UK businesses spend £1.2 million recovering from a cybersecurity breach says new research

Submitted by: Origin Comms Ltd
Wednesday, 10 February 2016

Risk:Value 2016 report from NTT Com Security reveals over half of all firms expect a security attack

Most business decision makers in the UK admit that their organisation will suffer from a cyber security breach at some point. They also anticipate that to recover from a breach would cost upwards of £1.2 million on average for their organisation, the highest figure globally. This is according to a new Risk:Value 2016 (https://www.nttcomsecurity.com/en/landingpages/risk-value-2016/) report from global information security and risk management company, NTT Com Security (http://www.nttcomsecurity.com/en/), which surveyed business decision makers in the UK, as well as US, Germany, France, Sweden, Norway and Switzerland.

While nearly half (48%) of UK business decision makers say information security is ‘vital’ to their organisation and just half agree it is ‘good practice’, a fifth admit that poor information security is the ‘single greatest risk’ to the business, ahead of ‘decreasing profits’ (12%), ‘competitors taking market share’ (11%) and on a par with ‘lack of employee skills’ (21%).

Well over half (57%) agree that their organisation will suffer a data breach at some point, while a third disagree and one in ten say they do not know. Respondents estimate that a breach would cost them £1.2m, even before ‘hidden costs’ like reputational damage and brand erosion are taken into consideration, and take on average two months to recover from. They also anticipate a 13% drop in revenue, on average, following a breach.

The survey shows that recent high profile data breaches are starting to hit home. A similar report published by NTT Com Security in 2014 revealed that 10% of an organisation’s IT budget was spent on information security, compared to 11% this year. However, in the latest report around a quarter (23%) of UK businesses reveal more is spent on human resources (HR) than on information security.

In terms of remediation costs following a security breach, nearly a fifth (18%) of a company’s costs would be spent on legal fees, 18% on fines or compliance costs, 17% on compensation to customers, and 11% for third party remediation resources. Other anticipated costs include PR and communications (14%) and compensation paid to suppliers (12%) and to employees (11%).

According to the report, the vast majority of respondents in the UK admit they would suffer both externally and internally if data was stolen, including loss of customer confidence (66%) and damage to reputation (57%), as well as direct financial loss (41%). Over a third of decision makers (34%) expects to resign or expects another senior colleague to resign as a result of a breach.

Stuart Reed, Senior Director, Global Product Marketing, NTT Com Security, comments: “Attitudes to the real impact of security breaches have really started to shift, and this is no surprise given the year we have just had. We’ve seen several major brands reeling from the effects of serious data breaches, and struggling to manage the potential damage, not only to their customers’ data, but also to their reputation. While the majority of people we spoke to expect to suffer a cyber security breach at some

point, most fully expect to pay for it as well – whether that's in terms of third party and other remediation costs, customer confidence, lost business or even possibly their jobs."

Who's responsibility is it anyway?

· 41% of UK organisations have a disaster recovery plan in place, and 40% have a formal security policy in place. In both cases, almost half are in the process of implementing or designing one.
· When it comes to responsibility for managing the company's recovery plan, 15% say the CEO now has responsibility, although it still largely falls to the Chief Risk Officer (CRO), Chief Information Office (CIO) or Chief Security Officer (CSO).
· While 77% agree it is 'vital' their business is insured for security breaches, only 26% have dedicated cyber security insurance. However, 38% are in the process of getting a policy.
· One in five respondents in the UK say they do not know if their organisation has any type of insurance to cover for the financial impact of data loss or an information security breach.

"It's encouraging to see that almost all UK businesses now have a disaster recovery and formal information security policy in place, or are planning to implement one soon," adds Stuart Reed. "Clear, concise internal processes and policies for employees and contractors have so often been overlooked and this is what can lead to complacency and poor security hygiene. When we talk to clients, we make it clear that educating staff about security should be a top priority, supported by clear, simple procedures and backed up by a solid incident response plan."

The Risk:Value 2016 Executive Summary report and other materials, including UK and global infographics, can be downloaded here: (https://www.nttcomsecurity.com/en/landingpages/risk-value-2016/).

Twitter: @NTTComSec_UK
Hashtag: #riskvaluecosts

Global highlights from the research:

• Two-thirds (65%) of global decision makers say their organisation will suffer a data breach at some stage
• 54% say information security is 'vital' to their business and 18% agree that poor information security is the 'single greatest risk'
• The global figure for the cost of recovery from a breach could be from $907,053 (£629,000)
• Global decision makers say that 19% of their company's remediation costs would be spent on legal fees, 18% on compensation to customers, 15% on third party resources and 15% on fines or compliance costs
• A breach would take, on average, nine weeks to recover from, with an anticipated 13% drop in revenue
• 13% of an organisation's IT budget is spent on information security (compared to 10% in 2014).
• Over half (52%) have an information security policy in place, while 27% are implementing one
• 41% have insurance to cover for the financial impact of data loss and a security breach, while 12% are not covered for either. 35% have a dedicated cybersecurity insurance policy.

Research demographics

Commissioned by NTT Com Security the research was conducted by Vanson Bourne during October and November 2015. 1,000 business decisions makers (not in IT) were surveyed in the US, UK and Germany (200 in each), and France, Sweden, Norway and Switzerland (100 in each). Organisations had more than 500 employees, but those in Norway, Sweden and Switzerland could come from organisations with at least 250 employees. There were a minimum number of responses from the financial services sector (at least 50 in UK, US, France & Germany and minimum of 30 in the other countries).

About NTT Com Security

NTT Com Security is a global information security and risk management organisation, which delivers a portfolio of managed security, business infrastructure, consulting and technology integration services through its WideAngle brand. NTT Com Security helps organizations lower their IT costs and increase the depth of IT security protection, risk management, compliance and service availability. NTT Com Security AG, is headquartered in Ismaning, Germany and part of the NTT Group, owned by NTT (Nippon Telegraph and Telephone Corporation), one of the largest telecommunications companies in the world.

For more information, visit http://www.nttcomsecurity.com/en

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