11 April 2018

Synopsis

Scroll to read full summaries with links to news articles.

An **IDC** brief has revealed that **Singapore** leads amongst **APAC** countries in issuing the toughest penalties on breaches of **data**. Japan, India and Thailand were amongst the lowest.

A reminder on vigiliance against **cyberattacks** has been issued by the **Monetary Authority of Singapore**, amidst a series of growing attacks across the globe. The MAS has been working with financial firms to deepen their **cybersecurity**.

Cyber Cafes and other **wifi** providing shops in the city of **Qingdao** have been ordered to install government-verified wifi routers in order to comply with **cybersecurity** and counterterrorism regulations.

Arne Schonbohm, the head of **Germany's cybersecurity** agency, has said that member states in the **EU** are opposed to the Commission's new cybersecurity rules and system.

Amidst the **Cambridge Analytica** and **Facebook** data scandal it has been revealed that over 2.5 million Facebook user's in the EU have had their **data** accessed.

A new 'European approach' to **artificial intelligence** is emerging after 24 **EU** nations signed a pact to potentially support AI research with public funds.

Following its hearings with **Facebook**, the Senate has now stated its intent to hold hearings with other companies involved in the **user data** scandal, including **Cambridge Analytica**.

Paul Ryan, Speaker of the House of Representatives, has been asked by a group of leading Congressional Democrats to 'compel' **Homeland Security** to handover all documents on **cyberattacks** by **Russia** during the 2016 Presidential Election.

A survey released by **Accenture** has revealed that over 60% of citizens surveyed do not have confidence in their governments' ability to prevent **cyberattacks** and protect their **data**.

The **Guardian** (Nigeria) has reported that only 20% of the **technology** and digital sector in **Nigeria** is controlled by native companies. Over 80% of the market is led by foreign firms, consequently causing the nation to suffer vast loses in possible revenue.

Digitial strength has become central to **APEC's** new strategy to help new growth opportunities in the region. The 21 member nations have agreed that the way forward will be to secure a firm **digital economy**.

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

11 April 2018

Table of Contents

Europe

Internet governance

05.04.18

Reuters

Italy buys into Telecom Italia to shield strategic interests

5% of Telecom Italia has been bought by the Italian state in an effort to keep its interests safe. The move follows a series of reports that the largest shareholder of the telecom company is tightening its grip.

"Italian state lender CDP said on Thursday it would buy a stake of up to 5 percent of Telecom Italia (TIM) to safeguard Rome's interest in a company seen as strategic, and amidst a struggle between investors over its leadership.

The bank's decision comes as activist fund Elliott, which has built a potential holding of 5.7 percent in the former phone monopoly, has challenged the way TIM's biggest shareholder, France's Vivendi, manages the group."

Cybersecurity

09.04.18

Euractive

Commission should 'walk the walk' on cybersecurity, German chief says

Arne Schonbohm, the head of Germany's cybersecurity agency, has said that member states in the EU are opposed to the Commission's new cybersecurity rules and system.

"The European Commission should 'walk the walk' and use strong encryption to protect its computer networks against hackers instead of pushing member states to adopt controversial new legislation, the head of Germany's cybersecurity agency has said.

Arne Schönbohm, the director of Germany's Federal Office for Information Security (BSI), lashed out at the Commission for not being transparent about the technology it uses to prevent cybersecurity breaches."

11.04.18

Computerweekly

UK to launch crackdown on dark web

UK Home Secretary, Amber Rudd, has announced new measures and funding for cybercrime crackdowns in the UK at the CyberUK 2018 conference. The announcement comes following reports by the NCSC and NCA that businesses in the UK are getting attacked more than ever.

"The UK is to enhance its specialist law enforcement response to crack down on criminals operating on the dark web. Home secretary Amber Rudd is to announce funding to crackdown on criminals who exploit the dark web at the National Cyber Security Centre's CyberUK 2018 conference in Manchester.

On the first day of the conference, the National Cyber Security Centre (NCSC) and National Crime Agency(NCA) released a joint report showing that UK businesses are suffering more cyber attacks than ever before. The newly announced funding will see £9m allocated to enabling UK law enforcement to tackle those who use the anonymity of dark web that is not indexed by search engines for illegal activities such as the selling of firearms, drugs, malware and people."

