A MATTER OF TRUST

Andrius Palionis *reports on the cyber security threat to brand reputation*

A brand's reputation is no longer defined only by the services or products it offers, but also by its online presence. With a plethora of touchpoints for gathering consumer data on the internet – from social media to blogs, websites and online marketplaces – cyber security has become a fundamental pillar in maintaining and safeguarding a company's reputation.

It is essential to grasp the magnitude of the threat landscape. Cyber threats – ranging from data breaches to ransomware attacks – can hamper business activities, leading to substantial financial losses and damaging brand reputation. Trust, which takes years to build, can be destroyed in an instant.

Cyber security, therefore, is not an optional add-on, but in fact a strategic necessity for many companies, big and small. It's about protecting the brand's integrity by ensuring that customer data is safe, business operations are uninterrupted and trust in the brand is maintained. Proper cyber security measures can prevent data breaches, uphold user privacy and ensure continuity of service.

Every business, regardless of size, is subject to cyber attacks, and every organisation has various aspects, such as processes, brand reputation and revenue channels, that can be compromised if a breach occurs. There are many instances when data breaches damage brand reputation and revenue channels. As stated in the Fallout: The Consequences of IT Risk on Reputation report, nearly half (46 percent) of companies experienced harm to their reputation and brand worth due to a security breach.

According to the State of Corporate Reputation in 2020: Everything Matters Now research, a corporation's reputation is a highly valuable asset that significantly affects its financial performance. Additionally, on average, executives worldwide attribute 63 percent of their company's total market value to its reputation.

Based on a survey conducted by Deloitte, an overwhelming majority of executives – 87 percent, consider reputational risk as highly important or even more critical than other risks. Moreover, 88 percent of these executives confirmed that they prioritised reputational risk as a key business challenge. Therefore, the findings show that executives believe that failing to manage reputational risks effectively can swiftly transform into an organisation's strategic crisis.

Data breaches have become increasingly frequent and show no signs of diminishing in the foreseeable future. Prominent corporations such as LinkedIn, Facebook, and Marriott International have been victims of some of the most significant data breaches in the past years. In 2021, the United States encountered the highest number of data breaches, affecting approximately 212.4 million individuals (compared to 174.4-million people in 2020), as reported by Comparitech.

According to IBM's Cost of a Data Breach 2022 report, the global average cost of a data breach was $4.35-million. In the US, this number was more than double – $9.44 million. Interestingly, according to the same report, companies with a fully implemented AI and automation system detected and controlled a breach 28 days quicker than those without it, resulting in a cost saving of $3.05-million.

The impact of cyber threats on brand reputation extends far beyond the immediate fallout of a data breach or an attack

However, it's not an all-or-nothing situation. Even organisations with partially deployed AI and automation systems performed markedly better than those completely lacking such programs. It shows how important it is to invest in internal cyber security practices.

The impact of cyber threats on brand reputation extends far beyond the immediate fallout of a data breach or an attack. Cyber threats have the potential to trigger a cascade of harmful effects that can undermine a brand's reputation, causing lasting damage.

Data breaches can lead to the exposure of sensitive customer data, which is a direct violation of the trust relationship between a brand and its customers. Customers are increasingly concerned about their privacy and the security of their personal information. If a brand fails to protect this data adequately, it could face a backlash from its customers and the public, leading to a damaged reputation and loss of customer loyalty. The news of a data breach can spread rapidly on news sites and social media, further amplifying the impact and reach of the incident.

Furthermore, cyber threats can disrupt a brand's operations, causing inconvenience to customers and tarnishing the brand's image. If customers cannot rely on a brand to provide consistent, uninterrupted service due to cyber attacks, their trust in the brand can be significantly eroded. The reputational damage in such cases can be far-reaching and long-lasting, as rebuilding customer trust can be complex and time-consuming.

Cyber threats can also have legal and regulatory implications. If it is found to be non-compliant with data protection regulations, it can face penalties, further diminishing its reputation. Additionally, such incidents can lead to increased scrutiny from regulatory bodies, affecting the brand's ability to conduct business.

INVESTING IN A ROBUST CYBER SECURITY INFRASTRUCTURE IS A STRATEGIC NECESSITY

The financial impact of cyber threats can also affect a brand's reputation. The costs associated with managing a cyber attack, including incident response, remediation, legal costs and potential fines, can significantly affect a brand's financial health. If a brand is perceived as financially unstable due to these costs, it could lose stakeholder confidence.

