19 July 2017

Synopsis

Scroll to read full summaries with links to news articles.

A new report from **Lloyd's** of London has estimated that a major global **cyberattack** could lead to the same economic damage as the 2012 US **Superstorm Sandy** inflicted, with over $53billion worth of economic losses likely.

The **UK's** Information Commissioner's Office has published its annual report, which amongst administrative reporting issues has identified the introduction of the EU's **General Data Protection Regulation** as a significant challenge for the year to come and has provided further guidance.

Although the **US** State Department has ruled out a formal partnership with **Russia** in **cybersecurity**, recent statements from **Tom Bossert**, Homeland Security Advisor at the White House indicate that the Trump administration remain open to further dialogue.

Tesla CEO **Elon Musk** has warned that **cybersecurity** poses a significant challenge to the future of **autonomous vehicles**, with security flaws potentially allowing hackers to control entire fleets of vehicles.

The **House of Representatives** Appropriations Committee has given its support to an amendment that will prevent the future warrantless **access** to **digital files** for law enforcement currently provided by exiting law.

The Government of **Indonesia** has instructed **internet service providers** in the country to prevent access to **Telegram** messenger, over fears that it is being used as a communication channel by **terrorists**.

The **Cyber Security** Agency of **Singapore** has conducted its **Cyber Star** exercise with over 200 sector leads and critical information infrastructure (CII) owners from 11 sectors in a bid to protect both public and private infrastructure.

China have moved to strengthen the country's **"Great Firewall"** with encrypted messaging program **WhatsApp** reported to no longer operate without the support of a **VPN**.

Several internet groups have begun to lobby the **Nigerian** Communications Commission on the topic of **net neutrality** as part of the regulator's current work to establish a code of practice for communications technologies.

Deakin University and **Dimension Data** are currently seeking submissions from **cybersecurity** startups from across the **APAC** region as part of a joint cybersecurity accelerator program established in Melbourne.

ITU have published a **Global ICT Regulatory** outlook for the first time, identifying global trends and their implications on different economies.

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

19 July 2017

Table of Contents

Europe

Internet governance

No new items of relevance

Cybersecurity

14.07.17

SC Media

Multiple vulnerabilities found in connected IoT home security device

Cybersecurity firm Bullguard has issued a report in which it has found multiple flaws in the iSmartAlarm security device that relies on IoT connectivity to provide its service.

"Security researchers have discovered a number of vulnerabilities in an internet-enabled burglar alarm that could see the device being remotely switched off by an attacker.

According to a blog post, Ilia Shnaidman , head of security research at Bullguard, said that the discovery of multiple flaws in iSmartAlarm is another example of a poorly engineered device that offers attackers an easy target."

17.07.17

Euractiv

Global cyber-attacks could spur $53 billion in losses

A new report from Lloyd's of London has estimated that a major global cyberattack could lead to the same economic damage as the 2012 US Superstorm Sandy, with over $53billion worth of economic losses likely.

"A major global cyber-attack could trigger an average of $53 billion (€46.30) of economic losses, a figure on par with a catastrophic natural disaster such as US Superstorm Sandy in 2012, Lloyd's of London said in a report on Monday (17 July).

The report, co-written with risk-modeling firm Cyence, examined potential economic losses from the hypothetical hacking of a cloud service provider and cyber-attacks on computer operating systems run by businesses worldwide."

17.07.17

Computer Weekly

IBM claims breakthrough in mainframe encryption

IBM's new Z mainframe is capable of running 12 billion encrypted transactions according the company in what they see as a major advancement in mainframe technology.

"The latest IBM Z mainframe enables organisations to encrypt all data all the time, and is capable of running more than 12 billion encrypted transactions a day, according to IBM.

The mainframe's new cryptographic capability now extends across any data, networks, or applications – such as the IBM Cloud Blockchain service – without any application changes or impact on performance, the company said."

17.07.17

SC Media

Lastline says cyber-pros have some gaps in their malware knowledge

A report of European cyber professionals by Lastline has found significant gaps in the capabilities of these experts to respond to malware attacks. One example given by the company was that only 70% of respondents identified that malware can avoid sandboxes.

"Security firm Lastline says it has identified significant gaps in the cyber-security knowledge of people working in the sector.

