27 September 2017

Synopsis

Scroll to read full summaries with links to news articles.

techUK and the **US** Chamber of Commerce have held a roundtable event to discuss the impact of **cybersecurity** regulations in the UK and US.

Ian Levy, Technical Director at the **National Cyber Security Centre**, has suggested that a tier one level **cyberattack** is expected within the next few years. In order to combat the disaster of such an attack, Levy has called on the government to specify how it will plan and resource its response to such a cyberattack.

The **US** Senate, in its National Defense Authorization Act (**NDAA**), included a key aspect for the modernization of technology in government (**MGT act**) following a number of large **data breaches** in 2017. A number of hearings from companies, including **Facebook** and **Google**, will be held to aid the progress of the act.

The Securities and Exchange Commission (**SEC**) has become the latest to be hit in a number of large **data breaches**. The Wall Street regulator stated that it is only recently that the breach, occurring in 2016, has revealed an impact with potential unlawful trades occurring.

Trend Micro Incorporated has revealed that the **Asia-Pacific** region has been hit hard by **cyberattacks** during the first half of 2017. Over 80 million threats were found on average, with politically motivated and **fake news** attacks soaring.

The **USA** has formally asked **China** to reevaluate the **cybersecurity laws** introduced in June, claiming that the stringent security checks for overseas firms could impede on the **global trade** in services that relies heavily on the transfer of **data** across national borders.

Namibia hosts the **internet governance** forum this week. The Namibia Internet Governance Forum aims to raise discussion on **public policy** issues focusing on the internet and is hoping to build worldwide involvement in the governance of the internet.

A meeting between the Commissioner and the Executive of **ENISA** has been held to discuss the role of ENISA and cybersecurity in **Europe** in light of the EU Commission's new draft **Cybersecurity Act**.

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

27 September 2017

Table of Contents

Europe

Internet governance

No new items of relevance

Cybersecurity

21.09.17

ENSIA

Commissioner Mariya Gabriel visits ENISA

A meeting between the Commissioner and the Executive of ENISA has been held to discuss the role of ENISA and cybersecurity in Europe in light of the EU Commission's new draft Cybersecurity Act.

"The Commissioner, today, met with the ENISA Executive Director Professor Dr. Udo Helmbrecht and the staff for a discussion on the current and future role of the Agency in the cybersecurity of Europe. ENISA welcomed, for the first time, the visit of the Commissioner for Digital Economy and Society, Ms. Mariya Gabriel, in the Agency's premises in Athens."

22.09.17

Computer Weekly

Nation-state actors responsible for most cyber attacks

A US-based cybersecurity firm, FireEye, has stated that the majority of cyberattacks and data breaches are from nation-states or state-sponsored individuals, rather than non-state actors. It has been suggested that companies, as well as other nations, face the threat of being breached by a government.

"Companies of all sizes may find themselves faced with highly capable state-sponsored cyber attacks, but steps can be taken to shore up defences. With cyber attacks becoming more sophisticated and reflecting geopolitical conditions, more can be done to shore up cyber defences, said speakers at the Singapore International Cyber Week 2017."

25.09.17

Tech UK

Cyber Security Public Policy Roundtable

techUK and the US Chamber of Commerce have held a roundtable event to discuss the impact of cybersecurity regulations in the UK and US.

"On Thursday, September 21, techUK hosted a roundtable with a U.S. Chamber of Commerce delegation to discuss public policy approaches to cybersecurity in the UK and USA."

22.09.17

SC Magazine

Tier one incident expected, Government cyber-specs likely - NCSC

Ian Levy, Technical Director at the National Cyber Security Centre, has suggested that a tier one level cyberattack is expected within the next few years. In order to combat the disaster of such an attack, Levy has called on the government to specify how it will plan and resource its response to such a cyberattack.

"We can expect to see a cyber-security incident at a category one level within the next few years, Ian Levy, technical director, National Cyber Security Centre told delegates at today's Symantec Crystal Ball event, just around the corner from the NCSC offices in Victoria, London, today."

25.09.17

Computer Weekly

Firms look to security analytics to keep pace with cyber threats

Companies are increasingly using security analytics to augment their cybersecurity as traditional approaches have become less effective.

