Third of business decision makers would pay hacker’s ransom demands rather than invest in more security, NTT Security Risk:Value report reveals

Submitted by: Origin Comms Ltd

Monday, 4 June 2018

14% of UK respondents regard Brexit as single greatest business risk, but only 4% say the same about poor information security

London, UK; 4 June, 2018 – One third of global business decision makers report that their organisation would try to cut costs by considering paying a ransom demand from a hacker rather than invest in information security. In the UK, this figure drops to a fifth (21 per cent) of respondents. The findings from the 2018 Risk:Value Report (https://www.nttsecurity.com/en-uk/risk-value-2018), commissioned by NTT Security (https://www.nttsecurity.com/en-uk), the specialised security company of NTT Group, show that another 30 per cent in the UK are not sure if they would pay or not, suggesting that only around half are prepared to invest in security to proactively protect the business.

Examining business attitudes to risk and the value of information security, NTT Security’s annual Risk:Value Report surveys C-level executives and other decision makers from non-IT functions in 12 countries across Europe, the US and APAC and from multiple industry sectors.

The findings are particularly concerning, given the growth in ransomware, as identified in NTT Security’s Global Threat Intelligence Report (https://www.nttsecurity.com/en-uk/landing-pages/2018-gtir) (GTIR) published in April. According to the GTIR, ransomware attacks surged by 350 per cent in 2017, accounting for 29 per cent of all attacks in EMEA and 7 per cent of malware attacks worldwide.

Confidence levels unrealistic

Levels of confidence about being vulnerable to attack also seem unrealistic, according to the report. Forty-one per cent of respondents in the UK claim that their organisation has not been affected by a data breach, compared to 47 per cent globally. More realistically, of those in the UK, 10 per cent expect to suffer a breach, but nearly a third (31 per cent) do not expect to suffer a breach at all. More worrying is the 22 per cent of UK respondents who are not sure if they have suffered a breach or not.

Given that just 4 per cent of respondents in the UK see poor information security as the single greatest risk to the business, this is unsurprising. Notably, 14 per cent regard Brexit as the single greatest business risk, although competitors taking market share (24 per cent) and budget cuts (18 per cent) top the table.

Business impact and estimated costs of a breach

When considering the impact of a breach, UK respondents are most concerned about what a data breach will do to their image, with almost three-quarters (73 per cent) concerned about loss of customer confidence and damage to reputation (69 per cent). The highest figures for any country.

The estimated loss in terms of revenue is 9.72 per cent (compared to 10.29 per cent globally, up from 2017's 9.95 per cent). Executives in Europe are more optimistic, expecting lower revenue losses than those in the US or APAC.

The estimated cost of recovery globally, on average, has increased to USD1.52m, up from USD1.35m in 2017, although UK estimates are lower at USD1.33m this year. Globally, respondents anticipate it would take 57 days to recover from a breach, down from 74 days in 2017. However, in the UK, decision makers are more optimistic believing it would take just 47 days to recover, one of the lowest estimates for any country.

Kai Grunwitz, Senior VP EMEA, NTT Security, comments: "We're seeing almost unprecedented levels of confidence among our respondents to this year's report, with almost half claiming they have never experienced a data breach. Some might call it naivety and perhaps suggests that many decision makers within organisations are simply not close enough to the action and are looking at one of the most serious issues within business today with an idealistic rather than realistic view.

"This is reinforced by that worrying statistic that more than a third globally would rather pay a ransom demand than invest in their cybersecurity, especially given the big hike in ransomware detections and headline-grabbing incidents like WannaCry. While it's encouraging that many organisations are prepared to take a long-term, proactive stance, there are still signs that many are still prepared to take a short-term, reactive approach to security in order to drive down costs."

Whose responsibility is security anyway?

According to Risk:Value, there is no clear consensus on who is responsible for day to day security, with 19 per cent of UK respondents saying the CIO is responsible, compared to 21 per cent for the CEO, 18 per cent for the CISO and 17 per cent for the IT director. Global figures are very similar.

One area of concern, however, is whether there are regular boardroom discussions about security, with 84 per cent of UK respondents agreeing that preventing a security attack should be a regular item on the Board's agenda. Yet only around half (53 per cent) admit it is and a quarter don't know.

How prepared are organisations?

UK respondents estimate that the operations department spent noticeably more of its budget on security (17.02 per cent) than the IT department did (12.94 per cent). This compares to the global figures of 17.84 per cent (operations) and 14.32 per cent (IT), on average.

Each year the NTT Security Risk:Value report shows that companies are still failing when it comes to communicating information security policies. An impressive 77 per cent in the UK (compared to 57 per cent globally) claim to have a policy in place, while 10 per cent (26 per cent globally) are working on one. While 85 per cent of UK respondents with a policy in place say this is actively communicated internally, less than a third (30 per cent) admit that employees are fully aware of it.

In terms of incident response planning, the UK is the most well prepared with 63 per cent of respondents saying their organisation has already implemented a response plan, well above the global figure of 49 per cent, while 18 per cent are in the process. Just 1 per cent in the UK say they have no plans to implement an incident response plan.

“The UK is leading the pack when it comes to planning for a security breach or for non-compliance of information/data security regulations,” adds Kai Grunwitz. “Given that the GDPR has just come into force, this is encouraging. However, while the majority claim their information security and response plans are well communicated internally, it seems it’s only a minority who are ‘fully aware’ of them. This continues to be an area that businesses are failing on time and time again and needs to be addressed as a priority.”

For further information on NTT Security’s 2018 Risk:Value report and to download a copy, visit: https://www.nttsecurity.com/en-uk/risk-value-2018

Notes for editors:

For a PDF of the 2018 Risk:Value Report or a copy of the global/UK infographic, images or further information/stats, please contact: nttsecurity@origincomms.com.

To learn more about the NTT Security 2018 Global Threat Intelligence Report (GTIR), visit: https://www.nttsecurity.com/en-uk/landing-pages/2018-gtir

Research demographics

Commissioned by NTT Security, the 2018 Risk:Value report research was conducted by Vanson Bourne in Feb and March 2018. 1,800 non-IT business decision makers were surveyed in the US, UK, Germany, Austria, Switzerland, France, Benelux, Sweden, Norway, Hong Kong, Singapore and Australia. Predominately, organisations had more than 500 employees and were selected across a number of core industry sectors.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis, is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies 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 Managed Security Services, Security Consulting Services and Security Technology 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 about NTT Security or visit http://www.ntt.co.jp/index_e.html to learn more about NTT Group.

Media:
Amanda Hassall, Consultant
amanda@origincomms.com
+44 (0)1628 822741
+44 (0)7855 359889

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Origin Comms Ltd