A UK business will spend more than £1m recovering from a data security breach – NTT Security 2017 Risk:Value

Submitted by: Origin Comms Ltd
Monday, 17 July 2017

- Estimates that companies will take 80 days to recover and suffer a 9.5% revenue drop

- Less than half of executives say preventing a security attack is a board-level topic

The cost of recovering from of a security breach for UK organisations has been estimated in a new report launched today by NTT Security, the specialised security company of NTT Group. The 2017 Risk:Value (https://www.nttcomsecurity.com/en/risk-value-2017/) report, the company's third annual study of business decision makers' attitudes to risk and the value of information security to global organisations, reveals that a UK business would have to spend £1.1m ($1.4m) on average to recover from a breach – more than the global average of £1m ($1.3m), which has gone up from the previous report's $907,000 estimate.

The study of 1,350 non-IT business decision makers across 11 countries, 200 of which are from the UK, also reveals that respondents anticipate it would take, on average, almost three months (80 days) to recover from an attack, almost a week longer than the global average of 74 days. UK respondents also predict a significant impact of their organisation's revenue, suggesting as much as a 9.5% drop, which fares slightly better than the global average of nearly 10%.

In the UK, business decision makers expect a data breach to cause short-term financial losses, as well as affect the organisation's long-term ability to do business. More than two-thirds (64%) cite loss of customer confidence, damage to reputation (67%) and financial loss (44%), while one in 10 anticipate staff losses, and 9% expect senior executives to resign following a security incident.

Most telling from the report is that 63% of respondents in the UK 'agree' that a data breach is inevitable at some point, up from the previous report's UK figure of 57%. However, less than half (47%) say that preventing a security attack is a regular board agenda item, suggesting that more still needs to be done for it to be taken seriously at a boardroom level in the UK.

Linda McCormack, Vice President UK & Ireland at NTT Security, comments: "Companies are absolutely right to worry about the financial impact of a data breach – both in terms of short-term financial losses and long-term brand and reputational damage. Although this year's £1.1m figure is slightly down on last year's report (£1.2m), no company, regardless of its size, sector or focus, can afford to ignore the consequences of what are increasingly sophisticated and targeted security attacks, like the widespread and damaging ransomware attack we recently witnessed."

On a positive note, an encouraging 72% of UK business decision makers say their organisation has a formal information security policy in place, compared to the global average of over half (56%) and another 16% are in the process of implementing one. But while 83% say it has been communicated internally, less than one third (31%) say company employees are fully aware of the policy.

The study also raises concerns over the use and sharing of incident response plans for when a breach does

happen. Around two-thirds (65%) of UK respondents say their organisation has an incident response plan, well above the global average of 48%. However, less than half (44%) of business decision makers in the UK are fully aware of what the incident response plan includes.

“Creating security policies seems to be a work in progress for many UK businesses, unfortunately they become redundant if they are not properly communicated and shared throughout the whole organisation, and sadly this report backs that up. We see time and again organisations with good intentions when it comes to security and response planning, but then it falls to the bottom of the priority list due to a lack of resources, budgets and time. The fact that they are struggling to find the right resources and processes to support the fundamentals in information security and risk management planning is a major concern,’’ adds McCormack.

On the subject of budget, according to UK respondents, only an estimated 14.4% of their organisation’s operations budget is spent on information security, and 13.7% of their IT budget is estimated to be spent on security. This compares to 15.5% and 14.6% respectively across all of the countries surveyed. More than a third in the UK say their organisation is spending less on information/data security than R&D (36%), HR (36%) and Marketing (36%).

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

Notes for editors:

Research demographics

Commissioned by NTT Security, the 2017 Risk:Value (https://www.nttcomsecurity.com/en/risk-value-2017/) 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.

Media contact:

Amanda Hassall, Consultant, Origin Comms
T: +44 (0) 16 2882 2741
M: +44 (0) 78 5535 9889
E: amanda@origincomms.com