"Traditional approaches to cyber security no longer enable organizations to keep up with cyber threats, but security analytics is an increasingly popular addition to the cyber arsenal. Security has changed dramatically over the decades. Companies can no longer risk focusing just on protecting physical assets such as offices and stock. With firms becoming increasingly reliant on technology and software to streamline everyday operations, it is crucial to have systems in place to protect digital property."

Privacy

No new items of relevance

Internet Inclusion

26.09.17

Public Technology

Shortage of civil service skills forces GDS to 'rely heavily' on temporary staff in 2016/17

IT skills have been lacking in the civil service, forcing the Government Digital Service to rely on temporary staff. The Cabinet Office revealed that spending shot up by over 54% since last year on temporary staff for the department.

"A shortage of IT skills within the civil service has forced the Government Digital Service to lean heavily on temporary workers to ensure delivery of some of biggest projects, according to the latest Cabinet Office accounts. The department's annual accounts reveal that its spending on temporary staff over the course of the 2016/17 year came in at £43.8m – an increase of 54.2% on the £28.4m figure of the prior year."

United States of America

Internet governance

26.09.17

Reuters

U.S. asks China not to enforce cyber security law

The USA has formally asked China to reevaluate the cybersecurity laws introduced in June, claiming that the stringent security checks for overseas firms could impede on the global trade in services that relies heavily on the transfer of data across national borders.

"The United States has asked China not to implement its new cyber security law over concerns it could damage global trade in services, a U.S. document published by the World Trade Organization showed on Tuesday. China ushered in a tough new cyber security law in June, following years of fierce debate around the move that many foreign business groups fear will hit their ability to operate in the country. The law requires local and overseas firms to submit to security checks and store user data within the country."

Cybersecurity

22.09.17

The Technews

Kaspersky Lab denies allegation brought by the USA

Kaspersky has objected to the US government's dismissal of its software. The US believed the Russia firm to have the potential to breach US systems and access sensitive government information and has called for all of its software to be removed from government.

"AP reported that worries rippled through the consumer market for antivirus software after the U.S. government banned federal agencies from using Kaspersky Lab software on Wednesday, 13th September. However, Kaspersky Lab denies allegation brought by the USA. Russian cybersecurity firm Kaspersky Lab says it is disappointed by a vote in the US Senate stopping it's software from being used by federal agencies and insists it is not affiliated with any government, including that of Russia."

25.09.17

Tech UK

Cyber Security Public Policy Roundtable

techUK and the US Chamber of Commerce have held a roundtable event to discuss the impact of cybersecurity regulations in the UK and US.

"On Thursday, September 21, techUK hosted a roundtable with a U.S. Chamber of Commerce delegation to discuss public policy approaches to cybersecurity in the UK and USA."

22.09.17

Computer Weekly

Nation-state actors responsible for most cyber attacks

A US-based cybersecurity firm, FireEye, has stated that the majority of cyberattacks and data breaches are from nation-states or state-sponsored individuals, rather than non-state actors. It has been suggested that companies, as well as other nations, face the threat of being breached by a government.

"Companies of all sizes may find themselves faced with highly capable state-sponsored cyber attacks, but steps can be taken to shore up defences. With cyber attacks becoming more sophisticated and reflecting geopolitical conditions, more can be done to shore up cyber defences, said speakers at the Singapore International Cyber Week 2017."

Privacy

22.09.17

NextGov

Congress tackles data breaches, Russian meddling and it modernization

The Senate, in its National Defense Authorization Act (NDAA), included a key aspect for the modernization of technology in government (MGT act) following a number of large data breaches in 2017. A number of hearings from companies, including Facebook and Google, will be held to aid the progress of the act.

"The Modernizing Government Technology Act received new life last week with its inclusion in the Senate's National Defense Authorization Act, but the IT

modernization legislation isn't a done deal yet. Meanwhile, Congress will take a hard look at cybersecurity policies at two agencies this week: the State Department, which plans to shutter a cyber office, and the Securities and Exchange Commission, which disclosed this week that one of its systems was breached."

25.09.17

NextGov

Deloitte says no government information compromised in breach

The accounting firm Deloitte had a large data breach, but has claimed that no government information or data was impacted. This is despite Deloitte having over $1 billion in 2017 government contracts.

