

Protecting Data No Longer Just an IT Problem According to Centrifly-Commissioned Ponemon Study

Submitted by: Origin Communications (Thames Ditton)

Thursday, 18 May 2017

Report highlights the damaging impact of data breaches with share prices dropping an average of 5 per cent, customer churn increasing as much as 7 percent and brand reputation severely tarnished

C-suite blind spot exposed as 39 per cent of IT practitioners and 36 per cent of CMOs don't believe they take brand protection seriously

Bracknell UK 18 May, 2017 — When it comes to the biggest threats facing U.K. companies, IT practitioners and CMOs both believe a data breach ranks at the top, behind poor customer service, as it relates to their company's reputation and brand value. Yet 39 per cent (IT) and 36 per cent (CMOs) don't believe that brand protection is taken seriously by senior level executives. The findings were part of The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the UK (<https://www.centrifly.com/lp/ponemon-data-breach-brand-impact-uk/>). This Ponemon research study was commissioned by Centrifly, the leader in securing hybrid enterprises through the power of identity services, and has revealed the far-reaching consequences of data security breaches across an organisation -- including sales, marketing and IT - and the significant negative effect on company finances, shareholder value and brand reputation. And while the study found a data breach has a significant impact on brand reputation, a startling 71 per cent of IT practitioners do not believe that brand protection is their responsibility.

The study found that the share value index of 113 companies declined an average of five per cent immediately following the disclosure of the breach and experienced up to a seven per cent customer churn. What's more, one in four (27 per cent) of consumers impacted by a breach stated they discontinued their relationship with an organisation that experienced a data breach.

Commenting on the findings, Independent Cybersecurity Expert, Dr Jessica Barker said: "With so many data breaches hitting the headlines, there can be a sense of defeatism among some organisations. Breaches are seen as inevitable so some organisations question the value of spending on security when it won't make them 100% secure. However, this research has found that investing in security helps protect the organisation when even the worst happens, as companies with a strong security posture experience much quicker stock price recovery than those with a poor security posture following a data breach."

"In this past year alone we've seen high-profile data breaches, such as Yahoo and TalkTalk, experience the significant consequences that a breach can have on shareholder value and brand reputation," said Bill Mann, senior vice president of products and chief product officer, Centrifly. It's clearly a blind spot for the C-suite and it's time leadership recognise that protecting data is no longer just an IT problem, but a bottom-line business concern that needs a holistic and strategic approach to protecting the whole organisation."

How poor security posture impacts company value and customer loyalty

A portfolio of share prices was composed for 113 publicly traded benchmarked companies who had experienced a data breach involving the loss of customer or consumer data. The index value was tracked 30

days prior to the announcement of the data breach and 120 days following the data breach.

- These companies experienced a 5 per cent price decline immediately following the disclosure of the breach. More revealing are those companies with a strong security posture – companies that have made investments in people, process and technologies -- which are less likely to see a decline in share prices mainly because they are better equipped to respond.
- Those companies with a self-reported superior security posture saw a decline of no more than three per cent, and after 120 days following a breach, successfully rebounded with a three percent gain in stock price prior to the breach. In contrast, those with a poor security posture experienced a share price decline as high as seven per cent, and 120 days following the breach, did not fully recover the share price it had prior to the breach.
- Customer loyalty was also impacted with 65 per cent of consumer having lost trust in the breached company and 27 per cent of consumers discontinuing their relationship altogether.

IT under scrutiny

While 63 per cent of IT feared losing their job after a breach, the reality is the IT function is placed under greater scrutiny following a data breach. For those IT practitioners that had experienced a data breach, the most negative consequences were: significant financial harm (52 per cent), greater scrutiny of the capabilities of the IT function (51 per cent) significant brand and reputation damage (35 per cent) and decreased customer and consumer trust in their organisation (35 per cent).

Business impact and organisational disconnect

The study showed a significant disconnect across the business when it comes to responsibilities and brand reputation ownership:

- 70 per cent of IT practitioners do not believe their companies have a high-level ability to prevent breaches, however 58 per cent of CMOs are confident that their company would be resilient to a data breach that results in the loss or theft of high value assets
- There's a clear blind spot when it comes to data breaches and the impact they have on share price. Just 23 per cent of CMOs and 3 per cent of IT practitioners are concerned about a decline in their company's share price. For those that had a breach, only five per cent of CMOs and six per cent of IT professionals say that there was a decline in share price as a result of the breach.
- While IT practitioners and CMOs are both worried about the loss of reputation after a breach, their concerns apply only to their specific job function. For CMOs the top three concerns from a data breach were lost of reputation (67 per cent), decline in revenues (53 per cent) and loss of customers (46 per cent). For IT, the biggest concerns were loss of their jobs (63 per cent), loss of reputation (43 per cent) and time to recover decreases productivity (41 per cent).

To download a copy of the report visit <https://www.centrify.com/lp/ponemon-data-breach-brand-impact-uk/>

The Study

The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the UK, a Ponemon study, surveyed 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 share 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.

- ends -

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.

###

Centrify is a registered trademark of Centrify Corporation in the United States and other countries. All other trademarks are the property of their respective owners.

Media Contact:

Louise Burke
louise@origincomms.com
07917 176095