It conducted a survey of 326 cyber-professionals at InfoSecurity Europe 2017 and found a significant number had some gaps in their knowledge of current malware and its tactics."

19.07.17

SC Media

[More staff cyber-security aware following WannaCry devastation in May]

A new study across the UK, US, Germany and Australia has found that cybersecurity awareness has risen amongst decision makers and employees following recent global cyberattacks.

"The WannaCry attack may have laid waste to vast tracts of the NHS as well as other organisations and individuals, but it appears to have also focused attention on cyber-security in a way that hasn't been seen before.

That's according to a survey conducted by technology research firm Vanson Bourne on behalf of Clearswift in which 600 business decision makers and 1200 employees were asked about WannaCry. This included personnel in the UK, US, Germany and Australia."

19.07.17

Reuters

[London Stock Exchange Group tests blockchain for private company shares]

IBM and the London Stock Exchange have announced a new collaboration to use a blockchain platform to issue private shares to SME's in Italy.

"The London Stock Exchange Group Plc has teamed up with IBM to build a blockchain-based platform to digitally issue private shares of small and medium enterprises in Italy.

The platform is being built and tested by Borsa Italiana, the LSEG's Italian exchange operator, and will seek to make it easier to track and exchange shareholder information of unlisted businesses, the companies said on Wednesday."

Privacy

14.07.17

Government Computing

ICO annual report highlights funding and staff challenges

The UK's Information Commissioner's Office has published its annual report, which amongst administrative reporting issues has identified the introduction of the EU's General Data Protection Regulation as a significant challenge for the year to come and has provided further guidance.

"The Information Commissioner's Office (ICO) had identified issues such as ensuring a sufficient number of internal staff, new funding models and providing clear guidance on the incoming European General Data Protection Regulation (GDPR) as key challenges for the next year.

With the publication of the data regulator's 2016/17 annual report this week, information commissioner Elizabeth Denham said the changing data protection landscape represented by GDPR, which will become UK law from May 2018, was a main area of uncertainty for its operations."

18.07.17

Computing

'No evidence' that government understands the seriousness of Brexit for data protection

A new report from the House of Lords has criticised the UK Government arguing that not enough has been done to prepare for the introduction of GDPR and the Police and Criminal Justice Directive.

"The ability to move data across borders has become central to both trade and security - but Brexit is threatening both. A report from the Lords Select Committee, 'Brexit: the EU data protection package', the House of Lords reiterates that there is 'no prospect of a clean break' with Europe when it comes to data flows."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

15.07.17

Politico

White House leaves door open to U.S.-Russia cyber 'dialogue'

Although the US State Department has ruled out a formal partnership with Russia in cybersecurity, recent statements from Tom Bossert, Homeland Security Advisor at the White House indicate that the Trump administration remain open to further dialogue.

"The Trump administration is still open to a cyber dialogue with Russia — despite having no plans to form the joint U.S.-Russian election security team that President Donald Trump floated to much disbelief last weekend.

White House homeland security adviser Tom Bossert on Friday tried to dispel the confusion that has reigned since Trump offered his suggestion, which he later walked back. After that backlash, it appeared that the administration had essentially scuttled the State Department's previously expressed intent to have broader cyber policy talks with Moscow."

Cybersecurity

17.07.17

Computer Weekly

IBM claims breakthrough in mainframe encryption

IBM's new Z mainframe is capable of running 12 billion encrypted transactions according the company in what they see as a major advancement in mainframe technology.

"The latest IBM Z mainframe enables organisations to encrypt all data all the time, and is capable of running more than 12 billion encrypted transactions a day, according to IBM.

The mainframe's new cryptographic capability now extends across any data, networks, or applications – such as the IBM Cloud Blockchain service – without any application changes or impact on performance, the company said."

17.07.17

SC Media

Elon Musk: biggest concern for autonomous vehicles is fleet hack

Tesla CEO Elon Musk has warned that cybersecurity poses a significant challenge to the future of autonomous vehicles, with security flaws potentially allowing hackers to control entire fleets of vehicles.

"As automakers rush to bring autonomous vehicles to market, white hat cybersecurity researchers continue to find vulnerabilities that could be exploited remotely some of which could have jeopardized entire fleets of vehicles prompting recalls.

