



7 February 2018

Synopsis

Scroll to read full summaries with links to news articles.

The **US-China Business Council** has urged the Chinese Government to loosen its **cybersecurity** rules with the adoption of a narrower definition of 'national security' in order to widen **internet**, cloud and technology **access** and trade.

The newly established **cybersecurity** agency in **Indonesia** is set to recruit a vast number of staff as its looks to set its ambitions high. The agency is still not clear on whether it will be able to prosecute, but it aims to identify the criminals and crimes.

Following the passing of a Bill in the **Singaporean Parliament** this week, a new head of **cybersecurity** will be given significant powers. They will be able to access **information** that would otherwise be confidential, from organisations in order to carry out investigations.

A number of countries and companies outside of the **EU** are still failing to see full compliance with the incoming **GDPR**. **EY's** report on the issue revealed that just 33% of countries and companies are currently compliant and ready for the **data protection** and **privacy regulations** that will be in place within a few months.

The **European Dialogue on Internet Governance** conference will be held in **Georgia's** capital this year. It will provide a platform to allow officials and states to plan on better governance and standards for the internet in **Europe**.

The **Safer Internet Day Programme** launched around the world this week is aiming to promote the safer use of internet for young people. The programme developed from an agreement between the **European Commission** and **Homeland Security** that will address, amongst other things, **cyber issues**.

The **Polish Government** and the **International Telecommunication Union (ITU)** have collaborated to map out the **ICT infrastructure** in the nation. The collaboration will allow for Poland to understand the current connectivity to the **internet** in the nation and develop new initiatives to **broadband access**.

Plans for a new **cyberspace** and **digital economy** bureau have been set in motion by **Rex Tillerson**, Secretary of State. It aims to unify a number of offices that have remit over **cyber issues** and to tackle the ever rising issue of attacks.

A bill imposing **net neutrality** restrictions on **internet service providers** has been passed by the Senate. Despite its passing, electronic rights group the **Electronic Frontier Foundation** have suggested that it could be thrown out by the courts.

Google has launched a programme for a number of schools in **Nigeria** to promote the safer use of the **internet**. It will aim to educate people on the risks of and on the Internet and how they can better use it in a safer way.

Following reports that a large percentage of **Nigeria**, over 50% of the population, does not have access to the Internet, The **Internet Society** has outlined new plans to increase **internet access**.

The **European Commission** has published its implementation regulation for the **NIS Directive**, **ENISA** has highlighted its contribution to the formation of these regulations and their implementation.

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

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

7 February 2018

Table of Contents

Synopsis	1
Europe	4
Internet governance.....	4
Cybersecurity	5
Privacy.....	6
Internet Inclusion	7
United States of America	9
Internet governance.....	9
Cybersecurity	9
Privacy.....	11
Internet Inclusion	12
Pan-Asia	13
Internet governance.....	13
Cybersecurity	13
Privacy.....	15
Internet Inclusion	17
Rest of the World	18
Internet governance.....	18
Cybersecurity	19
Privacy.....	20
Internet Inclusion	20
Global Institutions	21
Diary Dates	23

Europe

Internet governance

05.02.18

Georgia Today

[European Dialogue on Internet Governance to Be Held in Georgia](#)

The European Dialogue on Internet Governance conference will be held in Georgia's capital this year. It will provide a platform to allow officials and states to plan on better governance and standards for the internet in Europe.

"Georgia's capital Tbilisi is to host the European Dialogue on Internet Governance (EuroDIG) 2018 on June 4-6.

The information was released by Georgia's Ministry of Economy and Sustainable Development, which says that the preparatory meeting was held in Technopark, attended by the representatives of the Ministry of Economy, the EuroDIG, the International Internet Community (ISOC) and the International Organization for Domain Names (ICANN)."

05.02.18

NextGov

[Students Around the World Prepare to Celebrate Safer Internet Day](#)

The Safer Internet Day Programme launched around the world this week is aiming to promote the safer use of internet for young people. The programme developed from an agreement between the European Commission and Homeland Security that will address, amongst other things, cyber issues.

"That's the purpose of the [Safer Internet Day program](#). Held Tuesday, February 6, it's billed as a "worldwide event aimed at promoting the safe and positive use of digital technology for all users, especially children and teens." The program this year includes a conference held in Austin, Texas and Federal Communications Commissioner Mignon Clyburn will speak."

