# GDPR compliance not relevant to us say UK decision makers, while one in five admit they don’t know – new NTT Security Risk:Value report shows

Submitted by: Origin Comms Ltd
Monday, 10 July 2017

- UK executives badly informed about where data is stored compared to other countries

London, UK; 10 July 2017 – According to new research, when it comes to data compliance matters, one in five business decision makers within the UK admit they do not know which compliance regulations their company is subject to, while a worrying number do not believe the forthcoming General Data Protection Regulation (GDPR) applies to them. The findings are part of the 2017 Risk:Value report commissioned by NTT Security (http://www.nttsecurity.com/RiskValue2017), the specialised security company of NTT Group, which looks at attitudes to risk and the value of information security to the business.

The survey of 1,350 non-IT business decision makers across 11 countries, 200 of which are from the UK, reveals that just 39% of UK respondents think the GDPR will apply to them, the lowest of all the European countries surveyed, including Germany/Austria, France, Sweden, Norway and Switzerland. A further 20% in the UK say they don’t know, suggesting that 41% are in denial of their future obligations relating to GDPR, which comes into force on 25 May 2018 – leaving companies with less than a year to comply with strict new regulations around data privacy and security.

The picture outside of Europe is also a concern, given that the legislation applies to any organisation anywhere in the world holding or collecting data on citizens in Europe and could result in penalties of up to €20m or 4% of annual turnover, whichever is higher.  Just 25% of respondents in the US believe it applies to them (20% don’t know) and 26% in Australia say they are subject to the new rules (19% don’t know). However, respondents in Germany/Austria (53%) and Switzerland (58%) seem to be well informed about the forthcoming legislation.

With data management and storage a key component of GDPR, the report raises serious concerns about knowledge of what data is being stored securely and where. Just four in ten (41%) UK respondents believe that all of their organisation’s data is secure, while around half (55%) say that all of their company’s critical data is secure. However, UK decision makers are much less well informed than their counterparts in other countries about where their data is physically stored, with a little over half (57%) admitting they know – compared to a global average of 67%.  Only France is lower, with just 54% of respondents knowing where their company data is stored.

Asked if emerging new regulations will impact on where and how their organisation’s data is stored, 42% of respondents in the UK say ‘definitely’, 31% ‘think so’ and nearly one in five (18%) say ‘no’, which is double the global average of 9%, and the highest number of all of the countries surveyed.

“In theory, UK organisations should be well ahead of the curve when it comes to the EU GDPR, given that it is a European data protection initiative,” comments Linda McCormack, Vice President UK & Ireland at NTT Security. “You would hope that the date of 25 May 2018 is clearly marked in the calendars of any business, UK or otherwise, that collects or retains personally identifiable data from any individual in

Europe. And Brexit is no excuse, as UK companies will still need to comply when dealing with countries in the EU. What's clear from our report is that a significant number do not yet have it on their radar or simply do not know if it applies to them. The fact they do not know means there is no plan of action in place."

"While our respondents are not in an IT function, they should still be aware of any new compliance regulations affecting their company's security and data, especially as the implications of non-compliance are very serious. The problem is that many see it as a costly and time-consuming exercise that delivers little or no value to the business, yet without it, they could find themselves losing customers, or having to pay very large regulatory fines."

Additional UK figures:

• UK respondents estimate, on average, that it would cost £1.1m ($1.4m) to recover from a data breach – above the global average of £1m ($1.3m).
• The estimated percentage drop in company revenue in the UK is 9.45%. Globally it is down from 12.51% in 2015 to 9.95% in 2017, on average.
• UK respondents estimate it would take 80 days to recover from a breach (74 days globally) on average.
• Around two-thirds (64%) cite loss of customer confidence, damage to reputation (67%) and financial loss (44%) following a breach, while 10% expect staff losses and 9% say that senior executives would resign.
• 63% in the UK 'agree' that a breach is inevitable at some point, compared to an average of 57% globally.
• 59% 'agree' they are kept fully up to date by their IT security team about attacks and potential threats to the security of the organisation (compared to an average of 67% globally)
• Less than half in the UK (47%) report that preventing a security attack is a regular boardroom agenda item, suggesting that more needs to be done for it to be taken seriously at a boardroom level.
• 72% of UK respondents say their organisation has a formal information security policy in place, compared to the global average of 56%. While 83% say it has been actively communicated internally, less than a third (31%) say employees are fully aware of the company's security policy.
• Nearly two-thirds (65%) of UK respondents say their organisation has an incident response plan, well above the global average of 48%. But just 44% are fully aware of what the incident response plan includes.

Download the 2017 Risk:Value report (http://www.nttsecurity.com/RiskValue2017).

Notes for editors:

Research demographics

Commissioned by NTT Security, the 2017 Risk:Value research was conducted by Vanson Bourne in March to May 2017. 1,350 non-IT business decision makers (35% at C-level) were surveyed in the US, UK, Germany and Austria, Switzerland, France, Sweden, Norway, Hong Kong, Australia and Singapore. Organizations had more than 500 employees and were selected across a number of core industry sectors. Approximately a third of

responses came from the financial services sector.

About NTT Security

NTT Security is the specialized security company of NTT Group.  With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more.

For further information please contact

Louise Burke
Origin Communications
louise@origincomms.com
+44 (0)7917 176095