Privacy

06.04.18

Euractive

Cambridge Analytica harvested 2.7 million Facebook users' data in the EU

Amidst the Cambridge Analytica and Facebook data scandal it has been revealed that over 2.5 million Facebook users' in the EU have had their data accessed.

"Personal data from around 2.7 million Facebook users in the EU was shared with analytics firm Cambridge Analytica, the European Commission announced on Friday (6 April).

Facebook shared the new figure with EU Justice Commissioner Vera Jourova in a letter that she received Thursday evening, Commission spokesman Christian Wigand told reporters."

06.04.18

Nextgov

[Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security]

A survey released by Accenture has revealed that over 60% of citizens surveyed do not have confidence in their governments' ability to prevent cyberattacks and protect their data.

"In the face of relentless security threats, how can government preserve faith in its ability to protect citizen data?

A recent Accenture survey of more than 6,000 citizens across the United States, France, Germany, Australia, Singapore and the United Kingdom found that almost two-thirds (62 percent) of respondents are less confident today in their government's ability to defend their personal information against a security breach or a cyberattack than they were a year ago. Meanwhile, only 40 percent of survey respondents are confident that law enforcement agencies can protect them against cyber crime."

09.04.18

Ars Technica

[Data firm that worked on Brexit suspended by Facebook]

AggregateIQ (AIQ), the data company hired by VoteLeave during the Brexit referendum, has been suspended by Facebook. The suspension comes after users' data may have been used 'improperly' by the company during the referendum.

"According to The Guardian, a Canadian data analytics firm called AggregateIQ (or AIQ) has been suspended from use of Facebook's platform. Facebook claims the firm may "have improperly received FB user data." AIQ was contracted by parties campaigning in favor of Brexit in 2016, pulling in a total of £3.5 million from Vote Leave, BeLeave, Veterans for Britain, and Northern Ireland's Democratic Unionist party, per The Guardian.

Facebook said this week that it was suspending AIQ from its platform "following reports the company may be connected to Cambridge Analytica's parent company, SCL."

Internet Inclusion

10.04.18

Gov.UK

World-leading cyber centre to be developed in London's Olympic Park

A new cyber centre is opening in the Olympic Park in London. £13.5 million has been given for the London Cyber Innovation Centre, aiming to bring 2000 jobs and a boost to Britain's cybersecurity capability.

"A new world-first £13.5 million cyber innovation centre, located in the Queen Elizabeth Olympic Park, will help secure the UK's position as a global leader in the growing cyber security sector.

The London Cyber Innovation Centre will boost the thriving East London digital cluster and spur the development of cutting-edge technology to keep the nation safe from online threats. Estimates suggest it could also help create 2,000 UK jobs in cyber security."

10.04.18

Euractiv

Twenty-four EU countries sign artificial intelligence pact in bid to compete with US & China

A new 'European approach' to artificial intelligence is emerging after 24 EU nations signed a pact to potentially support AI research with public funds.

"Twenty-four EU countries pledged to band together to form a "European approach" to artificial intelligence in a bid to compete with American and Asian tech giants. Ministers signed a declaration on Tuesday (10 April) saying they will consider putting public research funding into AI, but did not promise a specific amount of dedicated new investments.

All EU member states except for Cyprus, Romania, Croatia and Greece vowed to "modernise national policies" as part of an effort to develop large-scale AI research. One Commission official said the four EU countries that did not sign were not opposed to the initiative but might still need formal approval before signing. Norway also signed the declaration.

11.04.18

Computerweekly

Finnish government backs national AI development strategy

A new plan has been formulated by the Finnish government to further its artificial intelligence strategy. The new National Steering Group has been formed by the Economic Affairs ministry to help aid the growth and development on the strategy.

"Government is harnessing Finland's tech base to help make the country a leading location for the artificial intelligence industry. Finland is mobilising its technology base in a bid to become a leading global player in artificial intelligence (AI). The centre-right government has, amid record investment activity in the sector, set in motion a plan to develop a far-reaching national AI development strategy.

For Finland's economic planners and industrialists, AI has become the new internal combustion engine, or electric light, with infinite unexplored uses and commercial frontiers. At a more fundamental level, Finland is looking to unearth the next-generation tech star – an innovator that will put the country firmly on the world AI map, just as Nokia did when it emerged from virtual obscurity in the 1980s to become a global powerhouse in mobile communications."

