance to grow, and provide goods and services when and where they are needed, all while reducing operating costs and lowering friction between buyers and sellers. But as the value of personal data becomes more widely appreciated, the importance of securing that data becomes more important—both to a company’s reputation and to its bottom line.

We used to look at the “social contract” between businesses and customers as a simple financial transaction: a customer provides money and the company provides goods or services in return. A company’s reputation depended primarily on its ability to deliver on its promise.

Today—thanks in part to the digital transformation—that contract has changed. Reputations still depend on a company’s ability to provide goods and services, but a company’s ability to protect data plays a critical role as well.

In cases like this, the social contract is murkier. Customers may be receiving a service—but they are paying with their data, not dollars, or rupees, or yen. Furthermore, unlike dollars which become the company’s once the transaction is finished, data is fundamentally still tied to the customer, and will remain so forever.

Companies who collect and deal in valuable personal data, and that includes pretty much all organizations, thus have a much higher obligation to protect the data that they are gathering—not only to their customers, but to their owners and shareholders as well.

Data breaches can have dramatic effects on a company’s market value. A 2019 analysis published by British consumer-advocate website Comparitech found that the share price of companies who suffered a data breach lost an average of 7.27% in the immediate aftermath. The real damage occurs over the long term. While stock prices largely recover within a year, breached companies still lag behind the broader market, by 6.5% after one year, and nearly 13% after two.

The costs of cyber-threats

The decline in corporate value after a cyberattack has many causes. Some of the costs are obvious: the value of the information stolen, the disruption to customers and corporate productivity, and the cost of addressing the attack itself. There are longer-term costs as well. The company may incur fines or liabilities stemming from the attack, they may lose business or customers, or their share price may drop because of the hit to their reputation.

In 2018, Microsoft commissioned a study which found that these long-term, indirect losses can really add up. Microsoft found that cyber-attacks could cost large firms in Asia up to $30 million, a majority of which came from the deeper impacts on the company’s business, ecosystem, and economy.

Cyberattacks can also do damage before they even occur. The Microsoft study found that nearly 60% of their respondents were putting off initiatives to take advantage of the digital transformation because of concerns over cybersecurity.

This is the most tragic cost of cyber-security. Sixty percent of businesses aren’t taking advantage of opportunities afforded by the digital transformation, choking off growth before it even has a chance to begin.

Next level networking: A new model for network security

As enterprises build networks for this new digital era, we are finding that they have very different architectures from the traditional hub-and-spoke, data-center-centric model.

As the pace of digital transformation accelerates, the way that businesses operate, procure, and consume technology is changing more quickly than ever before. Organizations need to embrace this change and understand that in this new era, the way that we build secure networks is changing as well. We call this new paradigm “next level networking.”

Organizations need to think differently about network security in this new era of networking. Companies need to change their mindset: as the digital transformation seeps through industries in all sectors, the way organizations procure and consume technologies is changing as well.

Organizations can’t afford to think of network and security as separate fields, with individual solutions siloed from one another. Concepts like SOAR (Security Orchestration, Automation and Response) demand networking professionals to re-think their architecture from the ground up. Fundamental services like DNS can’t be an afterthought to security, but rather can be brought into the security picture and leveraged for a stronger defense.

This paradigm shift will not be comfortable for many. It is never easy to fundamentally change two decades of expertise and learn something new.

But if businesses are to succeed in this new era and take advantage of the benefits of digital transformation, they will need to embrace innovation quickly and rethink the role that cybersecurity plays across their network. Integrated, robust cybersecurity must be a fundamental consideration when considering business strategy, not only for today, but for the future.
Today’s IT landscape is constantly evolving and looks drastically different than it did a few years ago. Cyber threats are surfacing faster than security teams can adapt. The proliferation of data from dozens of security products is outpacing the ability of security teams to process it. Furthermore, budget and talent shortfalls limit the ability of security teams to expand rapidly.

Business networks and infrastructures are more digitised and complex due to new, emerging technologies (like Internet of Things (IoT), edge computing, APIs and bots), and applications are more customer-centric, cloud-native, and public-facing.

Understanding the modern IT environment

With users, devices and applications everywhere, IT teams and security professionals are struggling with visibility of the network and trying to understand the following:

- Are users legit or malicious?
- What is on the network and how does it connect?
- How vulnerable are our clouds? Who/what accesses it?
- How can we view and secure all connections?
- What exists in the cloud and how does it connect?
- How do you protect something you can’t see?

First, we need to understand the threat landscape and how it impacts security considerations in network infrastructure, applications and the cloud.

The rise of multi-cloud

We see greater movement towards the cloud across all industries, including multi-cloud environments. The traditional data center has morphed into a private cloud and at the same time, many applications hosted locally are now hosted in multiple public clouds. This has changed the threat landscape considerably, as the attack surface is now much wider and more vulnerable.

Transitioning to the cloud means losing visibility and control over computing assets. Cloud-hosted workloads are managed remotely, making it difficult for security teams to supervise access to sensitive cloud resources. As a result, many organisations are unable to prevent cloud misconfigurations, identify cyberattacks as they are happening and respond in time.

The changing landscape of technology

In response to changes in environment, technology is likewise changing and creating the following main threats:

- API - With APIs becoming the main information corridor between applications, threat actors are starting to find ways to infiltrate and abuse them.
- IoT - International Data Corporation (IDC) estimates that by 2025, there will be 41.6 billion connected IoT devices generating 79.4 zettabytes (ZB) of data. IoT devices have no standard of security built in, and the burden of their security vulnerabilities is something that enterprises have never had to deal with before. These devices can easily get infected and attack applications across the entire enterprise.
- SSL - SSL is now going to be based on UDP/DTLS and QUIC; SSL-based attacks, which previously impacted mainly e-commerce and financial services industries, may very well affect all industries moving forward, especially as most enterprises can’t see threats with their SSL encrypted traffic.
- Bots - Bots are increasingly becoming more sophisticated; they can mimic human behavior by using keystrokes and mouse movements, take over user accounts, scrape data, hold inventory and disrupt services. Unfortunately, almost 80% of organisations cannot make a determinative distinction between a ‘good’ and a ‘bad’ bot.

Company information is no longer solely in the hands of IT. The rapidly changing nature of business, coupled with the availability of technologies has led to multiple teams within the organisation using digital assets and handling data - outside the control of the traditional IT department. DevOps, cloud architects and even marketing are all making independent decisions.
and gaining greater influence on the overall security posture. This is leaving security staff in a constant state of playing catch up and trying to hire scarce security resources.

