Hacking's Brand-Equity Nexus

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2018)." Hacking's Brand-Equity Nexus", IEEE *Computer, 51 (*3), 74-77.

Made available courtesy of IEEE: https://doi.org/10.1109/MC.2018.1731061

Abstract:

Cyberattacks can significantly affect brand reputation, but companies can take measures to repair the damage.

Keywords: cyberattacks | brand equity | consumer trust | corporate hacking

Article:

Companies experiencing cyberattacks are likely to suffer a loss in reputation. According to a January 2012 Ponemon Institute study, the average decline in brand equity from a data breach ranged from about $184 million to $330 million, or 17 to 31 percent of the brand's value.[1] A recent survey of retailers found that 55 percent considered reputation protection to be their top priority for IT security spending. According to the survey, 89 percent of retailers felt vulnerable to data threats and 51 percent had already experienced a data breach.[2]

LINKING CYBERSECURITY TO BRAND EQUITY

Brand equity denotes consumer perception of a product or service's value or attractiveness. Brand equity has two key determinants, perceived quality and brand loyalty,[3] and surveys indicate that consumers have a more negative perception and a less positive perception of companies that have been hacked, especially if consumer data has been compromised.

Products containing insecure software are perceived as being of lower quality, and there's growing awareness of the need to build cybersecurity into modern devices and systems.[4] For example, a recent *Wired* article chronicled the successful hack of a 2015 Jeep Cherokee by two researchers, who remotely changed the climate control system setting, turned on the radio and windshield wipers, and stopped the accelerator. "Automakers need to be held accountable for their vehicles' digital security," the author asserted. The lead researcher noted that "If consumers don't realize this is an issue, they should, and they should start complaining to carmakers. This might be the kind of software bug most likely to kill someone."[5]

Brand loyalty indicates consumers' tendency to repeatedly choose one brand over alternatives. Firms experiencing cybersecurity breaches will likely observe a decrease in brand loyalty. In a 2014 survey conducted for CreditCards.com by Princeton Survey Research Associates International, 45 percent of respondents with credit or debit cards indicated that they would "definitely or probably avoid" retailers that experienced hacks. Among households earning $75,000 or more annually, 31 percent would avoid such retailers compared to 56 percent of those earning less than $30,000.[6] Likewise, following the October 2016 botnet attack on DNS provider Dyn, more than 14,000 Internet domains stopped using its services.[7]

SUFFERING BRAND-IMAGE EROSION DUE TO ATTACKS

Table 1 lists some examples of businesses that experienced significant negative branding effects following cyberattacks. One widely used measurement of brand popularity is the "Buzz" score developed by the polling site You-Gov BrandIndex (www.brandindex.com). A company's score, which ranges from 100 to −100, is calculated by subtracting negative feedback from positive feedback. As the table shows, companies victimized by high-profile cyberattacks in recent years including the Sony PlayStation Network,[8,9] Target,[9,10] Sony Pictures Entertainment,[11,12] Anthem,[13,14] TalkTalk,[15-17] and Yahoo[18,19] have suffered major declines in their Buzz scores as well as in other measures of brand equity and popularity.

Table 1. Cyberattacks on companies and impact on brand equity.

Company	**Cyberattack**	**Brand Impact**
Sony PlayStation Network	In 2011, hackers extracted personally identifiable information of more than 77 million users.	The YouGov BrandIndex Buzz score fell from 5 the week before to −14 one day after announcement of the breach.
Target	A security breach during the peak holiday shopping season of 27 November to 15 December 2013 compromised 40 million credit and debit card accounts and 70 million customers' personal data.	The Buzz score dropped from 26 the week before to −9 one day after announcement of the breach and another 10 points within a few days, for a total decline of 45 points. Target's sales fell by 46 percent in the fourth quarter of 2013.
Sony Pictures Entertainment	In 2014, hackers downloaded 100 Tbytes of data including unreleased films and TV shows and leaked more than 47,000 Social Security numbers (SSNs), details on salary negotiations, and other sensitive information.	The Buzz index dropped about 14 points after announcement of the breach. The company also fell from third to eighth place in the Brand Keys Customer Loyalty Engagement Index.
Anthem Blue Cross and Blue Shield	In early 2015, 80 million records were breached including customers' and employees' SSNs, birthdays, addresses, emails, employment information, and income data. The chief executive's information was also compromised.	The proportion of consumers who thought that Anthem Blue Cross and Blue Shield was a better brand than other insurers decreased from 51 percent before the breach to 45 percent afterward.
TalkTalk	In October 2015, hackers accessed details of 150,000 customers and 15,000 bank accounts.	In a two-week period following the hack, the Buzz score plummeted from −1 to −50. The company's share of new customers in the broadband home services market fell by 4.4 percent in the last quarter of 2015, and 7 percent of customers switched to a different provider.
Yahoo	In September 2016, Yahoo reported that hackers might have stolen information on at least 500 million users in 2014.	A day after the breach announcement, online mentions of the company increased 474 percent, with 70 percent of the mentions negative.