09.04.18

Computerweekly

Norway government backs ambitious datacentre investment plan

In a similar vein to Finland, Norway is also looking to grow its strategy on data. The new Norway As A Data Centre Nation plan has been formulated by the government.

"Norway has a plan to be a leading location for datacentres with a policy that will put it in direct competition with some of its Nordic neighbours. Norway, in no mood to lag behind the rapid forward leaps recorded by near neighbours Sweden and Denmark, has rolled out an ambitious new strategy to position the country as a leading location for IT-datacentre operations.

The project development strategy now being championed by prime minister Erna Solberg's conservative-led government, under its Norway As A Data Centre Nation (NADCN) plan, represents a shot across the collective bow of Denmark and Sweden."

United States of America

Internet governance

10.04.18

Reuters

Senate plans future hearing on Cambridge Analytica, other firms

Following its hearings with Facebook, the Senate has now stated its intent to hold hearings with other companies involved in the user data scandal, including Cambridge Analytica.

"The U.S. Senate Commerce Committee plans to hold a future hearing on Cambridge Analytica and other companies that may have improperly obtained Facebook Inc user data, the chairman of the panel said on Tuesday.

"There are plenty of questions about the behavior of Cambridge Analytica, and we expect to hold a future hearing on Cambridge and similar firms," Senator John Thune said in a written statement ahead of Tuesday's hearing with Facebook chief executive Mark Zuckerberg."

Cybersecurity

10.04.18

SCMagazine

House Democrats beseech Ryan to compel DHS to provide all docs related to Russian cyberattacks on state election systems

Paul Ryan, Speaker of the House of Representatives, has been asked by a group of leading Congressional Democrats to 'compel' Homeland Security to handover all documents on cyberattacks by Russia during the 2016 Presidential Election.

"A group of leading Democrats asked House Speaker Paul Ryan, R-Wis., to force the Trump administration to turn over documents related to Russia's cyberattacks on U.S. state election systems.

"We have been trying to work through the committee process, but we have faced two obstacles: the Trump Administration is refusing to provide the documents we requested, and Republicans appear to have no interest in compelling the Trump Administration to produce them," the Ranking Members of the Committees on Oversight and Government Reform, Judiciary, Intelligence,

House Administration, Homeland Security, and Foreign Affairs, wrote in a letter to *Ryan.*

06.04.18

Nextgov

[As Atlanta Recovers From Ransomware Attack, Georgia Looks to Boost Cyber Collaboration]

Georgia's Cybersecurity Workforce Academy is expanding to help local governments avoid cyberattacks in the future, following a recent attack in Atlanta.

"Local officials in Atlanta haven't asked for the Georgia Technology Authority's help since City Hall was hit with a ransomware attack on March 22, but the state's Cybersecurity Workforce Academy could assist local governments in avoiding similar crises in the future.

The city had until March 28 to transfer 6 bitcoins, worth about $51,000, to a bitcoin wallet disabled days before the deadline—lest the hackers encrypting some government systems delete the data they had access to."

Privacy

06.04.18

Nextgov

[Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security]

A survey released by Accenture has revealed that over 60% of citizens surveyed do not have confidence in their governments' ability to prevent cyberattacks and protect their data.

"In the face of relentless security threats, how can government preserve faith in its ability to protect citizen data?

A recent Accenture survey of more than 6,000 citizens across the United States, France, Germany, Australia, Singapore and the United Kingdom found that almost two-thirds (62 percent) of respondents are less confident today in their government's ability to defend their personal information against a security breach or a cyberattack than they were a year ago. Meanwhile, only 40 percent of survey respondents are confident that law enforcement agencies can protect them against cyber crime."

10.04.18

SCMagazine

Facebook slapped with class action suit over privacy, data gathering infractions

Mark Zuckerberg of Facebook has appeared before Congress this week over data privacy complaints following the Cambridge Analytica scandal. As a consequence, the US District Court in California has filed a class action lawsuit.

"Facebook "stood idly by" while Cambridge University professor Aleksandr Kogan raided user accounts through a quiz app and shared the information with data analytics firm Cambridge Analytica and "made only the weakest attempts to prevent further access to this data," according to a class action lawsuit filed in a U.S. District Court in California.