The intertwined relationship between cyber security and brand reputation underscores the need for a robust, proactive cyber security strategy. It should not only focus on preventing cyber threats but also on mitigating the potential damage to a brand's reputation if an incident does occur. A strong cyber security posture can demonstrate a brand's commitment to protecting its customers' data, enhancing its reputation as a trustworthy and reliable entity.

To safeguard a brand's reputation, investing in proactive risk management and a robust cyber security infrastructure is crucial. It includes employee training and awareness programmes to prevent human errors, regular security audits, vulnerability assessments, and penetration testing. By implementing strong cyber security measures, companies can minimise the risk of breaches and their potential impact on a brand's reputation.

It is important to understand that the role of cyber security extends beyond the sole aim of preventing breaches. While this preventive aspect is undoubtedly vital, it is equally crucial to consider the potential aftermath of a successful attack. Hence, cyber security is not just about defence, it is also a strategic asset for damage control in the wake of a breach, adopting a dual approach of protection and remediation.

An organisation's ability to promptly detect, respond to and recover from an attack is a reflection of its robust cyber security posture. Immediate and effective response mitigates the potential damage caused by a breach, minimising disruptions in operations and preserving the integrity of sensitive data that could be compromised.

Necessary action often includes identifying the breach's source, isolating affected systems to prevent further intrusions, repairing vulnerabilities and communicating transparently with stakeholders about the incident. This communication includes details about the steps taken in response to the breach and plans to prevent such incidents in the future. A well-planned and executed response to a breach

▶

can limit immediate harm and serve as a testament to the organisation's dedication to its cyber security obligations. Customers, stakeholders, and the wider public perceive such entities as more resilient and better equipped to handle future threats.

In this way, even in adverse situations, brands can exemplify commitment to protecting customers' data. This commitment, demonstrated in action, fosters enhanced trust and reinforces its reputation as a reliable and secure entity in the increasingly risky digital landscape.

DATA BREACHES HAVE BECOME INCREASINGLY FREQUENT AND SHOW NO SIGNS OF DIMINISHING

Web scraping is a tool that provides extensive applications in cyber security and brand reputation management. In cyber security, web scraping can serve as a proactive measure to identify potential threats and vulnerabilities. For instance, by scraping data from sources such as hacking forums, dark web platforms, or other online communities, organisations can identify potential security threats like planned cyber attacks, stolen credentials for sale or undisclosed software vulnerabilities. Early identification allows businesses to take preventative action, strengthening their cyber security posture and thereby protecting their brand reputation.

In terms of brand reputation, web scraping can also help monitor online brand perception across multiple platforms. Brands can scrape data from various sources like social media, review sites, blogs and forums to gain insights into customer sentiment, feedback, and overall brand perception. Negative reviews or complaints, if detected early, can be addressed promptly to prevent damage to the brand image.

Additionally, web scraping can be used to detect potential brand-related threats like defamation, fake news or disinformation campaigns. By identifying and addressing these threats early, companies can protect and manage their reputation effectively. Hence, web scraping becomes an essential tool for maintaining a positive brand image in the digital age.

As the digital world evolves, brands encounter new challenges and risks. Given the importance of brand reputation and the potential impact of cyber threats, investing in a robust cyber security infrastructure is no longer an option but a strategic necessity.

The direct correlation between cyber security and brand reputation necessitates brands to prioritise proactive risk management and implement best practices to enhance their cyber security posture. In light of the growing cyber dangers, it is evident that businesses must consider cyber security an essential component of their overall business strategy and a critical determinant of their success in the digital age ●

BEST PRACTICES FOR STRENGTHENING CYBER SECURITY:

- Educate employees about threats, fostering a culture of security awareness.
- Implement multi-factor authentication and strong password policies to reduce unauthorised system access.
- Ensure that all software, including operating systems, applications and security tools, are up to date.
- Adopt a comprehensive incident response plan to ensure that in the unfortunate event, the organisation could quickly respond to and recover from a cyber security breach.
- Utilise encryption and secure communication tools to protect sensitive data from unauthorised snooping.
- Collaborate with cyber security experts and stay informed about emerging threats to improve security measures continuously.
- Use AI and ML-powered web intelligence tools to ensure the brand reputation and monitor threats.

Andrius Palionis is VP Enterprise at Oxylabs

A corporation's reputation is a highly valuable asset that significantly affects its financial performance

Picture credit: Unsplash