Firms hit by cyberattacks usually also suffer a decline in brand loyalty. Three months after a major 2015 hack, TalkTalk lost 101,000 customers, 95,000 of them as a direct result of the cyberattack.[17] Consumers might also question the reliability of services provided by a firm that has lost sensitive information. About 20 percent of those who left TalkTalk cited "poor reliability" as the reason compared to less than 1 percent who had left in the previous quarter.[16]

POST-BREACH RESILIENCE AND REPARATION OF BROKEN TRUST

Recent studies have shown that reputation damage from a data breach can be irreparable. A KPMG survey of 448 consumers found that 19 percent would stop shopping with a retailer that had been a cyberattack victim even if the company took measures to fix the security issues.[20] Further, companies that experience hacks and fail to disclose details are viewed as dishonest, suspicious, and untrustworthy and find it difficult to repair broken trust. TalkTalk, for example, was taken to task for keeping the details of its cyberattack secret for a week.[21] Yahoo faced similar criticism for not coming clean about the extent of its own massive data breach. Senator Richard Blumenthal noted: "As law enforcement and regulators examine this incident, they should investigate whether Yahoo may have concealed its knowledge of this breach in order to artificially bolster its valuation in its pending acquisition by Verizon."[22]

It's possible for a company to repair—at least partially—broken trust from consumers after a cyberattack.[23] The success of such an effort depends on both the speed and nature of the response.[24]

It's especially important to have a detailed, well-developed plan in place for responding to cyberattacks, continual security training and education for employees, a designated spokesperson in the event of a breach, and prepared language for distribution to customers, social media, and news outlets. The company website and social media feeds should also have built-in emergency messaging capabilities.[25] Transparency is also critical—the company must honestly explain what went wrong. Finally, the company should consider offering discounts or complimentary services to customers, such as free credit monitoring.

The damage to a company's reputation following a cyberattack isn't just a function of the sensitivity of the compromised data and extent of the breach; it's also based on consumers' perception of the organization's cybersecurity practices (or lack thereof) and the nature of the postbreach response. Firms that have been hacked can minimize the adverse effects on brand equity and repair trust with customers, but only if they respond quickly and aggressively.

REFERENCES

1. "How Data Breaches Harm Reputations," blog, 17 Jan. 2012; www.experian.com/blogs/data-breach/2012/01/17/how-data-breaches-harm-reputations.

2. J. Goldman, "Acer Hacked," eSecurity Planet, 20 June 2016; www.esecurityplanet.com/hackers/acer-hacked.html.

3. D.A. Aaker, *Managing Brand Equity*, The Free Press, 1991.

4. “Cybersecurity in the Age of Digital Transformation,” *MIT Technology Rev.*, 23 Jan. 2017; www.technologyreview.com/s/603426/cybersecurity-in-the-age-of-digital-transformation/?ref=rss.

5. A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *Wired*, 21 July 2015; www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

6. K.H. Queen, “Poll: Many Cardholders Will Avoid Stores Hit by Data Breaches,” CreditCards.com, 19 Oct. 2014; www.creditcards.com/credit-card-news/shopping-after-breach.php.

7. “Exclusive: Mirai Attack Was Costly for Dyn, Data Suggests,” The Security Ledger, 3 Feb. 2017; securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests.

8. “PlayStation Network Hackers Access Data of 77 Million Users,” *The Guardian*, 26 Apr. 2011; www.theguardian.com/technology/201/apr/26/playstation-network-hackers-data.