The complaint accuses the social media firm – whose CEO Mark Zuckerberg is testifying before Congress today about the Cambridge Analytica fiasco, the company's data collection and sharing practices and the steps it has taken to tighten privacy and data protection – of violating its own policies and privacy law."

06.04.18

South China Morning Post

Hundreds of thousands of Delta customers had their data exposed during a major cyber attack

A data hack on the airline revealed that thousands of customers may have had their data exposed. Payment information may be included in the personal information according the Delta.

"Delta Air Lines confirmed that payment information belonging to its customers may have been compromised after a cyber attack on a third-party chat service used by the airline.

According to Delta, "several hundred thousand" customers may have had their names, addresses, and payment card information exposed."

Internet Inclusion

No new items of relevance.

Pan-Asia

Internet governance

10.04.18

Channel News Asia

Anti-trust case against Google in India goes to appeal

India has ruled that a 'search bias' was used by Google, to which the internet company has appealed. The initial fine was around $21 million, however, Google has disagreed with the ruling.

"*Google has appealed against a ruling by India's competition watchdog that found it guilty of "search bias", while the website that brought the case also challenged the outcome, complaining the online search giant had got off too lightly.*

In February, the Competition Commission of India (CCI) fined Google 1.36 billion rupees (US$21 million), saying it was also abusing its dominance by giving its own online airline flight search product an unfair advantage over rivals."

Cybersecurity

07.04.18

Reuters

Iran hit by global cyber attack that left U.S. flag on screens

A US flag has been left on screens across Iran following a large cyberattack. The IT Ministry of Iran stated that a message of "don't mess with our elections" also appeared alongside the flag.

"Hackers have attacked networks in a number of countries including data centers in Iran where they left the image of a U.S. flag on screens along with a warning: "Don't mess with our elections", the Iranian IT ministry said on Saturday.

"The attack apparently affected 200,000 router switches across the world in a widespread attack, including 3,500 switches in our country," the Communication and Information Technology Ministry said in a statement carried by Iran's official news agency IRNA."

06.04.18

Channel News Asia

Financial institutions reminded to stay vigilant against cybersecurity threats: MAS

A reminder on vigiliance against cyberattacks has been issued by the Monetary Authority of Singapore, amidst a series of growing attacks across the globe. The MAS has been working with financial firms to deepen their cybersecurity.

"The Monetary Authority of Singapore (MAS) on Friday (Apr 6) issued an advisory to remind financial institutions to remain vigilant against cybersecurity threats. This follows recent reports of cyber incidents overseas where attackers attempted fraudulent fund transfers using the SWIFT system - a messaging platform that banks use to communicate payment instructions to each other.

MAS' Chief Cyber Security Officer Tan Yeow Seng said: "The recent cyber incidents present yet another reminder of the constant cyber threats to our financial sector. It is important for all financial institutions to be vigilant."

Privacy

05.04.18

NetworkAsia

These APAC countries have the harshest penalties for data breaches

An IDC brief has revealed that Singapore leads amongst APAC countries in issuing the toughest penalties on breaches of data. Japan, India and Thailand were amongst the lowest.

"Singapore, Australia, and Hong Kong are the top markets that incur the harshest penalties for data breaches as a percentage of the country's gross domestic product (GDP), while Japan, India and Thailand are at the bottom of the scale, according to an IDC InfoBrief, Data Risk Management Barometer – Gauging Asia-Pacific's Potential.

Conducted by global market intelligence firm IDC for Dell EMC, the study reveals the severity of financial penalties for non-compliance with data privacy legislation across key APJ markets."

05.04.18

Straitstimes

Information of over 65,000 Singapore Facebook users may have been improperly shared with Cambridge Analytica

Singapore has faced improper data access on its Facebook users by Cambridge Analytica. Over 65,000 users were involved in the breach.

"Information from the accounts of more than 65,000 Facebook users in Singapore might have been "improperly shared" with data analytics company Cambridge Analytica, prompting the local privacy watchdog to step in and look into the matter.

The social media giant said on Thursday (April 5) that the information of 65,009 Facebook users here was likely affected in the growing data breach involving Cambridge Analytica, a political consultancy firm which applies data mining and analysis to elections."