06.02.18

The Guardian

[EU data protection law may end up protecting scammers, experts warn](#)

Raj Samani chief scientist at McAfee has warned that the introduction of GDPR in May, could actually protect scammers and those that misuse the internet, arguing that the regulations will end the important transparency currently in place on the internet.

“Sweeping new European data protection regulations may have the accidental effect of protecting scammers and spammers by killing the WHOIS system used to link misdeeds online to real identities offline, security experts have warned.

The General Data Protection Regulation (GDPR), which comes into effect in May, contains a raft of measures intended to strengthen data protection for Europeans. But some of the new rights and responsibilities will conflict with decades-old technologies that have provided much-needed transparency on the internet, says Raj Samani, the chief scientist at cybersecurity firm McAfee.”

Cybersecurity

05.02.18

Europol

[International Crackdown On Anti-Spyware Malware](#)

A UK-led operation has successfully ended a hacking tool widely used by cybercriminals. It formerly allowed attackers to get control over a computer, but the UK National Crime Agency successful removed the Remote Access Trojan.

“A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim’s computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.”

07.02.18

SCMagazine

[FIC 2018: European cyber-security cooperation will endure post Brexit](#)

The director of France's cybersecurity agency has suggested that cybersecurity defences should go beyond the national level. He believes that while France has a duty to tackle cyber risks, so to do the European Commission and other groups within Europe, to work together on the issue.

"Guillaume Poupard, director general of ANSSI (Agence Nationale des Systèmes d'Information), France's cyber-security agency - an equivalent of the UK's NCSC but one which reports directly to the French Prime Minister - told SC Media UK during FIC 2018 that while cyber-security is a matter of national sovereignty, it should not stop at this level. "Cooperation between States is absolutely essential.

Within Europe, the European Commission and the different Member States are really keen to work together to develop cyber-security. At the European level he emphasises the need to put a cooperation network in place, currently underway with the European Agency (ENISA)."

Privacy

02.02.18

SCMagazine

[UK's Snoopers' Charter 'inconsistent with EU law' says Court of Appeal](#)

The EU Court of Appeal has found that the UK's 'Snoopers' Charter' is unlawful. The Act passed in 2014 allowed the UK Government to carry out vast surveillance and data collect operations in order to investigate crimes.

"Earlier this week the Court of Appeal found the UK's Data Retention and Investigatory Powers Act 2014, commonly known as the Snoopers' Charter, unlawful as far as the prevention, investigation, detection and prosecution of serious crimes are concerned.

The Data Retention and Investigatory Powers Act was passed in 2014 to enable the government to carry out mass surveillance and to collect data belonging to citizens to prevent or investigate serious crimes in the UK."

01.02.18

ComputerWeekly

[€7.1m EU Data Pitch accelerator recruits 18 startups](#)

100,000 euros worth of funding for 18 separate start-ups has been given by Data Pitch, a EU programme. The programme is part of the Horizon 2020 initiative.

“[Data Pitch](#), a €7.1m three-year European Union (EU) programme aimed at supporting startups, has announced €100,000 in funding for each of 18 companies across Europe.”

The University of Southampton, the [Open Data Institute](#), Portuguese company Beta-i, and French data marketplace platform Dawex have combined forces to deliver the programme, which is funded by the EU’s Horizon 2020 research and innovation initiative.”

Internet Inclusion

01.02.18

ITU

[ITU and Poland sign agreement to map the country’s current ICT infrastructure](#)

The Polish Government and the International Telecommunication Union (ITU) have collaborated to map out the ICT infrastructure in the nation. The collaboration will allow for Poland to understand the current connectivity to the internet in the nation and develop new initiatives to broaden access.

“The International Telecommunication Union (ITU) and the Government of Poland’s Office of Electronic Communication (UKE) signed an agreement on 25 January 2018 to produce updated comprehensive and interactive terrestrial transmission maps of Poland’s information and communication technology (ICT) infrastructure.”

The signing extends for a further two years an existing agreement signed in November 2013. The new transmission maps produced through this extension will take stock of Poland’s national broadband connectivity including optical fibres and microwaves – as well as other key ICT sector metrics.”