As technology, environments and processes change, blind spots are created. How do you protect what you can’t see? The complexity of keeping up with quickly changing network environments has made visibility a growing and major issue. How does a network security team improve the ability to scale and minimise data breaches when all the while dealing with increasingly complex attack vectors? The answer is automation.

The role of automation in security

Cybercriminals are becoming savvier and their attacks increasingly automated. It’s evident that traditional DDoS mitigation methods, such as rate-based or manually tuned protection, are outdated solutions to safeguard sensitive data in the wake of automated cyberattacks.

IT organisations now face advanced persistent threats that are spearheaded not by human assailants but by automated bots. Security personnel are no match for these intense, sustained attacks and are incapable of keeping up with the sheer volume and complexity of incoming threats. Legacy DDoS mitigation solutions that leverage rule-based event correlation can generate thousands of alerts in a 24-hour span. On a good day, a SOC can only investigate approximately one hundred.

Additionally, their ability to make quick and impactful decisions to manually address an attack is equally inefficient. Research shows that machine-learning botnets are now capable, in certain situations, of scanning a network for vulnerabilities and successfully breaching its defences in less than 20 seconds. That is why automation is becoming such a powerful and effective component of cybersecurity. To combat the onslaught of incoming threats, organisations must employ an army of equivalent strength and sophistication, far greater than any human combatant.

Attackers leverage automation

Cybercriminals are weaponising automation and machine learning to create increasingly evasive attack vectors, and IoT has proven to be the catalyst driving this trend. IoT is the birthplace of many of the new types of automated bots and malware.

At the forefront are botnets, which are increasingly sophisticated, lethal and highly automated digitised armies running amok on corporate networks. For example, hackers now leverage botnets to conduct early exploitation and network reconnaissance prior to unleashing an attack.

The Mirai botnet, which was made famous by its use in the 2016 attack on DNS provider Dyn, along with its subsequent variants, embodies many of these characteristics. It leverages a network-scanning and attack architecture capable of identifying “competing” malware and removing it from the IoT device to block remote administrative control. In addition, it leverages the infamous Water Torture attack to generate randomised domain names on a DNS infrastructure. Follow-up variants use automation to allow the malware to craft malicious queries in real-time.

Modern-day botnets are an equally sophisticated multi-vector cyberattack weapon designed to elude detection using an array of evasion tools and camouflage techniques. Hackers now leverage machine learning to create custom attacks that try to trick or camouflage themselves from a company’s defences.

The discovery of BrickerBot marked the first time a software-based botnet would render a physical (IoT) device permanently unusable. It also foreshadowed a new genre of botnets and attack techniques that automate dastardly deeds. The WannaCry and NotPetya ransom attacks that followed each demonstrated crude forms of automation.

Automation for detection and mitigation

So how does a network security team improve its ability to deal with these increasingly multifarious cyberattacks? Fight fire with fire. A automated cybersecurity solutions provide the data-processing muscle to mitigate these advanced threats.

Traditional DDoS solutions use rate limiting and manual signature creation to mitigate attacks. Rate limiting can be effective but can also result in a high number of false positives. As a result, manual signatures are then used to block offending traffic to reduce the number of false positives. Moreover, manual signatures take time to create because identifying offending traffic is only possible AFTER the attack starts. With machine-learning botnets now breaching defences in less than 20 seconds, this hands-on strategy does not suffice. By the time a manual signature is available, the attack has already penetrated the target and achieved its objective (ransom, IP theft, etc...)

Automation and, more specifically, machine learning overcome the drawbacks of manual signature creation and rate-limiting protection by automatically creating signatures and adapting protection to changing attack vectors. Machine learning leverages advanced mathematical models and algorithms to look at baseline network parameters, assess network behavior, automatically create attack signatures in real time and adapt security configurations and/or policies to mitigate attacks. Machine learning transitions an organisation’s DDoS protection strategy from manual, ratio- and rate-based protection to behavioral-based detection and mitigation. It’s the move from reactive to proactive protection.

A market-leading DDoS protection solution combines machine-learning capabilities with negative and positive security protection models to mitigate automated attack vectors, such as the aforementioned DNS Water Torture attacks made notorious by Mirai. By employing machine learning and ingress-only positive protection models, this sort of an attack vector is eliminated, regardless of whether the protected DNS infrastructure is an authoritative or a recursive DNS.

The final step of automated cybersecurity is automated self-learning. DDoS mitigation solutions should leverage a deep neural network (DNN) that conducts post-analysis of all the generated data, isolates known attack information and feeds those data points...
back into the machine-learning algorithms. DNNs require massive amounts of storage and computing power and can be prohibitively expensive to house and manage within a privately hosted data center.

As a result, ideally a DNN is housed and maintained in a cloud by the organisation’s DDoS mitigation vendor, which leverages its network of cloud-based scrubbing centers (and the massive volumes of threat intelligence data that it collects) to process this information via big data analytics and automatically feed it back into the organisation’s DDoS mitigation solution via a real-time threat intelligence feed. This makes the input of thousands of malicious IPs and new attack signatures into an automated process that no SOC team could ever hope to accomplish manually.

The result is a DDoS mitigation system that automatically collects data from multiple sources and leverages machine learning to conduct zero-day characterisation. Attack signatures and security policies are automatically updated and not reliant on a SOC engineer who is free to do the advance work of research the upcoming wave of new threats and preparing for tomorrow, not firefighting today.

Automation is the future of cybersecurity

As cybercriminals become savvier and increasingly rely on automation to achieve their mischievous goals, automation and machine learning will become the cornerstone of cybersecurity solutions to effectively combat the onslaught from the next generation of attacks. It will allow organisations to improve the ability to scale network security teams, minimise human errors and safeguard digital assets to ensure brand reputation and the customer experience.
Encryption is a crucial privacy and security tool for the Asia-Pacific region

by Rajnesh Singh, Regional Vice-President, Asia-Pacific, Internet Society

Encryption is a method of scrambling data using a secret value or key. The data can be decrypted, or made readable, using a related key. When data is sent over the Internet, the key is usually known by both the sender and receiver. For stored data, such as personal information stored on a smartphone, only the owner knows the key.

Many messaging and email apps now enable encryption by default, giving users privacy and security protections without them having to take any action.

Rajnesh Singh is Regional Vice-President for the Asia-Pacific at the Internet Society, a non-profit organisation dedicated to ensuring the open development, evolution and use of the Internet worldwide.