"No federal government information was compromised by a data breach that the consulting and accountancy firm Deloitte confirmed Monday, a spokeswoman told Nextgov. The breach also did not impact any state or local government information."

24.09.17

The Hill

Breach of Wall Street's top regulator triggers scrutiny

The Securities and Exchange Commission (SEC) has become the latest to be hit in a number of large data breaches. The Wall Street regulator stated that it is only recently that the breach, occurring in 2016, has revealed an impact with potential unlawful trades occurring.

"The Securities and Exchange Commission (SEC) is coming under fire in Washington after revealing a data breach that may have allowed hackers to profit from stolen insider information."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

26.09.17

Reuters

U.S. asks China not to enforce cyber security law

The USA has formally asked China to reevaluate the cybersecurity laws introduced in June, claiming that the stringent security checks for overseas firms could impede on the global trade in services that relies heavily on the transfer of data across national borders.

"The United States has asked China not to implement its new cyber security law over concerns it could damage global trade in services, a U.S. document published by the World Trade Organization showed on Tuesday. China ushered in a tough new cyber security law in June, following years of fierce debate around the move that many foreign business groups fear will hit their ability to operate in the country. The law requires local and overseas firms to submit to security checks and store user data within the country."

Cybersecurity

22.09.17

Network Asia

Google selects Singapore's Quann as cyber security partner

Quann, a Singaporian cybersecurity firm, has partnered with Google on cybersecurity and analytics in order to boost intelligence and preparation for future cyberattacks. It has focused its attention in Google's Cloud services and analytics technology.

"Quann announced that it has become a Google Cloud Platform Services Partner. Under the partnership, Quann will offer comprehensive cyber security services – from security architecture assessments, data penetration to testing and incident response management – which are critical for securing IT infrastructure on the cloud."

22.09.17

Computer Weekly

Nation-state actors responsible for most cyber attacks

A US-based cybersecurity firm, FireEye, has stated that the majority of cyberattacks and data breaches are from nation-states or state-sponsored individuals, rather than non-state actors. It has been suggested that companies, as well as other nations, face the threat of being breached by a government.

"Companies of all sizes may find themselves faced with highly capable state-sponsored cyber attacks, but steps can be taken to shore up defences. With cyber attacks becoming more sophisticated and reflecting geopolitical conditions, more can be done to shore up cyber defences, said speakers at the Singapore International Cyber Week 2017."

26.09.17

Network Asia

Cyber attacks heavily hit APAC in 1H of 2017

Trend Micro Incorporated has revealed that the Asia-Pacific region has been hit hard by cyberattacks during the first half of 2017. Over 80 million threats were found on average, with politically motivated and fake news attacks soaring.

"Asia Pacific had been heavily hit from January to June 2017, leading other regions in most threat categories, according to Trend Micro Incorporated. Globally, Trend Micro detected 82 million ransomware threats and found that on average, 28 new ransomware families were created every month. The company also blocked more than 3,000 BEC attempts; and discovered and responsibly disclosed 382 new vulnerabilities."

Privacy

23.09.17

The Economic Times

India needs data-protection laws in place

Calls for India to increase and form data protection and privacy laws have surged following the many attacks that have occurred in 2017. WannaCry was just one of those breaches that has raised issues over the current lack of policy that addresses cybersecurity issues.

“There is growing demand for India to write laws on data protection and privacy in the wake of the Supreme Court ruling privacy to be a fundamental right. Concerns over cybersecurity, data protection and privacy have increased manifold, with the alarming rise in incidents of breach in India and the world over —the most recent case being the data breach at Equifax, the credit monitoring firm that handles sensitive financial information. Reportedly, the pilfered data includes credit card and social security numbers of 143 million, mostly US citizens, leaving them vulnerable.”

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

26.09.17

Xinhua Net

Namibia to join global internet governance community with maiden forum

Namibia hosts the internet governance forum this week. The Namibia Internet Governance Forum aims to raise discussion on public policy issues focusing on the internet and is hoping to build worldwide involvement in the governance of the internet.