"I think one of the biggest concern for autonomous vehicles is somebody achieving a fleet-wide hack," Tesla CEO Elon Musk told the National Governors Association this weekend in Providence, Rhode Island."

18.07.17

The Hill

Dems call for review of pipeline cybersecurity rules

A bipartisan partnership has asked the GAO and TSA to provide information on whether fuel pipelines in the USA require upgraded or codified cybersecurity defences.

"Sen. Maria Cantwell (D-Wash.) and Rep. Frank Pallone Jr. (D-N.J.) asked the Government Accountability Office and Transportation Security Administration on Tuesday whether voluntary guidelines for cybersecurity defenses for fuel pipelines need to be updated or codified.

"An assessment of these guidelines and their effectiveness is needed as a number of major trends have emerged, with potentially significant implications for our energy, national and economic security," the lawmakers wrote in a letter."

19.07.17

SC Media

More staff cyber-security aware following WannaCry devastation in May

A new study across the UK, US, Germany and Australia has found that cybersecurity awareness has risen amongst decision makers and employees following recent global cyberattacks.

"The WannaCry attack may have laid waste to vast tracts of the NHS as well as other organisations and individuals, but it appears to have also focused attention on cyber-security in a way that hasn't been seen before.

That's according to a survey conducted by technology research firm Vanson Bourne on behalf of Clearswift in which 600 business decision makers and 1200 employees were asked about WannaCry. This included personnel in the UK, US, Germany and Australia."

Privacy

14.07.17

The Hill

House pushes to require warrants for all emails with appropriations amendment

The House of Representatives Appropriations Committee has given its support to an amendment that will prevent the future warrantless access to digital files for law enforcement currently provided by exiting law.

"The House Appropriations Committee Thursday night unanimously approved a legislative block to a law that allows law enforcement to seize emails, photographs and other cloud-hosted documents without a warrant.

Under current law established in 1986 — before the invention of the world-wide web — law enforcement can demand any file stored on a third-party server for more than 180 days."

17.07.17

Reuters

U.S. appeals court upholds gag orders on FBI data surveillance

The 9th Circuit Court of Appeals has upheld a gag order that allows the FBI to secretly order customer data from communications firms.

"A U.S. federal appeals court on Monday upheld nondisclosure rules that allow the FBI to secretly issue surveillance orders for customer data to communications firms, a ruling that dealt a blow to privacy advocates.

A unanimous three-judge panel on the 9th U.S. Circuit Court of Appeals in San Francisco sided with a lower court decision in finding that rules permitting the Federal Bureau of Investigation to send national security letters under gag orders are appropriate and do not violate the First Amendment of the U.S. Constitution's free speech protections."

18.07.17

SC Media

FBI PSA says connected toys may present privacy risks to children

The FBI have issued a public service announcement warning parents of the risks posed by IoT connected toys to the privacy of children.

"Connected toys may be putting children's personal information at risk leaving them vulnerable to child identity theft or worse, the Federal Bureau of Investigation (FBI) warned parents.

The agency encouraged parents to do their due diligence into the cybersecurity of toys that connect to the internet both directly through Wi-Fi and indirectly via Bluetooth to a mobile device connected to the internet as they often contain sensors, microphones, cameras, data storage components, and other multimedia capabilities, according to the July 17 public service announcement (PSA)."

Internet Inclusion

14.07.17

Ars Technica

FCC chief not concerned about number of pro-net neutrality comments

FCC Chairman Ajit Pai has stated that he will not be swayed by the number of pro-net neutrality comments the FCC receives, arguing that the content of these comments are more important to him than receiving numerous identical submissions.

"One day after a large protest of his plan to gut net neutrality rules, Federal Communications Commission Chairman Ajit Pai was asked if the number of pro-net neutrality comments submitted to the FCC might cause a change in course.

In response, Pai maintained his stance that the number of comments is not as important as the content of those comments."

17.07.17

Reuters

Major tech firms, internet providers clash over U.S. net neutrality rules

Major technology companies represented by the Internet Association have urged the FCC to abandon plans to remove net neutrality controls, arguing that the changes would create uncertainty in the market and could derail innovation in the sector.