In this role he works with a broad range of stakeholders including governments, civil society, academia, the private sector, the technical community and influencers in the Asia-Pacific region to promote technologies, policies and best practices to keep the Internet open, globally connected, secure and trusted for the benefit of people all across the world.

Prior to joining the Internet Society, Rajnesh played founding and leading roles in several technology and private equity investment firms. He has extensive experience in business management and strategy development across multiple industries, including telecommunications, power infrastructure, agriculture, manufacturing and real estate.

He has provided consulting and mentoring support to start-ups and SMEs in the Asia-Pacific region, and has held advisory roles across multiple sectors ranging from governmental organisations to sporting organisations and the private sector.

Rajnesh has worked extensively with the technology sector, and has held several leadership roles, including Chair of the Asia-Pacific Regional Internet Governance Forum (APrIGF) and Founding Chair of ICANN’s Asia Pacific Regional At-Large Organisation (APRALO). He has served on a number of Advisory Boards, and on Expert Working Groups for regional and international organisations on infrastructure, policy and regulatory reform, and development issues.

The use of encryption by Internet users – an essential tool to protect the privacy and security of Internet users – is under attack in several parts of the world.

While using the strongest tool we have to protect personal data like banking information does not seem like it should be a controversial issue, politicians and law enforcement agencies in some countries disagree. They have criticized it in recent years, saying it is a tool that criminals use to hide their activities.

Dusting off rejected arguments from the past, they have proposed the need for a so-called “safe backdoor” to encrypted communications, in which they – and no one else – would have access to these messages.

This argument is not only wrong, it suggests a counter-productive way to catch criminals that threatens the safety of people, economies, and national security everywhere.

There is no such thing as a safe backdoor to encryption. If technology companies build these exceptions into their encrypted products, cybercriminals – and other actors – will find a way to exploit them. History shows us that criminals will find security vulnerabilities and use them to their advantage.

The argument for encryption backdoors also ignores the fact that criminals use many legal tools for illegal means. Bank robbers, for example, often use cars to aid their getaways. But like with cars, the benefits of encryption far outweigh the negative effects from a few bad users.

What is encryption?

To understand how bad things can get without encryption, it’s important to know how it works.

Encryption is a method of scrambling data using a secret value or key. The data can be decrypted, or made readable, using a related key. When data is sent over the Internet, the key is usually known by both the sender and receiver. For stored data, such as personal information stored on a smartphone, only the owner knows the key.

Many messaging and email apps now enable encryption by default, giving users privacy and security protections without them having to take any action.

But encryption protects more than just our communications. When it comes to things like online banking, encryption is the only thing standing in between a hacker and your bank account.

In addition to services that enable encryption by default, much of the debate in recent years involves end-to-end encryption, intended to allow only the sender and the intended recipient to read the message involved. No
third party, not even the Internet service provider or the maker of the devices or applications used to send the message, has knowledge of the encryption key.

Depending on how it’s implemented, end-to-end encryption can be impossible or extremely difficult to break into and prevents cybercriminals from reading encrypted messages. State and non-state actors who may want to “listen in” to conversations and messages - or carry out mass surveillance activities - are also unable to do so easily.

**Encryption for everyone**

While some have argued for encryption backdoors, the Internet Society and other groups concerned about privacy and security have called for strong encryption to protect Internet users in the Asia-Pacific region and across the globe.

Other cybersecurity products, including anti-malware protection and firewalls, are also valuable tools for Internet users. But studies show Internet users deploy them inconsistently, and these tools focus more on protecting individual devices, not on securing Internet communications the way encryption does.

Likewise, consumer education and cybersecurity awareness are equally important, but not everyone in every country has the means, and the access, to those resources. Encryption deployed by default on devices, communications services and applications ensures their activities online have a level of protection.

**Other encryption tools**

Another encryption tool is a VPN, or virtual private network. VPNs provide a “secure envelope” between the sending device and a trusted secure third-party server, making the data unreadable to eavesdroppers. There are many VPN products available, some of them are even free. Other Internet users prefer Tor, an open-source tool that allows for anonymous communication by using encryption.

PC and smartphone users can also encrypt the data on their devices, in addition to their messages. Most modern operating systems include a built-in utility that makes device level encryption relatively easy to configure.

In addition to using encrypted messaging apps and turning on device-level encryption, users should also take other steps to protect their data. These include the use of strong passwords, regularly updating software (most of which can be configured to run automatically), turning on two-factor log-in authentication, and enabling automatic data wipe or lockdown on devices after several failed log-in attempts.

**Protected from prying eyes**

Encryption is necessary because, in many cases, Internet users approach their online activity with the assumption that the services they are using are secure and trusted. Many people tend to only start thinking about online security when their information or device is compromised or a website they use is breached. Encryption by default helps create a secure online environment for users where their communications are not readily visible to cybercriminals and other third parties.

Malicious actors are constantly trying to find vulnerabilities or using social engineering tactics to glean personal details and data. There are few roadblocks in their efforts to gain access to personal data when there’s no encryption enabled on websites, apps and application software. Without encryption, such malicious actors have it much easier.

**Security in Asia-Pacific**

With more than 2 billion Internet users - and growing - encryption is particularly important for users in the Asia-Pacific region. As the world’s largest Internet market, the Asia-Pacific region is becoming increasingly reliant on online information and services, and it is important that the users online experience is safe, trusted, and secure.

More and more services are shifting online as a means to improve efficiency, productivity and convenience - for users and vendors alike. People now use the Internet for a diverse range of services - from filing tax returns to booking flights and hotel rooms to banking to ordering groceries and taxis. All of these services and others demand secure online interactions where payment and personal information is protected.

Even as the number of Internet users expands in the region, cybercriminals are stepping up their activity. With some funded by nation states or large criminal enterprises, cybercriminals are becoming more and more sophisticated in their methods and avenues of attacks.

In addition, most countries in the region see the digital economy as key to their people’s future prosperity. Throughout the Asia-Pacific region, traditional industries are being transformed through the use of Internet technologies, and many countries are prioritizing the development of the new digital ecosystem.

Cybersecurity is critical to digital transforma-

tion, and a key component of cybersecurity is encryption.

Encryption also plays an important role in enabling a trusted Internet environment for users in countries where English is not the primary language spoken. Too often, cybersecurity awareness resources are available only in English, potentially limiting the level of security awareness for Internet users who speak other languages. Encryption gives these Internet users a level of protection, even if they don’t have access to such cybersecurity educational resources.