07.02.18

ComputerWeekly

[Government must hurry to recruit digital skills needed for Brexit, says PAC](#)

A mass digital skills shortage is set to hit the UK as it prepares to leave the EU, according to the Public Accounts Committee. It reported that a robust plan is not in place to offset any issues.

“The government skills shortage, including the lack of digital skills, must be addressed to support the UK’s exit from the EU, the Public Accounts Committee (PAC) has found.

[The PAC report](#) on exiting the EU said the civil service needs to address the lack of skills urgently, pointing out that the current process has been “too slow”. “The Department for Exiting the European Union and the Cabinet Office do not have a robust enough plan to identify and recruit the people and skills needed quickly,” the report said.”

United States of America

Internet governance

05.02.18

NextGov

[Students Around the World Prepare to Celebrate Safer Internet Day](#)

The Safer Internet Day Programme launched around the world this week is aiming to promote the safer use of internet for young people. The programme developed from an agreement between the European Commission and Homeland Security that will address, amongst other things, cyber issues.

"That's the purpose of the [Safer Internet Day program](#). Held Tuesday February 6, it's billed as a "worldwide event aimed at promoting the safe and positive use of digital technology for all users, especially children and teens." The program this year includes a conference held in Austin, Texas and Federal Communications Commissioner Mignon Clyburn will speak."

Cybersecurity

06.02.18

NextGov

[State Dept. Reverses Course, Plans to Launch Cyber and Digital Economy Bureau](#)

Plans for a new cyberspace and digital economy bureau have been set in motion by Rex Tillerson, Secretary of State. It aims to unify a number of offices that have remit over cyber issues and to tackle the ever rising issue of attacks.

"Secretary of State Rex Tillerson plans to launch a new cyberspace and digital economy bureau, seemingly reversing course under congressional pressure after he shuttered the department's cyber coordinator's office in August."

Tillerson announced plans for the new bureau in a letter to House Foreign Affairs Chairman Ed Royce, R-Calif., delivered in the middle of a Tuesday hearing on cyber diplomacy issues. Among the witnesses testifying at that hearing was the department's ousted cyber coordinator Chris Painter."

06.02.18

SCMagazine

[Study claims most businesses lack cyber expertise to prevent attacks](#)

A survey has revealed that most businesses do not have enough cybersecurity expertise to prevent attacks and protect customers. Hiscox, a cyber insurance company, found just 11% of companies scored high enough to qualify as 'expert'.

"Cyber insurance company Hiscox surveyed 4,000 organizations and rated them on a cyber readiness model that divided respondents into 'cyber novices', 'cyber intermediates' and 'cyber experts' and found that only 11 percent scored highly enough in both cyber security strategy and the quality of its execution to qualify as cyber security 'experts'

Nearly three quarters, 73 percent, fell into the novice category but not for underinvestment in technology but because firms are failing to support their investment in security technology with a formal strategy, sufficient resourcing and training, and sound processes."

02.02.18

NextGov

[Booz Allen Hamilton Wins \\$621 Million DHS Cyber Contract](#)

Booz Allen Hamilton has been awarded a 6 year contract with Homeland Security to lead on Government cybersecurity. It will aim to enhance cybersecurity across all Government departments and help them to respond to suspect activity.

"The Homeland Security Department granted Booz Allen Hamilton a \$621 million, six-year contract Friday to lead the next phase of a major government wide cybersecurity program.

Under the program, called Continuous Diagnostics and Mitigation, or CDM, Homeland Security provides a suite of cybersecurity tools that help agencies monitor and respond to suspicious activity on their networks. The program feeds alerts about that activity into a central agency dashboard."

Privacy

05.02.18

All Africa

[Nigeria: Report Reveals Slow Compliance With EU Data Protection Regulation](#)

A number of countries and companies outside of the EU are still failing to see full compliance with the incoming GDPR. EY's report on the issue revealed that just 33% of countries and companies are currently compliant and ready for the data protection and privacy regulations that will be in place within a few months.

“With barely four months to the deadline on EU General Data Protection Regulation (GDPR) compliance, Global companies, including African countries are still unprepared to comply with the regulations, according to a survey report conducted recently by Ernst & Young (EY), a global leader in assurance, tax, transaction and advisory services.