"Tech companies clashed with internet service providers on Monday over whether a landmark 2015 net neutrality order barring the blocking or slowing of web content should be scrapped by the U.S. Federal Communications Commission.

A group representing major technology firms including Alphabet Inc (GOOGL.O) and Facebook Inc (FB.O) urged the FCC to abandon plans to rescind the rules barring internet service providers from hindering consumer access to web content or offering paid "fast lanes."

Pan-Asia

Internet governance

14.07.17

Straits Times

Indonesia requests ISPs to block Telegram messenger over terror fears

The Government of Indonesia has instructed internet service providers in the country to prevent access to Telegram messenger, over fears that it is being used as a communication channel by terrorists.

"Indonesia's Communications and Information Ministry has told Internet service providers (ISP) in the country to block access to web messenger Telegram because it has been found to be used by terrorists.

"There are many channels on their service that contain radicalism propaganda, terrorism, hatred, provocation and instructions to assemble bombs, strategies to attack, disturbing images, and other contents that are against the Indonesia law," said the ministry in the statement issued on Friday (July 14)."

Cybersecurity

17.07.17

Computer Weekly

IBM claims breakthrough in mainframe encryption

IBM's new Z mainframe is capable of running 12 billion encrypted transactions according the company in what they see as a major advancement in mainframe technology.

"The latest IBM Z mainframe enables organisations to encrypt all data all the time, and is capable of running more than 12 billion encrypted transactions a day, according to IBM.

The mainframe's new cryptographic capability now extends across any data, networks, or applications – such as the IBM Cloud Blockchain service – without any application changes or impact on performance, the company said."

19.07.17

MIS Asia

Singapore tests its cyber incident management and emergency response plans

The Cyber Security Agency of Singapore has conducted its Cyber Star exercise with over 200 sector leads and critical information infrastructure (CII) owners from 11 sectors in a bid to protect both public and private infrastructure.

"The second run of Cyber Security Agency of Singapore's (CSA) Exercise Cyber Star yesterday (18 July 2017) saw the participation of more than 200 sector leads and critical information infrastructure (CII) owners from 11 sectors.

Last year, participants were from the Banking and Finance, Government, Energy and Infocomm sectors. Besides those four sectors, this year's exercise included participants from the Aviation, Healthcare, Land Transport, Maritime, Media, Security & Emergency, Water."

Privacy

No new items of relevance

Internet Inclusion

17.07.17

Computer Weekly

Siemens to open Singapore digitalisation hub in IoT push

Siemens has announced that it will open a digitalisation hub in Singapore as part of a new drive to support IoT development in Southeast Asia.

"Global industrial technology supplier Siemens is opening a digitalisation hub in Singapore to develop internet of things (IoT) applications that cater to the needs of diverse industries in Southeast Asia.

Located in Macpherson in the central region of Singapore, the facility will be the first of its kind globally and will tap on Mindsphere – Siemens' cloud-based IoT operating system – to develop and commercialise digital systems across all Siemens business divisions."

18.07.17

The Hill

China stifles WhatsApp with 'Great Firewall'

China have moved to strengthen the country's "Great Firewall" with encrypted messaging program WhatsApp reported to no longer operate without the support of a VPN.

"WhatsApp users in China are reporting that the app isn't properly working across the country, sparking concerns that the Chinese government is censoring the encrypted messaging app.

Many users on the app in China have not been able to send videos, pictures and, in some cases, even texts, reports The New York Times. One Beijing-based reporter tweeted that the app had not been working since Sunday and could only be used with the help of a VPN."

Rest of the World

Internet governance

15.07.17

Politico

White House leaves door open to U.S.-Russia cyber 'dialogue'

Although the US State Department has ruled out a formal partnership with Russia in cybersecurity, recent statements from Tom Bossert, Homeland Security Advisor at the White House indicate that the Trump administration remain open to further dialogue.

"The Trump administration is still open to a cyber dialogue with Russia — despite having no plans to form the joint U.S.-Russian election security team that President Donald Trump floated to much disbelief last weekend.

White House homeland security adviser Tom Bossert on Friday tried to dispel the confusion that has reigned since Trump offered his suggestion, which he later walked back. After that backlash, it appeared that the administration had essentially scuttled the State Department's previously expressed intent to have broader cyber policy talks with Moscow."