**Long-running debate**

Despite all the benefits that encryption provides Internet users in the Asia-Pacific region and elsewhere - and despite the security it provides to digital economies in the region - the debate over the use of encryption has been flaring up on and off for more than 15 years.

In the early 1990s, the U.S. National Security Agency (NSA) proposed an encryption backdoor called the clipper chip, a piece of hardware that would encrypt voice and data traffic but give the agency access to the encryption key. The clipper chip proposal was soundly rejected after complaints from privacy and civil liberties groups.

One of the major problems with the NSA proposal - and the current encryption backdoor discussions - is there’s no guarantee these methods would help law enforcement agencies catch criminals or terrorists.

Most cybersecurity experts agree that law enforcement access is unlikely to prevent criminals from secretly communicating with each other. If countries make encryption illegal unless law enforcement has access, some experts suggest that criminals will find other tools on the black market or make their own. A safe backdoor is very difficult to keep safe, and will more than likely be compromised.

The end result is that everyday users, including businesses and governments themselves, would be highly vulnerable to criminals as well as state actors who may have discovered how to exploit encryption backdoors.

As the Internet becomes even more ingrained into everyday life, it is critical that our online activities remain secure, and the platforms and services we use continue to be trusted. Without strong encryption, online security would be severely compromised in today’s digital age.
Small and medium enterprises (SMEs) are more dependent than ever on external IT support, and for good reason. Keeping pace with rapid technology advancements on their own can be tough, so they increasingly rely on external IT professionals who provide services on a recurring basis. Some capitalise on the opportunity to assume the role of a virtual CIO for their clients as well.

Digitalisation is progressing quickly in all industry areas. Capitalising on the new capabilities of the Internet of Things, choosing and managing the best network and cloud services and responding to the ever-changing cyber threat landscape are all complex challenges for SMEs, who have limited resources and internal expertise.

At the same time, Managed Service Providers (MSPs) are evolving into SME’s trusted partners, becoming not only more sophisticated in how they anticipate and support their clients’ needs, but also increasingly able to deliver enterprise-grade solutions that are easy and cost-effective enough to use for SMEs.

A virtual CIO, they can play a very similar role to that of a conventional, in-house CIO — but with more extensive know-how and brainpower as they are made up of bigger teams. Hiring a virtual CIO could be the solution to many SME technology headaches.

Cut down costs

Small and medium enterprises (SMEs) are the backbone of the Asian economy. They already account for over 95% of all businesses in Asia and employ an estimated 60% of the region’s workforce. Many of the challenges SMEs face stem from their small size and lack of digitalisation, which is why a virtual CIO will provide an invaluable service, but at a fraction of the cost of a full-time in-house CIO. Information and data are today’s most valuable assets, but many SMEs lack the resources to hire a full-time employee devoted to it.

MSPs are the answer as they can offer assistance and support around the clock and if any IT issues arise, they have the expertise and experience to fix them very quickly — keeping the business up and running at all times. Less downtime and fewer business interruptions mean happier customers, more productive employees, higher revenue and ultimately, a boost to the bottom line.

Capitalise on the latest technology

In this digital age, global is the new local and small businesses in Asia are harnessing technology to drive their businesses forward. In fact, South China SMEs are leading A PAC when it comes to innovation and technology according to CPA Australia’s Asia-Pacific Small Business Survey. Organisations have all the technological resources they could possibly need at their fingertips, from innovative cloud services to data analytics and artificial intelligence to smart connected devices, but many struggle to take full advantage of this.

Often, it’s the business owner within an SME who makes the technology decisions — the same person who also looks after administration, finance, HR, customer relations and everything else. Fulfilling all those roles can be overwhelming, so it’s not surprising that many SMEs choose to stick with the technology and processes they’ve always used.

In addition, maintaining and improving technology often requires a huge amount of time and money that most SMEs simply don’t have.

But, with a capable MSP at their side, they can still harness innovative technologies to their advantage. A virtual CIO can advise on, deploy, and maintain a whole range of cloud-hosted applications or Software-as-a-Service solutions. The only infrastructure the SME will need is an Internet connection. Relying on the MSP to manage the necessary applications — whether it’s for communication, team cooperation, data management, finance, or security — will make the SME more agile and free up valuable time to focus on other aspects of the business.

Manage risks

SMEs may believe that they are too small to become targets of cybercrime, but in fact, for hackers, they present low-hanging fruit. The fact that they often have less sophisticated and sometimes outdated cyber defences in place makes them fairly easy prey.

Ryan is responsible for directing and managing Datto’s Information Security program. He spent 11 years securing enterprise applications, systems and sensitive customer financial data at FactSet Research Systems, the last four of those years spent orchestrating all facets of the global information security program.

Ryan holds a B.S. in Computer Information Systems from Ithaca College, a M.S. in Information Assurance from Northwestern University and active industry security certifications including the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM).
Small Enterprise Technology Issues

Datto’s most recent European State of the Channel Ransomware Report, for example, reveals that ransomware remains the most prominent threat to SMEs, with 83% of MSPs reporting it as the most common malware threat to their clients.

The same report also found there was a disconnect between MSPs and SMEs when it comes to the ransomware threat as, despite 82% of MSPs being “very concerned” about ransomware, only 8% cited their SME clients felt the same. And Strategy Analytics reports that on average two in five SMEs say they’ve fallen victim to an attack – with those who don’t outsource their IT services more at risk. Roughly six in ten MSPs reported attacks against their clients, but only 19% saw their clients suffer multiple attacks in one single day. While the aftermath of a ransomware attack can be challenging for any business, SMEs suffering business-threatening downtime are at risk of losing out financially and damage to their reputation.

The average ransom requested by hackers is increasing. MSPs report the average request for SMEs is now around £2,000 but the cost of downtime is increasing by 300% year-on-year. Datto’s latest report shows that the average cost of downtime is 53 times more than the average ransom requested in 2019. These figures show that SMEs are by no means immune, and an attack can be particularly crippling for them.

An MSP as the SME’s security partner of choice can help manage this risk effectively with state-of-the-art cyber protection, backup and recovery technology. Outsourcing this important task means that all of it happens automatically in the background, so it doesn’t affect or slow down the SME’s day-to-day operations.

Eighty one per cent of MSPs report that clients with BCDR solutions in place are less likely to experience significant downtime during a ransomware attack, and two in three MSPs also report that victimised clients with BCDR in place recovered from the attack in 24 hours, or less.