9. T. Marzilli, “Target Perception Falls after Data Breach,” YouGov BrandIndex, 23 Dec. 2013; www.brandindex.com/article/target-perception-plummets-after-data-breach.

10. E.A. Harris and N. Perlroth, “For Target, the Breach Numbers Grow,” *The New York Times*, 10 Jan. 2014; www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html

11. A. Picchi, “How Big of a Hit to Sony’s Brand?,” CBS MoneyWatch, 19 Dec. 2014; www.cbsnews.com/news/can-sonys-brand-recover-from-the-interview-fiasco.

12. C. Atkinson, “Sony Hack Hurts More Than Stars’ Egos—Brand Loyalty Takes a Hit,” *New York Post*, 15 Dec. 2014; nypost.com/2014/12/15/sony-hack-hurts-more-than-stars-egos-brand-loyalty-takes-a-hit.

13. R. Abelson and M. Goldstein, “Anthem Hacking Points to Security Vulnerability of Health Care Industry,” *The New York Times*, 5 Feb. 2015; www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0.

14. J.K. Wall, “Anthem’s Brand Suffers Small Ding from Data Breach,” *Indianapolis Business J.*, 11 May 2015; www.ibj.com/blogs/12-the-dose-jk-wall/post/53151-anthems-brand-suffers-small-ding-from-data-breach.

15. R. Spillett, “TalkTalk Reveals Personal Details of 150,000 Customers and 15,000 Bank Accounts Were Accessed in Last Month’s Cyber Attack,” *Daily Mail*, 6 Nov. 2015; www.dailymail.co.uk/news/article-3306600/Hackers-accessed-details-150-000-TalkTalk-customers.html.

16. A. Sword, “Rebuilding Brand Trust: TalkTalk’s Path Back from Cyber Attack,” *Computer Business Rev.*, 22 Jan. 2016; www.cbronline.com/news/cybersecurity/data/rebuilding-brand-trust-talktalks-path-back-from-cyber-attack-4790671.

17. J. Lewin, “Cyber Attack Cost TalkTalk up to £60M and 101K Customers,” *Financial Times*, 2 Feb. 2016; www.ft.com/content/410f5477-d061-3cd4-a064-5563c91bd7fb.

18. J. Peters, “Yahoo and Others Face Cybercrime-Related Brand Damage,” blog, 2 Nov. 2016, blog.surfwatchlabs.com/2016/11/02/yahoo-and-others-face-cybercrime-related-brand-damage.

19. T. Dua, “Yahoo’s Data Breach Further Dents Its Already Flailing Brand,” Digiday, 23 Sept. 2016; digiday.com/brands/yahoos-data-breach-dents-already-flailing-brand.

20. “Cyber Attacks Could Cost Retailers One-Fifth of Their Shoppers: KPMG Study,” press release, KPMG, 23 Aug. 2016; home.kpmg.com/us/en/home/media/press-releases/2016/08/cyber-attacks-could-cost-retailers-one-fifth-of-their-shoppers-kpmg-study.html.

21. J. Staufenberg, “TalkTalk Cyber Attack: Call Centre Workers Arrested in India as Part of Hacking Probe,” *Independent,* 28 Jan. 2016; www.independent.co.uk/life-style/gadgets-and-tech/news/talktalk-call-centre-workers-arrested-in-india-in-cyber-hacking-probe-a6838381.html.

22. D. Volz, “Yahoo Faces Growing Scrutiny over When It Learned of Data Breach,” Reuters, 24 Sept. 2016; news.trust.org/item/20160923211729-stk2c.

23. W.P. Bottom et al., “When Talk Is Not Cheap: Substantive Penance and Expressions of Intent in Rebuilding Cooperation,” *Organization Science*, vol. 13, no. 5, 2002, pp. 497–513.

24. M.A. Korsgaard, S.E. Brodt, and E.M. Whitener, “Trust in the Face of Conflict: The Role of Managerial Trustworthy Behavior and Organizational Context,” *J. Applied Psychology*, vol. 87, no. 2, 2002, pp. 312–319.

25. K. Tynan, “Good Marketing Can Help Banks Survive a Cybersecurity Backlash,” *American Banker*, 12 Jan. 2015; www.americanbanker.com/opinion/good-marketing-can-help-banks-survive-a-cybersecurity-backlash.