According to the report, 78 per cent of those surveyed, consider data protection and data privacy compliance a growing concern, yet only 33 per cent of respondents have a plan in place for GDPR.”

06.02.18

Government Technology

[How Code for America, and a Lot of Partners, are Working to Smooth Out Kinks in the Safety Net](#)

Code for America is working towards developing software to help data privacy and safety. Despite their hopes, developments have been difficult with data, privacy and security issues being more challenging than first thought.

“Not surprisingly, when it comes to government technology, integrated benefits enrollment is more a lofty goal than a reality. Yet it's a challenge that Code for America (CfA), which matches cities with software developers to solve a problem, has decided to tackle.

CfA is working with the Chan Zuckerberg Initiative, the philanthropic organization started by Facebook's co-founder and his wife, as well as with the tech startup Nava, the Centers for Medicare and Medicaid Services, the U.S. Department of Health and Human Services, and the state of Michigan. CfA hopes to strip out the complexity — and cost — that gives online benefits enrollment such a bad name. The goal then is to design a simple way to enroll people who are eligible for both Medicaid and food stamps.”

Internet Inclusion

06.02.18

Arstechnica

[Charter's gigabit cable—starting at \\$105—is coming to over 40 million homes](#)

50 million homes and businesses are set to benefit from Charter's cable network. The network will allow for fast internet access for millions across the US.

"Charter's cable network extends to about 50 million homes and businesses across the US, and nearly all of them should have the opportunity to buy gigabit-speed cable Internet by the end of 2018. So far, prices for the service range from \$105 to \$125.

"By year-end, we'll offer gigabit services in virtually everywhere we serve at all 50 million passings," Charter CEO Tom Rutledge told investors in an earnings call Friday. The number of residential units among those 40 million locations is somewhere above 40 million. An earnings call transcript by Seeking Alpha is available [here](#), and Rutledge's remarks were [pointed out by news site Stop the Cap](#)."

01.02.18

Arstechnica

[California's net neutrality bill is vulnerable to legal attack, EFF says](#)

A bill imposing net neutrality restrictions on internet service providers has been passed by the Senate. Despite its passing, electronic rights group the Electronic Frontier Foundation have suggested that it could be thrown out by the courts.

"The California State Senate this week passed a bill that would [impose net neutrality restrictions on Internet service providers](#), but the Electronic Frontier Foundation (EFF) warns that the proposed law has a high chance of being thrown out in court.

"While well-intentioned, the legislators sadly chose an approach that is vulnerable to legal attack," EFF Legislative Counsel Ernesto Falcon wrote in a post yesterday. Falcon also provided California senators with a longer [legal analysis](#) a few weeks before the vote."

Pan-Asia

Internet governance

05.02.18

NextGov

[Students Around the World Prepare to Celebrate Safer Internet Day](#)

The Safer Internet Day Programme launched around the world this week is aiming to promote the safer use of internet for young people. The programme developed from an agreement between the European Commission and Homeland Security that will address, amongst other things, cyber issues.

"That's the purpose of the [Safer Internet Day program](#). Held Tuesday February 6, it's billed as a "worldwide event aimed at promoting the safe and positive use of digital technology for all users, especially children and teens." The program this year includes a conference held in Austin, Texas and Federal Communications Commissioner Mignon Clyburn will speak."

Cybersecurity

05.02.18

Straitstimes

[Indonesia's new cybersecurity agency looks to recruit staff of hundreds](#)

The newly established cybersecurity agency in Indonesia is set to recruit a vast number of staff as its looks to set its ambitions high. The agency is still not clear on whether it will be able to prosecute, but it aims to identify the criminals and crimes.

"Indonesia's recently established cyber security agency will recruit hundreds of personnel in the coming months, its chief said on Friday (Jan 5).

The agency has been set up amid rising concern over online misinformation and hoaxes ahead of simultaneous local elections set to take place across the country later this year. The head of the National Cyber and Encryption Agency, Djoko Setiadi, who was sworn in this week, will report directly to President Joko Widodo."

06.02.18

ChannelNewsAsia

[54% of Singaporean children exposed to at least 1 cyber risk](#)

Cyber risks have been working their way through to children, with a new report revealing that around 54% of children in Singapore being exposed to such risks.

“A new study released on Tuesday (Feb 6) showed that 54 per cent of Singapore children aged between eight and 12 are exposed to at least one cyber-risk, which includes cyberbullying, video game addiction, offline meetings and online sexual behaviour.

The Singapore findings of the 2018 DQ Impact Report issued by DQ Institute, an international think tank created to improve digital education, found that the 54 per cent figure is just below the global average of 56 per cent.”

05.02.18

Straitstimes

[Bill passed to grant cybersecurity commissioner powers to obtain confidential information for investigations](#)

Following the passing of a Bill in the Singaporean Parliament this week, a new head of cybersecurity will be given significant powers. They will be able to access information that would otherwise be confidential, from organisations in order to carry out investigations.

“Singapore will have a cybersecurity czar who is empowered to obtain confidential information from local organisations to investigate suspected cyber attacks, under a Bill passed in Parliament on Monday (Feb 5).

Nineteen MPs spoke in support of the Cyber Security Bill, during a lengthy three-hour debate. Many of them expressed concern, however, about the broad powers of that the new Commissioner of Cybersecurity - Mr. David Koh, chief executive of the Cyber Security Agency of Singapore - will wield.”

01.02.18

ChinaDaily

[Mobile Internet, cybersecurity highlighted in China's internet report](#)

A report on China's Internet development over 2017 revealed that there was a growth in the strength of cybersecurity. This followed the introduction of a cybersecurity law across the country that imposed a series of regulations.

“New applications on mobile internet and the strengthened cybersecurity management were highlighted in a statistical report on China's Internet development in 2017.

The report, the 41st of a bi-annual series, was released by the China Internet Network Information Center (CNNIC) Wednesday.”

07.02.18

Securitybrief Asia

[Japan firm Nihon Cornet to deliver BlackRidge next-gen cybersecurity](#)

A new initiative between two technology firms, Nihon Cornet and BlackRidge, will aim to increase technology developments in Japan. Cybersecurity is at the forefront of the initiative.

“Japan-based network and cybersecurity provider Nihon Cornet Technology will work with global cyber defense provider BlackRidge Technology on a new initiative that will bring BlackRidge technology to Japan.

Nihon Cornet is now an official reseller and integrator for BlackRidge Technology's next-generation cybersecurity solutions for Japan commercial and government customers. According to Nihon Cornet general manager Hideo Matsumoto, the company is committed to offering competitive solutions for both network and cybersecurity.”

Privacy

05.02.18

All Africa

[Nigeria: Report Reveals Slow Compliance With EU Data Protection Regulation](#)

A number of countries and companies outside of the EU are still failing to see full compliance with the incoming GDPR. EY's report on the issue revealed that just 33% of countries and companies are currently compliant and ready for the data protection and privacy regulations that will be in place within a few months.

“With barely four months to the deadline on EU General Data Protection Regulation (GDPR) compliance, Global companies, including African countries are still unprepared to comply with the regulations, according to a survey report conducted recently by Ernst & Young (EY), a global leader in assurance, tax, transaction and advisory services.

According to the report, 78 per cent of those surveyed, consider data protection and data privacy compliance a growing concern, yet only 33 per cent of respondents have a plan in place for GDPR.”

06.02.18

NextGov

[China's Surveillance State Should Scare Everyone](#)

China's surveillance system algorithm has been developing, allowing the Government to collect and analyze information on its citizens. It is aiming to create a 'citizen score' that will try to incentivize 'good' behavior.

“Imagine a society in which you are rated by the government on your trustworthiness. Your “citizen score” follows you wherever you go. A high score allows you access to faster internet service or a fast-tracked visa to Europe. If you make political posts online without a permit, or question or contradict the government's official narrative on current events, however, your score decreases. To calculate the score, private companies working with your government constantly trawl through vast amounts of your social media and online shopping data.”

05.02.18

Securitybrief Asia

[APEJ leads market demand for IoT security products](#)

As countries across the world are looking to increase their security and privacy, the market for the 'Internet of Things' will dramatically increase. Recent reports have suggested it will be worth over \$50 billion in ten years time, with Asia Pacific being the fastest growing area for the market.

“According to the Internet of Things (IoT) Security Product Market: Smart Grid Application Segment Projected to Register a High CAGR During the Forecast Period: Global Industry Analysis 2012-2016 and Opportunity Assessment 2017-2027 report, the growth will be driven by continuous launches of IoT security offerings by enterprises, an increase in the number of service providers and the emergence of niche players in the market.”