**Tap into extensive know-how**

As a virtual CIO, an MSP brings in-depth IT industry expertise and usually, extensive experience in helping other SMEs boost their business with optimised IT solutions and services. Whatever the issue at hand, the MSP has probably seen it all.

Technology is complex and constantly changing, but SMEs can rely on their MSP to stay on the cutting edge of technology, and mine this knowledge for the best advice and service.

If the partnership works as it should, the virtual CIO becomes a vital part of the SME’s organisation as an ongoing consultant, trusted adviser, and avid supporter of its business needs and goals - making a vital contribution to the company’s success.
Naturally, with new methodologies comes new challenges. For example, multiple cloud platforms offer a wider range of possible vulnerabilities. Thus, extra effort is required to achieve effective security, governance and compliance. Today however, businesses can take back some control over much of their security and governance. This includes mandatory IT staff training on avoiding security failures and reacting to breaches and data loss.

Cloud has been a key component of ongoing business evolution for a number of years. This is the era of cloud adoption, and when we look at the business benefits, it isn’t hard to see why.

Cloud computing provides value that is unlike that of any traditional IT environment. For businesses of all sizes, it offers economies of scale through aggregating computing resources and virtualization. Cloud computing ensures a reach of information and services that cross boundaries, using a computing environment that offers on-demand scalability, performance guarantees, minimal initial investment and ongoing cost containment. For SMBs in particular, these benefits can really help level the playing field when competing with larger organisations.

Consequently, the advantages of cloud are undeniable, the question though, is which cloud should your businesses deploy?

Digital transformation is an empowering solution and is being heralded as the ‘fix all’ for businesses. Particularly, small and medium sized enterprises that can often feel stretched on the ground. In these kinds of environments, automating processes is the way to box clever, providing the opportunity to free employee time to focus on more valuable innovations within an agile environment.

Despite the excitement around digital transformation, creating new business processes that take advantage of digitisation is difficult without core infrastructure that offers maximum flexibility. Businesses that wish to harness the power of digital technology to develop new business opportunities, must aim to leverage dynamic computing power and storage across multiple IT assets.

Taking a multi-cloud approach is the key to doing just that. It enables businesses to cater for their individual needs, instead of a one-size fits all approach.

**Powering successful digitisation: the engine of tomorrow’s growth**

**Analysing your needs**

As I alluded to above, every business is different and taking a multi-cloud approach means that the infrastructure can be tailored to facilitate exact requirements, instead of being one-size-fits-all. For this very reason, a multi-cloud strategy can significantly benefit the way that individual business units source their own IT, enabling the as-a-service model to ultimately increase the agility of their organization.

Subsequently, some businesses are multi-cloud by accident, because different services were adopted by different parts of the business as they were appropriate. As such, making multi-cloud an intentional strategy can maximise the benefits. The first step, of which, is the purchasing.

IT managers in companies of all sizes are now more experienced in buying cloud services so are considered ‘cloud natives’ that are more confident in adopting a multi-cloud approach. In the same vein, it is important that SMEs also consider being this type of cloud purchaser, so that they can get the flexible and customised infrastructure that they need to grow their business, to innovate, and to succeed.

**Cloud considerations: flexibility and cost**

A multi-cloud approach provides a comprehensive mix of public and private clouds, and they don’t necessarily need to be integrated, unlike hybrid cloud. Moreover, businesses today don’t have to be locked into one provider. Many platforms are built on open-source technologies like OpenStack and Kubernetes, which are widely supported by a range of cloud service providers and vendors such as OVHcloud. At the very least, opting for an open cloud gives businesses an extra element of flexibility.

It is important to remember that services are rarely used in isolation. So, enabling multi-cloud and hybrid cloud solutions with on-premises systems is key to customer success, as this will help to overcome cost-related challenges associated with flexibility and visibility.

Combining on-premises and cloud infrastructure with a multi-cloud strategy has allowed our customers to connect to networks in a totally isolated and secure way, via numerous points of presence around the world.
As a result, organisations can shift to the cloud at their own pace and take a flexible approach - all while responding to their strategic objectives. This means businesses can control and run an application, workload, or data on any cloud (public, private and hybrid) based on their individual technical requirements.

Another area of consideration when opting for cloud diversity, is budget management. To ensure maximum efficiency within a multi-cloud environment, it can be useful to have an internal team that can consolidate data and provide a cost/benefit analysis for the organisation. It’s also important to monitor cloud spend and finetune budgets depending on current and upcoming projects.

From experience, we know that greater price transparency and auto-shutdown of unused systems are key priorities for businesses. Business leaders don’t want to be burdened with working out the cost of each component within a service. They want an easier way to calculate their cloud expenditure and to predict future costs. To further simplify budget control, we have made the decision not to charge for ingress or egress traffic because we understand that this can be an impediment to moving data between different cloud providers. This is just one way that vendors can work to reduce the hurdles that some users perceive as being part of moving to and between clouds.

This is because, these days, people buying cloud services are more experienced, and their previous experience, often with very large providers, has shown them that cost is not only one of the main differentiators; it is also measurable and accountable and therefore an important metric. As a result, service providers are striving to set themselves apart by designing practical pricing models for core enterprise workloads.

Naturally, with new methodologies comes new challenges. For example, multiple cloud platforms offer a wider range of possible vulnerabilities. Thus, extra effort is required to achieve effective security, governance and compliance. Today however, businesses can take back some control over much of their security and governance. This includes mandatory IT staff training on avoiding security failures and reacting to breaches and data loss.

### Why hybrid isn’t enough

Although closely related, hybrid and multi-cloud are not the same and have some fundamental differences.

A multi-cloud approach provides a comprehensive mix of public and private clouds and unlike the hybrid version, the clouds do not need to be integrated. Flexibility also comes from the fact that you do not need to be locked into one provider since many platforms are built using open source. For example, OpenStack, which is supported by many cloud service providers, provides practical interoperability.

Our SME customers have had success using multi-cloud set-ups which combine multi-cloud solutions with on-premise systems, combining the security, compliance and visibility benefits of on-premise, with, for example, the scalability of public cloud. This type of flexible approach means that these companies have been able to shift to the cloud in a way that suits them best, running an application, workload, or data on any cloud (public, private and hybrid) based on their individual technical requirements.