"Namibia is expected to become the latest African nation to join the global debate on internet governance when it hosts its inaugural internet governance forum on Sept. 27 and 28, in the capital Windhoek. The Namibia Internet Governance Forum (NamIGF), is a multi-stakeholder platform consisting of government, development organizations, the private sector and media organizations, which aims to stimulate and enhance discussion around public policy related to the internet."

25.09.17

The Zimbabwean

'Freedom, privacy and security key to internet development' – MISA Zimbabwe

An Internet Governance Conference was held in Harare last week that aimed to broaden legislation on cybersecurity and attacks in Zimbabwe. However, access to internet across the nation was also a focus, hoping to try and further access.

"Internet stakeholders in Zimbabwe met in Harare on 21 September 2017 during MISA Zimbabwe's second Internet Governance Multi-Stakeholder Conference to assess the status of digital rights in the country. The conference, held under the theme Promoting Freedom, Privacy and Security on the Internet, focused on current legislative processes to enact a cyber crimes and cyber-security law and internet access patterns in the country."

Cybersecurity

22.09.17

The Technews

Kaspersky Lab denies allegation brought by the USA

Kaspersky has objected to the US government's dismissal of its software. The US believed the Russia firm to have the potential to breach US systems and access sensitive government information and has called for all of its software to be removed from government.

"AP reported that worries rippled through the consumer market for antivirus software after the U.S. government banned federal agencies from using Kaspersky Lab software on Wednesday, 13th September. However, Kaspersky Lab denies allegation brought by the USA. Russian cybersecurity firm Kaspersky Lab says it is disappointed by a vote in the US Senate stopping it's software from being used by federal agencies and insists it is not affiliated with any government, including that of Russia."

25.09.17

SC Magazine

Saudi Arabia strives to improve its cyber-readiness: Potomac assessment

Following cyberattack threats, Saudi Arabia is aiming to enhance its cybersecurity. Despite a lack of properly skilled workers on cyber issues, it has made gains on its cybersecurity and is hoping to continue this progress.

"In the face of external and domestic cyber-security threats, Saudi Arabia is taking significant steps to achieve cyber-readiness, but is being restrained by shortages of appropriately skilled Saudi-labour says Potomac Institute. Saudi Arabia's efforts to achieve cyber-readiness are well underway, following a range of external threats, from the 2012 Aramco attack to the more recent Iranian hacking team APT33, as well as significant attacks in 2016 (see below) in addition to internal cyber-threats faced by the regime – including perceived 'moral' threats."

25.09.17

Security Brief Australia

Govt announces $50m Cyber Security Cooperative Research Centre

A new cybersecurity Cooperative Research Centre has been invested in by the Australian government with $50 million. It has been suggested that it will boost the reputation of Australia as a secure place for business and aids in national security.

"The Australian Government's $50 million investment in a new industry-led cybersecurity Cooperative Research Centre (CRC) has been hailed as a victory for researchers at Edith Cowan University, a lead partner in the project. The CRC will be developed over the next seven years and will leverage a further $89 million from the 25 industry, research and government partners involved in the project."

26.09.17

Finextra

CBA says not 'stepping back' from cybersecurity despite offshoring plans

Reports of a possible neglectance of cybersecurity by the Commonwealth Bank of Australia has been refuted by the bank. It aimed to outsource its cybersecurity to an offshore provider which caused a disturbance in the nation.

"Commonwealth Bank of Australia has been forced to defend its commitment to cyber security after it emerged that the lender is set to offshore some critical IT functions. Earlier this month, The Australian reported that CBA was looking to outsource some cybersecurity work to an offshore provider, possibly in India, as part of a cost cutting exercise."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Global Institutions

21.09.17

ENSIA

Commissioner Mariya Gabriel visits ENISA

A meeting between the Commissioner and the Executive of ENISA has been held to discuss the role of ENISA and cybersecurity in Europe in light of the EU Commission's new draft Cybersecurity Act.

"The Commissioner, today, met with the ENISA Executive Director Professor Dr. Udo Helmbrecht and the staff for a discussion on the current and future role of the Agency in the cybersecurity of Europe. ENISA welcomed, for the first time, the visit of the Commissioner for Digital Economy and Society, Ms. Mariya Gabriel, in the Agency's premises in Athens."

Diary Dates

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