Internet Inclusion

05.02.18

South China Morning Post

[China's tough cyber rules raise risk of infiltration, US business group says](#)

The US-China Business Council has urged the Chinese Government to loosen its cybersecurity rules with the adoption of a narrower definition of 'national security' in order to widen internet, cloud and technology access and trade.

"A leading US business group has urged Beijing to loosen limits on data flow and storage that raise the risk of security breaches for foreign companies. The call from the US-China Business Council is part of a series of detailed recommendations to the Chinese government in response to its controversial cybersecurity law, which came into effect in June.

In a report released on Monday, the council said China should follow best international practice by opening access to cloud computing services, levelling the playing field in technology procurement and allowing foreign firms to send copies of data abroad for analysis and processing."

07.02.18

Economic Times India

[Number of people getting connected internet in India to double](#)

India is set to see a vast increase in the number of people with access to the internet. Google India has started developments on a solution to internet access that should allow 600-650 million of India's population to have access to the internet by 2020.

"The number of people getting connected to internet in India through smartphones is all set to double to 600-650 million by 2020, making it a challenge of opportunities to come up with technological solutions to meet the scenario, a top Google India official said here today.

Rajan Anandan, Google India Managing Director and Vice-President (South East Asia), was speaking after launching Kerala's first incubator "Mobile 10x Hub", an initiative by Kerala Startup Mission to create a mobile app-based ecosystem, on the sidelines of Kerala Mobile App Conference 2018 (K-MAC 2018) at UL CyberPark here today."

Rest of the World

Internet governance

05.02.18

NextGov

[Students Around the World Prepare to Celebrate Safer Internet Day](#)

The Safer Internet Day Programme launched around the world this week is aiming to promote the safer use of internet for young people. The programme developed from an agreement between the European Commission and Homeland Security that will address, amongst other things, cyber issues.

"That's the purpose of the [Safer Internet Day program](#). Held Tuesday February 6, it's billed as a "worldwide event aimed at promoting the safe and positive use of digital technology for all users, especially children and teens." The program this year includes a conference held in Austin, Texas and Federal Communications Commissioner Mignon Clyburn will speak."

06.02.18

NewTimes

[Experts move to bridge digital standards gaps in Africa](#)

A series of tech experts across Africa have joined together to call for better standards on the use of communication and technology. They suggested that shared international standards are needed to accommodate the use of all technologies in use and being developed.

"Different experts from across Africa are pushing for more standards that would see countries benefit fairly from the growth of information and communication technologies (ICTs).

This was one of the issues that transpired at a one-day conference held in Kigali yesterday that tackled bridging the standardisation gap on the African continent and beyond."

Cybersecurity

07.02.18

The Guardian

[Google offers help on safer Internet](#)

Google has launched a programme for a number of schools in Nigeria to promote the safer use of the internet. It will aim to educate people on the risks of and on the internet and how they can better use it in a safer way.

“To celebrate Safer Internet Day 2018, Google, in collaboration with the National Film and Video Censors Board (NFVCB), has organised an interactive programme for over 150 students from 10 public schools and five private schools across the Federal Capital Territory of Nigeria, Abuja.

Google’s Policy & Government Relations Manager, Titi Akinsanmi, said: “This year’s event, themed, ‘Create, connect and share respect: A better internet starts with you’, reflects our aim to train and inform active internet users in Nigeria about the dangers of online technologies and how users can keep themselves safe online.”

07.02.18

Securitybrief Asia

[Apple, Cisco, Aon & Allianz make a play for cyber risk management services](#)

A number of large corporations are working together to create a new cybersecurity management market. Bringing together their different expertise in various different areas, Apple, Cisco, Aon and Allianz are aiming to create a new service to help businesses tackle cyber risk.

“A joint effort between Apple, Cisco, Aon and Allianz is set to shake up the cyber risk management market by bringing together technology, cyber resilience evaluation services and cyber insurance.

The four companies believe that cyber threats are not the only problems for cybersecurity risk. Low adoption of cyber insurance, a fragmented security tech market, the security skills shortage and any active adversary all make up a melting pot of problems for organisations trying to understand and manage risk.”