### To multi-cloud or not

Clearly cloud can have a profound influence on business productivity and whether you opt for public, private or multi, it is here to stay. What is more important, is taking the time to observe the benefits of each cloud option, based on the needs of the organisation. With that being said, to accommodate the requirement for digitisation, it is necessary to harness the power of a scalable, multi-local cloud infrastructure that is based on cutting-edge technologies designed for specific needs and that offers unbeatable value for money. Only then, will small and medium sized businesses stand a chance of standing tall, while competing against technologically, well stablished companies in the race towards innovation.
Managed Security Services

How digital businesses can face off evolving cyber threats with managed security services

by Wai Kit Cheah, Director, Product Management (Security), CenturyLink Asia Pacific

Digital businesses in Asia Pacific (APAC) must be ready to fend off an onslaught of increasingly sophisticated cyber threats with a proactive security strategy.

Wai Kit is the Director of CenturyLink’s Security Practice in Asia Pacific, where he is responsible for the lifecycle management of CenturyLink’s security services portfolio and service delivery in the region. This includes strategizing, positioning and executing on the delivery of security services such as DDoS mitigation, Adaptive Network Security and Managed Security Services in key markets to optimize customer experience and value.

Prior to CenturyLink, Wai Kit has held stints with service providers Dimension Data, Sun Microsystems, Dell, IPsoft, and Equinix. An IT veteran of 25 years, he has also sat on the board of Cloud Security Alliance (Singapore) between 2011 to 2013.

Wai Kit is an advocate for digital transformation, with expertise in management consulting, operations and business change management.

As connectivity grows, the attack surfaces of digital businesses will expand. The perimeter is not so obvious anymore. Cybersecurity vulnerabilities will increase correspondingly, allowing attack vectors to cross the limits of Distributed Denial of Service (DDoS) attacks, SQL injection attacks or phishing attacks.

According to the CenturyLink 2019 Threat Report, the prevalence of a region’s cybercrime activities is directly related to the growth of connectivity infrastructures and networks.

As organizations drive towards digital transformation, coupled with the accelerated race in the deployment of 5G, there will be an increasingly vast number of connected assets across on-premise infrastructure, cloud and Internet of Things (IoT) networks. These are likely to introduce new attack paths for security threats.

Dawn of device-led attacks

Gartner forecasts that 14.2 billion connected things will be in use globally this year, and that the total will soon reach 25 billion by 2021.

These “things” refer to connected devices as diverse as short-range connected devices such as smoke detection alarms or thermostats; wireless LAN (WLAN)-connected industrial or factory devices or smart home consumer devices such as CCTV cameras, wireless smart sensors and even a light bulb that could be switched on or off through a mobile app.

IoT devices can be categorized into either industrial, enterprise or consumer groups. Unfortunately, the reality is that the majority of enterprise IoT devices are not managed by an organization’s IT team, while myriad consumer IoT devices out there are not likely hardened or secured. Their proliferation is set to propel device-centric cyberattacks to unprecedented levels.

These “things” refer to connected devices as diverse as short-range connected devices such as smoke detection alarms or thermostats; wireless LAN (WLAN)-connected industrial or factory devices or smart home consumer devices such as CCTV cameras, wireless smart sensors and even a light bulb that could be switched on or off through a mobile app.

IoT devices can be categorized into either industrial, enterprise or consumer groups. Unfortunately, the reality is that the majority of enterprise IoT devices are not managed by an organization’s IT team, while myriad consumer IoT devices out there are not likely hardened or secured. Their proliferation is set to propel device-centric cyberattacks to unprecedented levels.

According to IDC, the APAC region (excluding Japan) is projected to be the global leader in IoT spending in 2019, around 36.9% of worldwide spending. This increase in IoT deployments may potentially expand the attack surface due to device vulnerabilities and a lack of security controls.
Managed Security Services

One expected manifestation would be a direct hack of the device itself. Take for instance, wireless smart cameras used as home security surveillance. The popular ones are often in-built with cloud connectivity, so that users can view what’s happening at home regardless of where they are.

To achieve this, the smart camera is configured to act as a wireless hotspot, connecting it to the user’s main router via Wi-Fi. With a mobile app, users can watch the recording and control the camera to pan or zoom. Typically, the popular ones will come with an initial loader and thereafter a Linux core is loaded. The system is usually loaded to run with default services. If these devices are not hardened, they can easily be hacked by a perpetrator armed with basic knowledge of the default admin password.

There are numerous examples of how vulnerable IoT devices in combination with poor network security design could result in a successful breach. One such example was in the case of Target. There were no major obstacles in accessing their point of sale (POS) terminals inside their internal network. To illustrate this vulnerability, their external audit team supposedly accessed a cash register after they compromised a deli counter scale located in a different store.

So, can you imagine the volume of threats extrapolated on a sea of IoT devices, particularly when many are maintained by third party vendors and can be used to access your network.

A software-generated attack, however, manifests on a very different scenario, as in the case of a DDoS attack.

A single controlling device connected to numerous other compromised devices can trigger an attack. By commanding them to send synchronization (SYN) packets to the target in a rush, where the volume of bot traffic generated is so overwhelming that it can take down an online service or crash an entire website.

The aftermath of such attacks is often cumbersome, with a string of damages for CISOs and CSOs to work through—from unplanned downtime and monetary losses, to service recovery and long-term management of reputation loss.

The cybersecurity reality

Another grave concern is that DDoS attacks are no longer focused on traditional targets such as retail organizations or e-commerce sites—but are aimed at businesses of all sizes and industries.

CenturyLink has observed that several verticals such as online gaming service providers are potential targets for as high as hundreds of DDoS attacks each day. With multiple attack types and strategies such as multi-vector and diversionary attacks at their disposal, threat actors can go after a broader set of targets with much greater ease.

‘Burgeoning smart cities in APAC such as Singapore have the connected infrastructure to accelerate IoT on 5G networks, hence becoming hotbeds for DDoS attacks.’

Enterprises in APAC are well familiar with the demands of cybersecurity. However, their conventional defend-and-mitigate approach is passive against the scale and scope of what is upcoming. To effectively reduce the risk of a compromise, they must overcome their inertia for change, to adopt a holistic and proactive security monitoring and threat removal approach.

Learn why CenturyLink was ranked by IDC as a "major player" among companies that protect against DDoS.

Read More
For this to happen, they must first conquer their cybersecurity fatigue, which is the result of exhausting management and scaling of in-house security solutions that have become piecemeal from years of knee-jerk implementations. These could conflict, overlap and leave gaps in their security posture, and are challenges without easy fixes.

There is also the problem of security solutions flooding IT organizations with reports and alerts that lead to no action. This is mainly because they either lack the specialization or the manpower among their teams to effectively contextualize the wealth of data into actual cyberthreat intelligence.