06.04.18

Nextgov

Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security

A survey released by Accenture has revealed that over 60% of citizens surveyed do not have confidence in their governments' ability to prevent cyberattacks and protect their data.

"In the face of relentless security threats, how can government preserve faith in its ability to protect citizen data?

A recent Accenture survey of more than 6,000 citizens across the United States, France, Germany, Australia, Singapore and the United Kingdom found that almost two-thirds (62 percent) of respondents are less confident today in their government's ability to defend their personal information against a security breach or a cyberattack than they were a year ago. Meanwhile, only 40 percent of survey respondents are confident that law enforcement agencies can protect them against cyber crime."

10.04.18

OpengovAsia

New collaboration in Singapore to develop framework for safe and secure data exchange

A collaboration between IMDA, PwC and DEX has led to an attempt at creating a new data exchange framework that is safe and secure. The merge comes during a period of increased data breaches, aiming to make the handling and sharing of data more secure.

"Singapore's Info-communications Media Development Authority (IMDA), PricewaterhouseCoopers (PwC) Singapore and Singapore-based startup, DEX have entered into a collaboration to co-develop a Trusted Data Framework for safe, transparent, auditable and secure data exchange, that is compliant to regulations and scalable. (According to Channel NewsAsia, this model will not be the only project supported by IMDA.)

A blog post on Medium by Dex describes the objective of the collaboration as addressing trust and security concerns and introducing a new model where data providers and consumers can transact in a safe and secure manner to solve common social and business challenges."

Internet Inclusion

09.04.18

Channel News Asia

Rakuten gets government approval for wireless operations

Japanese e-commerce firm Rakuten has won a series of mobile service contracts as it looks to grow its business in other markets.

"Rakuten Inc said on Monday it won government approval to offer mobile services as the Japanese e-commerce company expands its business into a market dominated by three major carriers.

Rakuten, which has also entered new areas such as online securities trading, aims to start offering mobile services in October 2019. The government hopes a new entrant will intensify competition in a market led by NTT DoCoMo Inc, KDDI Corp and SoftBank Group Corp."

06.04.18

South China Morning Post

[Qingdao store owners providing Wi-fi to customers ordered to switch to government-verified routers]

Cyber Cafes and other wifi providing shops in the city of Qingdao have been ordered to install government-verified wifi routers in order to comply with cybersecurity and counterterrorism regulations.

"Stores offering Wi-fi to customers in eastern China's Qingdao city have received an order from the local police asking them to replace their routers with government-verified ones.

Businesses refusing to replace their routers will face fines of up to 100,000 yuan (US$18,589), according to a statement issued by a district police station under the Qingdao Public Security Bureau. The government will provide the store owners with the new routers, which are powered by Qualcomm chips, with the cost of the router and its installation fully covered."

Rest of the World

Internet governance

09.04.18

The Guardian Nigeria

Nigeria's ICT market loses billions as foreign firms control 80% share

The Guardian(Nigeria) has reported that only 20% of the technology and digital sector in Nigeria is controlled by native companies. Over 80% of the market is led by foreign firms, consequently causing the nation to suffer vast loses in possible revenue.

"*Despite the enormous growth and influence Nigeria's Information and Communications Technology (ICT) sector has recorded in the last 20 years, activities of local firms remain low, making foreign firms to continue to dominate.*

Currently, foreign brands, especially in the computing segment, control over 80 per cent of the market, leaving about 20 per cent to some indigenous players."

Cybersecurity

06.04.18

Nextgov

Deterring Russian Hacking Will Take More Than Latest Sanctions, Experts Say

New sanctions deployed on Russia by nations, particularly the USA, have been dismissed as not enough to prevent their hacking and cyberattacks. Top cyber officials have suggested that it is a step forward but more needs to be done.

"Sanctions the Trump administration announced Friday against Russian government officials and oligarchs are a major step forward in U.S. efforts to curb Russian cyber aggression.

Those sanctions alone, however, are unlikely to change Russian behavior in cyberspace, Russia watchers told Nextgov. "It's a start, but this is a long campaign that's going to last for years," said Jim Lewis, a top cyber official at the Center for Strategic and International Studies who previously worked for the State and Commerce departments."