Privacy

05.02.18

All Africa

[Nigeria: Report Reveals Slow Compliance With EU Data Protection Regulation](#)

A number of countries and companies outside of the EU are still failing to see full compliance with the incoming GDPR. EY's report on the issue revealed that just 33% of countries and companies are currently compliant and ready for the data protection and privacy regulations that will be in place within a few months.

“With barely four months to the deadline on EU General Data Protection Regulation (GDPR) compliance, Global companies, including African countries are still unprepared to comply with the regulations, according to a survey report conducted recently by Ernst & Young (EY), a global leader in assurance, tax, transaction and advisory services.

According to the report, 78 per cent of those surveyed, consider data protection and data privacy compliance a growing concern, yet only 33 per cent of respondents have a plan in place for GDPR.”

Internet Inclusion

07.02.18

The Guardian

[Internet Society unveils plan to deepen accessibility for Nigerians](#)

Following reports that a large percentage of Nigeria, over 50% of the population, does not have access to the internet, The Internet Society has outlined new plans to increase internet access.

“The Internet Society (ISOC) Nigeria, has expressed its commitment to ensuring that all Nigerians have access to Internet. The Society, while warning that Nigeria has a lot to lose if it fails to utilise the opportunities that Internet presents, regretted that most Nigerians have no access to internet and that this retards the development of the country.

The Guardian checks showed that about 93 million out of the estimated 180 million people in the country have access to Internet, majorly through the narrow band.”

Global Institutions

01.02.18

ITU

[ITU and Poland sign agreement to map the country's current ICT infrastructure](#)

The Polish Government and the International Telecommunication Union (ITU) have collaborated to map out the ICT infrastructure in the nation. The collaboration will allow for Poland to understand the current connectivity to the internet in the nation and develop new initiatives to broaden access.

“The International Telecommunication Union (ITU) and the Government of Poland's Office of Electronic Communication (UKE) signed an agreement on 25 January 2018 to produce updated comprehensive and interactive terrestrial transmission maps of Poland's information and communication technology (ICT) infrastructure.

The signing extends for a further two years an existing agreement signed in November 2013. The new transmission maps produced through this extension will take stock of Poland's national broadband connectivity including optical fibres and microwaves – as well as other key ICT sector metrics.”

05.02.18

Europol

[International Crackdown On Anti-Spyware Malware](#)

A UK-led operation has successfully ended a hacking tool widely used by cybercriminals. It formerly allowed attackers to get control over a computer, but the UK National Crime Agency successfully removed the Remote Access Trojan.

“A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.”

02.02.18

ENISA

[ENISA contributes to the development of groundbreaking EU cybersecurity regulation on Digital Service Providers in the context of the NIS Directive](#)

The European Commission has published its implementation regulation for the NIS Directive, ENISA has highlighted its contribution to the formation of these regulations and their implementation.

“The European Commission has published the [implementing regulation for the application of Directive \(EU\) 2016/1148 pursuant Art 16\(8\) of NIS Directive](#). This initiative provisions further specification of the elements to be taken into account by Digital Service Providers (DSPs) for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.”

The EU Cybersecurity ENISA closely supported the European Commission’s Network and Information Systems Security Committee responsible for developing the implementing act.”

06.02.18

ENISA

[Strong cybersecurity culture as efficient firewall for organisations](#)

The Cybersecurity Culture in Organisations report has been released by ENISA. It aims to set out how cybersecurity can be enhanced in organisations and how they can better understand the threats and situations that face them

“ENISA’s [Cybersecurity Culture in Organisations](#) report is based on a multi-disciplinary research, conducted to better understand the dynamics of how cybersecurity culture can be developed and shaped within organisations.”

This research draws from different disciplines, including organisational sciences, psychology, law and cybersecurity as well as the knowledge and experiences of large European organisations. The report provides good practices, methodological tools and step-by-step guidance for those seeking to commence or enhance their organisation’s cybersecurity culture programme.”

Diary Dates

GDPR Summit – 30.01.18

London, England

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

Cybersecurity and Data Opportunities in Sub-Saharan Africa – 05.03.18

London, England

Living in the Internet of Things- Cybersecurity of the IoT – 28.03.18-29.03.18

London, England

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

EuroDIG – 05.06.18-06.06.18

Tbilisi, Georgia