To resolve these issues, forward-thinking businesses are opting to face off the incoming wave of fast-evolving cyberthreats, by leveraging the expertise of external security talents and experts.

**Armed and ready to mitigate security threats**

Cyberthreats are not homogeneous and can occur from within an organization. Insiders, either employees or contractors, with authorized privileges or access, can potentially introduce risks which are tough to detect—making it a real challenge for enterprises to safeguard important customer data or confidential and proprietary information. A further risk within an organization is the human element, often in form of mistakes or misconfigurations to IT systems or networks.

Trusted security partners that offer user and entity behavioral analytics (UEBA) services, for example, are becoming essential in helping them identify and act on such insider threats.

‘With UEBA, artificial intelligence and machine learning are used to profile each user persona to baseline what is considered normal behavior and the network activities associated with these users.’

Together with information gathered from other sources, such as security information and event management (SIEM) and logs correlation, enterprises will be able to identify malicious activities and insider threats anchored deep within the network and hosts, separating activities which fall outside the boundaries of normal.

With the involvement of a security partner, businesses can step beyond their traditional log-based monitoring tools and find new ways to quickly and accurately detect, respond and mitigate potentially damaging attacks.

This method not only identifies potential insider threat activities and predicts risk propensity faster, but also removes the guesswork from security operations personnel, freeing them to conduct investigations, triage analysis accurately and to resolve threat situations quickly.

Partnering with a trusted, global managed security service provider

Today, digital businesses are also increasingly hosting business-critical data and applications across vast networks, increasing the risk of a security breach.

If you are a digital business with multiple offices that directly connect to the Internet on a single, corporate-wide MPLS network, you have a large attack surface. As such, merely having endpoint protection security and log correlation in your security program is likely ineffective for detecting data breaches, and this scenario is typical of many business operations in APAC.

Organizations need to adopt a ‘Connected Security’ approach in their cybersecurity strategy that is designed to help ensure holistic and proactive protection of data from both insider and external threats.

With CenturyLink Managed Behavioral Analytics, available on our Security Operations Center (SOC) in Singapore, companies can seek effective protection from cyber-attacks that steal administrator credentials or establish command-and-control channel from their servers.

By applying automated behavioral analytics service on the servers that house critical data, all the user and network activities will be monitored for signs of credential thefts, reconnaissance or lateral movement indicative of an attack. An attempt to exfiltrate data from the server will be detected by the service, followed by an investigation from our 24/7 SOC analysts, before notifying the customer, where the early breach detection enables us to remediate quickly to prevent further loss.

This strategic approach fortifies passive monitoring with necessary actions – to investigate and determine if an event is truly positive – before getting a recommended remediation solution.

As the digital landscape continues to evolve, it is imperative that enterprises act quickly to address their security shortcomings. Partnering with a trusted Managed Security Services Provider like CenturyLink is a fast and cost-effective way to achieving their desired outcomes, without loading their security programs with more management complexity.

Explore the key elements for network security for businesses to build digital trust.

[Download Whitepaper](#)
Managed Security Services

Implementing a successful security-as-a-service offering for mobile customers

by Hagay Katz, VP Cybersecurity, Allot

Mobile customers are looking for a trusted partner with the right level of expertise to handle these security challenges for them. Operators are in a prime position to help subscribers avoid dealing with the complexities of cybersecurity. With their considerable in-house cybersecurity expertise, their existing relationship with consumers and the right tools, operators can mitigate risks with minimum effort and minimal action on the part of the consumer.

Hagay serves as VP strategic accounts for Allot’s cybersecurity business. From 2010 until 2017, he served as the head of the VSAT line of business of Gilat Satellite Networks – a leading NASDAQ-listed satellite communications technology and services company. In this capacity, he transformed Gilat into the world business leader for LTE cellular backhaul over satellite and commercial In-Flight Broadband Connectivity.

Prior to that, Hagay held senior positions in Sales and Product Management at Modu Mobile that developed the smallest modular cellular handset in the world; PacketLight Networks, a leading supplier of compact DWDM devices for the data center (acquired), which he co-founded; and Telestra research laboratories where he represented Australia in network management standard activities. Hagay started his career in an elite technology unit of the IDF.

He is the co-author of nine granted patents and he served as the technical editor of the IEEE communications magazine. Hagay currently advises and serves on the advisory board of Screenovate and Nvento systems. He holds a BSc and MSc in Electronic Engineering from Tel-Aviv University and a MBA from Monash University.

New content, mobile apps, and unsecured IoT devices bring with them increased cyber risks from an ever-evolving set of sophisticated criminal activities, such as virus and other malware injection, phishing, ransomware and cryptojacking. The result is broad concern and considerable damage to the individuals affected.

The average consumer is unaware of most of the potential threats they are exposed to on a daily basis and is unequipped to deal with them. However, as consumers become more aware with every publicized attack, they demand more and more security services. Operators who want to differentiate their brands, re-engage with customers and put the brakes on further ARPU erosion are putting cybersecurity offerings high on their priority lists. Providing Security-as-a-Service (SECaaS) enables communication service providers (CSPs) to build on their trusted relationships and protect their customers from significant risks.

Mobile customers are looking for a trusted partner with the right level of expertise to handle these security challenges for them. Operators are in a prime position to help subscribers avoid dealing with the complexities of cybersecurity. With their considerable in-house cybersecurity expertise, their existing relationship with consumers and the right tools, operators can mitigate risks with minimum effort and minimal action on the part of the consumer.

Zero-touch onboarding

Many CSPs have tried to provide security software and apps to customers by rebranding a standard app, promoting the service, and then imploring subscribers to download, activate, and pay for the application. But success in implementing this ring of security has been very limited. Practically speaking, operators have not achieved more than 10% customer participation – typically 1-5% despite rigorous marketing efforts.

These issues are solved by application-less network-based cybersecurity solutions. CSPs can use network-based solutions to easily protect any device on the network, without having to rely on end-users to download or regularly update anything.

Network-based security: Early warning and protection

Network-based security stops threats at the network level before they reach the end-user’s smartphone and other connected devices. As opposed to end-point security, network-based cybersecurity analyzes user traffic as it moves through the service providers’ network. It allows CSPs to provide cybersecurity services to the mass-market with ease, independent of the type of operating system (Android/iOS), to offer an effortless non-intrusive service to the customer.

