Securing your brand is a C-suite challenge

By Paula Sartini

13 Dec 2019

Brand value is a key component to a company's success and it takes several years to establish by implementing a brand strategy that supports the business. However, in today's digital environment, brand value can be compromised in a matter of minutes and negatively impact the brand and company. As such brand security is an issue that needs constant attention from various departments including the C-suite to minimise possible reputational damage to the brand and the associated risk of losing customers.

Image source: Gallo/Getty Images.

Data hacks are happening more regularly today. These incidents impact brand reputation and safety and highlight the need for companies to take privacy issues more seriously as the repercussions of not doing so carry serious reputational damage for brands. According to the IBM 2018 Cost of Data Breach study, if a data breach causes an organisation to lose just 1% of its customers it will cost the business on average $2.8m (£2.1m), and if it loses more than 4% of the customer base the cost is closer to $6m (£4.7m). The costs associated with a data breach are made up of lost business, negative impact on reputation and employee time spent on recovery.

The financial impact of data breaches revealed

29 Jul 2019

As such companies cannot afford to ignore the reputational risk of a data breach and need to have measures in place to maintain trust with customers.

The role of compliance and regulation

Customers are often required to provide personal information to companies for a variety of reasons and expect companies to have stringent measures in place to protect this information and mitigate possible risks of data breaches and hacks. This is supported by findings of a recent study by RSA Security, which identifies that more than 57% of consumers blame companies for data breaches rather than hackers. Further, the study states that a loss of customer trust is the biggest risk associated with data breaches and hacks. This should be a key concern for every organisation, as once trust is lost, it is

near impossible to win it back.

Brand security means endpoint security

David Rozzio 11 Jan 2019

To alleviate some of the risk, countries have introduced regulations such as the local Protection of Privacy (PoPI) Act and Europe's GDPR, to ensure companies operate with transparency while protecting customer privacy and using data responsibility. While South Africa is yet to indicate the fines associated with breaches of the PoPI Act, the GDPR has announced two tiers of administrative fines for non-compliance: €10m or 2% of annual global turnover, whichever is higher; and €20m or 4% of annual global turnover, whichever is higher.

In many instances, this fee is equivalent to the 2-3% marketing budget that organisations assign annually. While this should be a concern for companies, the reputational damage of a breach should be the biggest concern for organisations as it is far greater than the value of a fine.

While government compliance and regulations should be adhered to, companies also need to implement their own compliance and risk standards internally to keep customer data secure from possible hackers and third parties. For example, marketing departments often use website tools to target customers online and share customer details with third-party companies to create personalised campaigns. Both of these examples expose customer details to third parties and increase the threat of customer data being hacked.

To combat this, companies need to remove the segregation of duties from a single department and combine the expertise of the marketing, legal and IT departments to build brand trust and mitigate possible brand risks at all times. In doing so they will be adding additional layers of security to prevent data breaches both within the company and via potential hackers.

Internal standards

While marketers are generally familiar with the threat of data breaches, in many instances they do not have insight into the particular vulnerabilities associated with marketing data and how to safeguard it. This requires the expertise of both the legal and IT departments to put measures in place to counter the possible risks.

To improve brand security, the marketing, IT and legal departments need to work closely together to combine technology, data management, content and customer experience. In larger organisations, Brand Security Officers have been appointed to focus entirely on protecting the brand reputation of the company. This role is charged with assessing, mitigating and managing marketing risks while looking at issues such as fraud, viewability and transparency. In essence, this role is responsible for guiding the organisation in terms of data security and customer privacy.

The role of technology in brand security

While technology is a key challenge for data breaches and fraud, it also has to be part of the solution. Governance, Risk and Compliance software offer companies a solution to address several of the GRC challenges they face by automating mundane reporting tasks and providing a single view of the requirements. However, companies need to also gain visibility into the compliance environment of the future if they are to limit potential risks and threats.

However, companies cannot rely on a single solution to address potential issues, they need to safeguard their customer data by implementing solutions that provide internal security standards and equip their customers to prevent possible data hacks and breaches.

Brands with a privacy-first culture tend to be governed by ethics [report]

10 Dec 2019

By using automation software solutions that help companies to deliver consistent brand experiences and provide verification tools in every email, for example, customers are less likely to fall victim of possible phishing scams. However, beyond this, the company needs to also have measures in place to prevent fraudulent emails from being sent from within the organisation too and minimise the possibility of identity theft.

Automation software presents a solution to help mitigate certain risks by automating tasks according to business objectives and brand standards. This will see all components and rules merged into a holistic solution and remove the segregation of duty from a single department to minimise potential risks to customer data and fraudulent activities.

Consistency and authenticity build trust

While marketing departments are faced with the challenge of capturing the imagination of the customer while ensuring data privacy at the same time, brand consistency and authenticity should be the foundation at which customers establish a relationship of trust. This is achieved, for example, by using primary fonts which can be harder to replicate, email signatures with built-in verification tools and documents that meet compliance standards such as correct director details and company addresses.

To achieve this, technology should be implemented, not only to automate repetitive tasks, but to ensure that the company is able to establish trust with customers in every interaction. In addition, technology should be used to provide a layer of added security to the organisation while providing data and analytics to determine possible risks, mitigate fraudulent activity and gain visibility into how its brand is being used to engage with customers.

Drivers and fears of SA's online consumers

Lauren Hartzenberg 28 Oct 2019

Customer trust and a company’s reputation is too important to be left to a single department. To be successful in safeguarding customer’s details, companies must tackle the challenge from various angles and implement several solutions that make it more challenging for hackers to access their information.

At this time, technology-savvy companies that implement solutions to safeguard their customer data are putting themselves at the forefront against the competition. However, in the future, this will become standard practice to protect their customers and meet their expectations.

ABOUT PAULA SARTINI

With over 20 years' experience helping leading organisations overcome various business challenges, Paula understands the challenges that companies face in delivering a consistent brand experience and the impact this has on their bottom line. An analytical thinker that strives to solve business problems with innovative solutions, Paula believes that technology plays a major role in solving critical business and branding challenges. As such, she established BrandQuantum to help businesses overcome their branding challenges in the digital age.

- Employee branding: Critical to customer experience - 14 Sep 2022
- #BizTrends2022: Data gives marketers insights to connect with customers - 5 Jan 2022
- Gathering customer data effectively to create great customer experiences - 25 Nov 2021
- The challenge of martech and automation - 20 Sep 2021
- Why brand health matters - 5 Aug 2021

View my profile and articles...