cybersecuritylaw&practice

STRATEGIC ANALYSIS BY DATAGUIDANCE
VOLUME 01 ISSUE 03 JUNE 2015 WWW.E-COMLAW.COM

ITU Index ranks cyber readiness across the globe

The ITU (the International Telecommunication Union) launched on 28 May its Global Cybersecurity Index & Cyberwellness Profiles Report 2015. The Index ('GCI') ranks jurisdictions in terms of their commitment to the ITU Global Cybersecurity Agenda, with the criteria spread across five areas such as legal measures and capacity building. The Report also contains cyber wellness country profiles and examples of good practice.

The GCI ranks the US as top globally, followed by Canada; the UK is in joint fifth place.

"The key takeaway is the wide global spectrum of cyber security maturity at the national level," said Dave Clemente, Senior Research Analyst at the Information Security Forum. "The Report talks of the need for a culture of cyber security and implementing cyber security mechanisms in all layers of society. This is extremely ambitious and beyond the capability of any multi-lateral body. It is a multi-generational challenge that will only be imperfectly addressed by myriad actors cooperating in (topically and temporally) narrow areas where self-interest overlaps."

IN THIS ISSUE

GDPR agreement includes 72 hour data breach notification

Ministers from the Justice and Home Affairs Council of the EU sealed on 15 June a general approach on the European Commission's ('EC') proposal for a General Data Protection Regulation ('GDPR'), due to replace the Data Protection Directive 95/46/EU. The approach includes agreement on the power for data protection authorities to issue penalties of up to €1 million or up to 2% of the global annual turnover of a company and rules to establish the 'one-stop-shop.' It is also stipulated that data controllers should report data breaches to the competent supervisory authority without undue delay, and, where feasible, within 72 hours of becoming aware of it.

"The Council's agreement on penalties produces a significant motivation to ensure that you are on the right side of the Regulation. This is reinforced with the bad publicity or potential reputational damage that could be caused by mandatory breach notification," said Steve Wright, Chief Privacy Officer at Unilever.

The Council also agreed that pseudonymisation should be included as an example of an appropriate security measure data processors and data controllers should consider implementing. "Should an organisation be found wanting for lack of adequate security provisions, such as pseudonymisation, then the aftermath of a significant data breach will be of particular interest to one of the 28 local data protection authorities, or worse, will come to the attention of the proposed EU Supervisory Authority," said Wright.

The EC, the Parliament and the Council can now officially enter into trilogue discussion to reach a final consensus on the proposed GDPR text. The first of the trilogue talks are set to take place on 24 June 2015.

"The Council's agreement implies that the final text should be feasible by the end of 2015, therefore requiring organisations' formal compliance by 2017 or two years after official publication of the Regulation. The main challenges for organisations of any size that capture both EU employee and customer data is being able to demonstrate that they have adequately captured consent, have the capability to ensure the right to erasure and that their profiling ambitions are brought in line with the new requirements. All this must happen within existing legacy systems or applications and this will create an avalanche of data configurations and keep both the IT and CISO departments extremely busy," concludes Wright.

NIST updates Guide on security of Industrial Control Systems

The US National Institute of Standards and Technology ('NIST') published in May its updated Guide to Industrial Control Systems ('ICS') Security, which presents a set of voluntary standards to help secure ICS by identifying threats and vulnerabilities and suggesting countermeasures.

"The Guide should be helpful in addressing the whole spectrum of potential threats by making it more difficult for malicious actors to gain control of an ICS and by making ICS more resilient in the face of an attack, an accident or a natural disaster," said Michael Vatis, Partner at Steptoe & Johnson. "Based on the major malware threats that focused on ICS in 2014, the Guide calls for applying similar controls and mitigations that are commonly used for enterprise networks," adds Evan Wolff, Partner at Crowell & Moring.

A new feature in the Guide details the application of the NIST Security and Privacy Controls for Federal Information Systems and Organizations publication, revised in 2013, to ICS. The controls detailed in this publication can be customised based on the specific security needs of each organisation.

"The industries that should pay closest attention to the Guide are those that use ICS to operate physical infrastructures," explains Vatis. "But numerous other industries also rely on various types of ICS to control the operations of their physical facilities, such as agricultural and pharmaceutical companies, and so it is highly relevant to them as well."