CSPs are best positioned to leverage this type of SECaaS solution by adding secured broadband services to their consumer
offering. As the providers of Internet access, they already have the trust and buy-in from their subscriber base. By providing this network-based security to customers, CSPs have a valuable opportunity to be trend setters instead of followers, by championing cybersecurity and rolling out SECaaS to protect their customers.

**Gain brand loyalty with engagement tools**

Building and maintaining a positive, high profile brand reputation is vital for CSPs, and that means delivering on their brand promise in every customer interaction and experience. By putting security front and center, CSPs are positioned as attuned and responsive to vulnerabilities and threats, and also as a secure brand that customers can trust.

CSPs can increase engagement and build perceived value with their customers by offering a SECaaS solution. The result is increased customer loyalty, higher customer satisfaction, and lower churn rates. In fact, we have seen CSPs measure a Net Promoter Score (NPS) greater than 30 when using a network-based security solution.

A customer engagement model should be selected to match the defined goals for the local market. For example, if brand positioning is among the greatest concerns, the service may be offered for free to premium subscribers. For other segments, there are a number of alternative go-to-market models.

With the Try and Buy model, for example, the service can be switched on for a given set of subscribers for a set period, typically 1-3 months. During that time, subscribers first should be told about the upgrade, and then they should be frequently reminded of the benefits and value of the service.

It is very important to emphasize that customer awareness is essential for the success of the service. This can be achieved via periodic messages and updates about evolving threats and how they personally have been protected. The network-based system will provide reports on the quantity and types of malware that customers are exposed to. These reports will enable the operator to describe the region-specific threat landscape and provide relevant security best practices.

Toward the end of the trial, customers are prompted to opt-in to the service. Existing results show that try and buy campaigns bundled with service plans can result in penetration rates of 50% after a few years of operation. This is ten times more than the 1-5% penetration rates of the app-based approach.

**Effective anti-phishing mechanism**

The network-based solution needs to work effectively and efficiently. Everyday users are exposed to a variety of cyber-attacks and CSPs must ensure they mitigate risks for their customers. One of the most prominent types of attacks is phishing, where customer credentials are stolen by misleading the consumer into believing that they are providing their details to a legitimate financial institution.

In this case, Domain Name Server (DNS) mechanisms are not suitable, as they may block entire suspected domains and cause a communication loss to legitimate traffic. Network-based solutions that are in-line can stop specific contaminated traffic only and allow other legitimate traffic top flow without interruption.

There are many ways to mitigate risks for customers and CSPs can be at the forefront of providing these security services. A network-based approach to SECaaS is essential in creating an opportunity for service providers to expand service penetration rates, customer satisfaction, revenue generation and significant differentiation of the operator’s brand.
Send me the following Connect-World issues

- [ ] Africa & the Middle East issue I, II & III (3 issues)
- [ ] Latin America Issue
- [ ] North America Issue I & II (2 issues)
- [ ] Asia-Pacific issue I & II (2 issues)
- [ ] Europe issue I, II & III (3 issues)
- [ ] Global Issue

A total of 12 issues for the publishing year of 2021 at a discounted rate of £100.
Online subscription also available.

### Subscription Form

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title (Mr/Mrs/Miss)</td>
<td>_</td>
</tr>
<tr>
<td>Company</td>
<td>_</td>
</tr>
<tr>
<td>Address</td>
<td>_</td>
</tr>
<tr>
<td>State/Province</td>
<td>_</td>
</tr>
<tr>
<td>Country</td>
<td>_</td>
</tr>
<tr>
<td>Fax</td>
<td>_</td>
</tr>
<tr>
<td>Name*</td>
<td>_</td>
</tr>
<tr>
<td>Job Title*</td>
<td>_</td>
</tr>
<tr>
<td>City*</td>
<td>_</td>
</tr>
<tr>
<td>Postcode/Zip*</td>
<td>_</td>
</tr>
<tr>
<td>Telephone*</td>
<td>_</td>
</tr>
<tr>
<td>Email*</td>
<td>_</td>
</tr>
<tr>
<td>Company*</td>
<td>_</td>
</tr>
<tr>
<td>Address*</td>
<td>_</td>
</tr>
<tr>
<td>State/Province</td>
<td>_</td>
</tr>
<tr>
<td>Country*</td>
<td>_</td>
</tr>
<tr>
<td>Fax</td>
<td>_</td>
</tr>
</tbody>
</table>

(Fill all fields marked*)

### Check preferred subscription medium

- [ ] UK - Printed Magazine for UK subscribers £95 (12 issues, hard copy by post)
- [ ] Europe - Printed Magazine for Europe subscribers £100 (12 issues, hard copy by post)
- [ ] ROW - Printed Magazine for Rest of the World subscribers £115 (12 issues, hard copy by post)
- [ ] Corporate - Printed Magazine for Corporate subscribers (1 issues, hard copy by post)

- sign my company up for a two-year subscriber to Connect-World Series of magazines with an additional 5% discount. Please charge my credit card once a year until I notify you otherwise. I'll get the same low subscription rate I've chosen above for as long as I am a subscriber. Please note: all Corporate subscriptions must be pre-paid. Please provide your credit card information when placing your order.

Note: Please allow up to four weeks for mailing of first issue

Please charge my:
- [ ] Visa
- [ ] Mastercard
- [ ] American Express

Card Number: ___________________________________ Expiry Date: ______/______(MM/YY)

Signature: ______________________________________

- Tick here to receive a VAT invoice
- Please sign _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ and send back by:-

Email: info@connect-world.com or
Post: Infocomms Media Ltd, 1 & 2 Riverside Offices, 17 Towcester Road, London, E3 3ND, United Kingdom

### Contact

Tel: +44 20 7537 9255  
Web: www.connect-world.com  
Email: info@connect-world.com  
Facebook: https://www.facebook.com/connectworld.ict/  
Twitter: https://twitter.com/ConnectWorldICT  
LinkedIn: https://www.linkedin.com/company/connectworldict
Expand Anywhere with High-Speed Connectivity

Making the impossible connections possible. Every day.

Whether trying to bridge the digital divide, or serve next-generation 5G, IoT and Connected Vehicles opportunities, no single access technology can meet every requirement. It’s time for a different approach. Hybrid networks that seamlessly blend terrestrial and satellite networks deliver the reach, performance and flexibility you require to open profitable new markets, drive new revenue streams and ensure the most secure and reliable communications anywhere in the world. Learn how you can leverage our Globalized Network to go farther...and faster.

www.intelsat.com/mr/cwame
Don’t be on track with 5G, be ahead of schedule.

Ericsson.
The quest for easy.