Study shows two-thirds of customers trust healthcare providers to protect personal data – more than double those who trust credit card companies

Submitted by: Origin Comms Ltd
Thursday, 18 May 2017

Ponemon report highlights damaging effects of data breaches on customer trust as one in four admit to leaving a company following a security incident

UK consumers expect healthcare providers, banks and credit card companies to be responsible for safeguarding their personal information, and are prepared to walk away from a company that does not take reasonable steps to secure their privacy. According to a new Ponemon study (https://www.centrify.com/lp/ponemon-data-breach-brand-impact-uk/) launched today and commissioned by Centrify (https://www.centrify.com), the leader in securing hybrid enterprises through the power of identity services, 65 per cent of customers affected by one or more data breaches lost trust in that organisation and one in four (27 per cent) ended their relationship with a company.

However, according to the report – The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the UK – consumers have very different expectations when it comes to the protection of their personal information compared to the companies themselves.

More than three-quarters (79 per cent) believe organisations have an obligation to take reasonable steps to secure personal data, but only 64 per cent of marketers and 66 per cent of IT professionals agree with them. The majority of consumers (73 per cent) also believe companies should control who has access to their personal information, but less than half of marketers (46 per cent) and IT practitioners (44 per cent) believe this is an obligation for the business.

Healthcare providers trusted more than credit card companies, but utilities hit rock bottom

The study, conducted before the unprecedented ransomware attack that has caused chaos across many NHS organisations, also reveals that 68 per cent of respondents say they trust healthcare providers to preserve their privacy and protect personal data – second only to banking institutions (77 per cent).

In contrast, a quarter (26 per cent) of customers trust credit card companies. Yet, healthcare organisations account for 34 per cent of all data breaches, while banking, credit and financial companies account for only 4.8 per cent*. Banking, credit and financial industries also spend two-to-three times more on cybersecurity than healthcare organisations**.

More than half of respondents (52 per cent) say privacy and security is most important to them when using social media, yet social media providers are among the least trusted organisations (19 per cent), along with airlines (11 per cent) and utilities companies (8 per cent).

Examining the negative effects of security beaches on reputation, company finances and share price, the report also reveals that more than half of all consumers (51 per cent) have been notified by a company or government body about their personal information being lost or stolen as a result of one or more data breaches.

“Given the recent attack on the NHS, this level of trust in healthcare providers may be misplaced,” comments Bill Mann, senior vice president of products and chief product officer, Centrify. “With more than one in four admitting they have walked away from a company following a security incident, it’s clear that this isn’t just about protecting data any more, but protecting the business as a whole. It is no longer just a problem for IT, but must be elevated to the boardroom as part of a holistic and strategic approach to protecting a company’s image, credibility and the trust of its customers.”

Additional findings:
• Seventy per cent of respondents say a company’s privacy and security practices are very important to preserving their trust. However, only 31 per cent believe companies and governmental organisations are able at a high level to protect their personal information and only 19 per cent of respondents believe they have a high level of control over the privacy and security of their information.
• The report found that the stock value index of 113 companies declined an average of five per cent the day a breach was disclosed and the organisation experienced up to a seven per cent customer churn.
• For senior marketers, the top three concerns about a data breach are loss of reputation (67 per cent), decline in revenues (53 per cent) and loss of customers (46 per cent). For IT professionals, the biggest concerns are loss of their jobs (63 per cent), loss of reputation (43 per cent) and time to recover decreases productivity (41 per cent).

Download the full report at: https://www.centrify.com/lp/ponemon-data-breach-brand-impact-uk/

*http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf
**https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Methodology of Ponemon/Centrify Study

The Ponemon study surveyed 1010 people in total in the UK, made up of 313 individuals in IT operations and information security, 292 senior level marketing professionals and 405 consumers. To determine the impact a data breach has on stock value, 113 benchmarked global public companies that experienced a data breach involving consumer data were selected for this analysis. These companies, which represented 16 industry sectors, were indexed against a match sample of companies that did not experience a data breach during the test period. The Security Effectiveness Score (SES) referenced in this study is determined by utilising the Ponemon Institute’s proprietary benchmark database and is derived from rating numerous security features or practices, including but not limited to, having a full-time CISO, employee training and awareness programs, regular audits and assessments of security vulnerabilities, and policies to manage third-party risk. This method has been validated from more than 50 independent studies conducted for more than a decade.

About Centrify

Centrify redefines security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise. As the only industry recognised leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure each user’s access to apps and infrastructure through the power of identity services. This is Next

Dimension Security in the Age of Access. Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organisations. To learn more visit www.centrify.com.
The Breach Stops Here.

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