NTT Security

2018 Risk:Value Report

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 the UK across multiple industry sectors.

The report highlights that many organisations are still making the same mistakes, failing to make any progress in crucial areas such as cybersecurity awareness and preparedness.

RANSOM DEMANDS vs. INVESTING IN SECURITY

One fifth (**21%**) would try to cut costs by paying a ransom demand from a hacker rather than invest in information security.

30% are not sure if they would pay a ransom or not.

Around half are prepared to invest in security and take a less reactive approach to the protection of their organisation.

CONFIDENCE LEVELS

Levels of confidence about being vulnerable to an attack seem to be unrealistic:

41% claim their organisation has not been affected by a data breach, but of these, **10%** expect to suffer one. **31%** do not expect to suffer from a breach at all.

More worrying is that **22%** are not sure if they have suffered a breach or not.

When it comes to the impact of a breach, **73%** are concerned about loss of customer confidence and **69%** about damage to reputation.

ESTIMATED COSTS OF A BREACH

The financial losses from a breach are less important than the damage an attack would do to an organisation's reputation:

9.72% The estimated loss in terms of revenue is **9.72%** on average, compared to **10.29%** globally.

$1.33m The estimated cost of recovery is **$1.33m**, compared to **$1.5m** globally.

47 days Respondents anticipate it would **47 days** to recover, compared to **57 days** globally and making it one of the lowest estimates for any country.

WHO'S RESPONSIBLE ANYWAY?

There is no clear consensus on who is responsible for day-to-day security:

21% say the CEO is responsible, compared to **19%** for the CIO, **18%** for the CISO and **17%** for the IT director.

84% agree that preventing a security attack should be a regular item on the board's agenda.

Only **53%** admit security is regularly discussed, and a quarter don't know.

PREVENTION IS BETTER THAN CURE

Some organisations in the UK are taking a long-term, proactive stance, but there are signs that many are still prepared to take a short-term, reactive approach to security in order to drive down costs.

In cybersecurity as in medicine, prevention is better than cure. NTT Security advises companies to follow both the spirit and the letter of regulatory guidelines, paying attention to how they evaluate risk and prepare for the time when hackers come calling.

The report and details of the research methodology can be downloaded at:
www.nttsecurity.com/en-uk/risk-value-2018