Privacy

06.04.18

Nextgov

Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security

A survey released by Accenture has revealed that over 60% of citizens surveyed do not have confidence in their governments' ability to prevent cyberattacks and protect their data.

"In the face of relentless security threats, how can government preserve faith in its ability to protect citizen data?

A recent Accenture survey of more than 6,000 citizens across the United States, France, Germany, Australia, Singapore and the United Kingdom found that almost two-thirds (62 percent) of respondents are less confident today in their government's ability to defend their personal information against a security breach or a cyberattack than they were a year ago. Meanwhile, only 40 percent of survey respondents are confident that law enforcement agencies can protect them against cyber crime."

05.04.18

Reuters

Australia begins privacy investigation into Facebook

Australia has become the latest country to begin an investigation into Facebook's activities in data privacy and access. The move follows news that around 300,000 Australian's had their data accessed illegally.

"Australia on Thursday said it had begun an investigation to decide whether social media giant Facebook Inc (FB.O) breached its privacy laws, after the company confirmed data from 300,000 Australian users may have been used without authorization.

Personal information of up to 87 million users, mostly in the United States, may have been improperly shared with political consultancy Cambridge Analytica, Facebook said on Wednesday, exceeding a media estimate of more than 50 million."

Internet Inclusion

11.04.18

The Guardian Nigeria

Tech4Dev, Microsoft Nigeria to train over 500,000 young Nigerians on digital skills

A Basic Digital Education Initiative is set to be rolled out across Nigeria, aiming to reach over 500,000 people. Microsoft is supporting the initiative as a way to boost digital skills in the nation.

"Over 500,000 young individuals' resident in Nigeria are to benefit from the Basic Digital Education Initiative (BDEI), an Initiative of Tech4Dev and supported by Microsoft.

This announcement was made at the official launch event held at the Civic Towers, Victoria Island, Lagos and had in attendance the former executive Governor of Ondo State, Dr. Olusegun"

10.04.18

The Guardian Nigeria

'There are more opportunities to transform Nigerian industries'

Microsoft has suggested that digital transformation across Nigeria still has the potential to impact industries across the whole of Africa. The company has stated its intension to help grow digital markets.

"Technology giant, Microsoft has disclosed that Nigeria has more opportunities to transform her industries digitally, which, it believes would impact positively on the African continent.

Besides, the company also revealed that Nigeria remains an important innovation hub influencing the digital transformation of the entire sub-region."

Global Institutions

08.04.18

APEC

Senior Officials Build Digital Resilience, Growth

Digitial strength has become central to APEC's new strategy to help new growth opportunities in the region. The 21 member nations have agreed that the way forward will be to secure a firm digital economy.

"Senior Officials from the 21 APEC member economies are taking the next steps to advance digitally driven trade and development. They are intent on securing new growth opportunities vital to improving livelihoods across the Asia-Pacific.

Meeting for the first time in 2018, in the aftermath of the strongest earthquake in Papua New Guinea's history and amid looming uncertainties in the global trading environment, officials offered sympathies for the disaster victims. They also underscored the urgency of revitalizing policy regimes as a force for recovery and resilience in the digital economy."

07.04.18

APEC

Singapore Joins APEC Data Privacy System

APEC's privacy rules system has gained another new member in Singapore. The new membership came after the organisation found the nation's personal data protection law to be firmly aligned with its own.

"Singapore has become the latest member of the APEC Cross-Border Privacy Rules System, a further boost for e-commerce growth and the protection of sensitive online consumer data in the Asia-Pacific.

The move recognizes that Singapore's personal data protection law is aligned with the system to facilitate data flows between economies and prevent accidental disclosure and misuse of personal data derived from transactions online. These range from internet banking, sales and transfers of education, health and travel records, to social media posts, instant messaging and GPS signals."

Diary Dates

RSA – 16.04.18–20.04.18

San Francisco, USA

Data Centre Risk Radar- Technical Skills Shortage – 26.04.18

London, England

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal

Cyber in the Digital Economy – 17.05.18

London, England

2018 Digital Festival – 21.05.18

London, England

Diversity in Technology – 24.05.18

London, England

EuroDIG – 05.06.18-06.06.18

Tbilisi, Georgia

Data Centres Risk Radar – 24.06.18

London, England