Cybersecurity

17.07.17

Computer Weekly

IBM claims breakthrough in mainframe encryption

IBM's new Z mainframe is capable of running 12 billion encrypted transactions according the company in what they see as a major advancement in mainframe technology.

"The latest IBM Z mainframe enables organisations to encrypt all data all the time, and is capable of running more than 12 billion encrypted transactions a day, according to IBM.

The mainframe's new cryptographic capability now extends across any data, networks, or applications – such as the IBM Cloud Blockchain service – without any application changes or impact on performance, the company said."

17.07.17

Security Brief Australia

Melbourne accelerator programme seeks APAC cybersecurity startups

Deakin University and Dimension Data are currently seeking submissions from cybersecurity startups from across the APAC region as part of a joint cybersecurity accelerator program established in Melbourne.

"A new cybersecurity accelerator program is set to launch in Melbourne this month, thanks to an incubator partnership between Deakin University and Dimension Data.

The program, CyRise, is now looking for early-stage cybersecurity entrepreneurs and professionals from across Australia, New Zealand and APAC to apply for the six-month program."

19.07.17

SC Media

More staff cyber-security aware following WannaCry devastation in May

A new study across the UK, US, Germany and Australia has found that cybersecurity awareness has risen amongst decision makers and employees following recent global cyberattacks.

"The WannaCry attack may have laid waste to vast tracts of the NHS as well as other organisations and individuals, but it appears to have also focused attention on cyber-security in a way that hasn't been seen before.

That's according to a survey conducted by technology research firm Vanson Bourne on behalf of Clearswift in which 600 business decision makers and 1200 employees were asked about WannaCry. This included personnel in the UK, US, Germany and Australia."

Privacy

No new items of relevance

Internet Inclusion

14.07.17

IT Web Africa

Internet groups lobby Nigeria's NCC for net neutrality

Several internet groups have begun to lobby the Nigerian Communications Commission on the topic of net neutrality as part of the regulator's current work to establish a code of practice for communications technologies.

"The Alliance for Affordable Internet (A4AI) in Nigeria and the World Wide Web Foundation have made a joint submission to the Nigerian Communications Commission (NCC) as the regulator considers a code of practice.

The two bodies says their proposal will help alleviate obstacles, including high prices, poor service quality and inadequate infrastructure, which keep 96 million Nigerians offline."

Global Institutions

14.07.17

ITU

ITU publishes first Global ICT Regulatory Outlook

ITU have published a Global ICT Regulatroy outlook for the first time, identifying global trends and their implications on different economies.

"The first-ever global report tracking market and regulatory trends in the ICT sector and their implications across economies, Global ICT Regulatory Outlook 2017, has been launched by the International Telecommunication Union (ITU) at its Global Symposium for Regulators taking place in Nassau, Bahamas 11-14 July 2017.

This ICT industry outlook report represents the first in a planned annual series. It tracks how the global digital economy has been shaping up over the past ten years – what impact regulation has had – and what the digital future might look like in the coming years."

19.07.17

DIGITALEUROPE

DIGITALEUROPE discusses 5G and spectrum policy with National Ministries

DIGITALEUROPE have published details of their engagement with European national governments on the expansion of 5G services within the EU.

"In the course of June and July, DIGITALEUROPE engaged actively with the national governments of the EU Member States on crucial issues related to telecoms reform and 5G. Delegations from DIGITALEUROPE reached out to regulators in Copenhagen and Paris to discuss the European Electronic Communications Code.

On June 23, President Markus Borchert, Director-General Cecilia Bonefeld-Dahl and Jochen Mistiaen met with the Danish trade association IT-Branchen's telecoms working group to give an update from Brussels, before meeting with senior staff at the Danish energy and infrastructure ministry to discuss digital infrastructure and 5G. On 6 July, Jochen Mistiaen and representatives from Qualcomm and Nokia discussed the EECC with French regulatory agencies ARCEP and ANFR."

Diary Dates

Modernising the regulations establishing the .eu top-level domain name – 05.05.17-04.08.17

European Commission

ITU WTDC-17 – 09.10.17–20.10.17

Buenos Aires, Argentina

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland