SECURITY COMPASS WHITEPAPER

Why Cybersecurity Is Important for Your Brand Reputation

Security Compass

"Nobody was ever fired for choosing IBM" was a phrase heard often back in the day. It meant that choosing IBM products and services over those of less established vendors was a safe option. IBM's reputation made it a safe choice.

Organizations work hard to build and protect their reputation and to become a "safe choice" for their customers. A good reputation can be built in a variety of ways. Product quality is an obvious method, as is exceptional customer service. Rapid development processes like CI/CD and DevOps can enhance brand reputation by delivering new features faster than competitors. Diligent protection of privacy made Swiss banks the first choice for the world's wealthy.

The most important trait, however, is a customer's trust.

Brand loyalty requires trust

Trust is critical to building a successful business. The 2020 Edelman Trust Barometer found that people were over 6 times more likely to pay a premium for a product and had higher brand loyalty for brands they trusted highly. This was reinforced by a FireEye study that found 52 percent of consumers would consider paying more for the same products or services from a provider with better data security.

Trust includes an organization's commitment to protecting confidential and sensitive information. While brand reputation can deprecate at any point in the business or supply chain, it is most impactful when a breach can be directly attributed to the organization charged with protecting the information.

Substandard data security can be viewed as a lack of respect for privacy. A breach that exposes personal or confidential information demonstrates that the organization did not prioritize the information entrusted to them. The same FireEye study found that 75 percent of consumers "were likely to stop purchasing from a company if a data breach was found to be linked to the board failing to prioritize cybersecurity."

Losing customer data severely damages brand reputation

A Ponemon Institute survey of over 800 executives found that losing confidential customer information was viewed as most damaging to an organization's reputation. 81 percent believed a widely reported breach would have a detrimental affect of 21 percent on the economic value of their organization's reputation and brand image. Restoring the reputation "would take, on average, about one year (11.8 months)."

Consumers agree, and 77 percent said cybersecurity and data privacy are the topmost reasons to select a retailer.

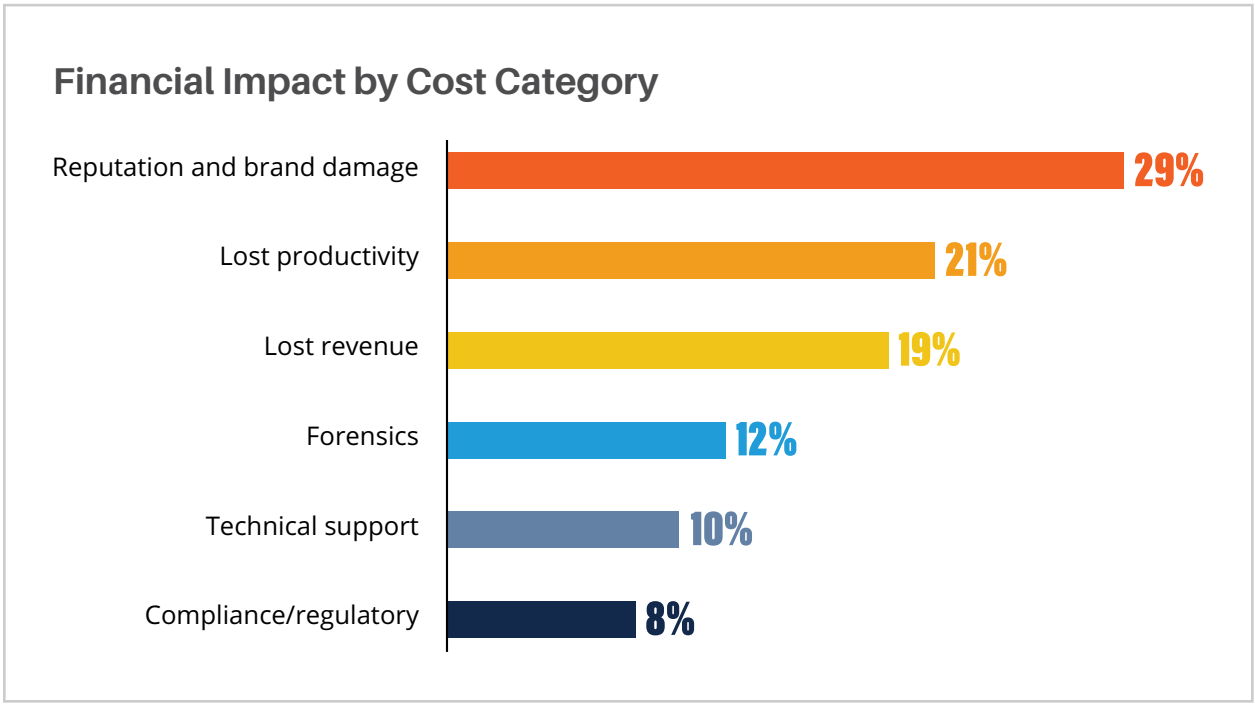
A similar study by Forbes and IBM found that reputation and brand damage had the greatest financial impact on an organization after a breach.

Data breaches attract widespread media coverage

A security breach often means an organization has not met its regulatory requirements. This has real costs. Attempting to hide a breach also has consequences.

Uber's Chief Security Officer faces federal charges for allegedly covering up its 2014 breach from the Federal Trade Commission.

Further, a breach is unlikely to remain a secret. In addition to the reporting requirements of each of the regulatory standards, a breach is big news for industry and mainstream media outlets. This means that in addition to customers and partners who are directly impacted by a breach, millions of others will also know, extending the impact on an organization's reputation.



Source: The Reputational Impact of IT Risk

Inadequate security as an existential threat

Inadequate security can be devastating to an organization. Small and medium-sized business are particularly hit hard. A recent study found that after a breach, 25 percent of small businesses filed for bankruptcy protection and 10 percent went out of business.

Mossack Fonseca & Co. was the world's fourth largest provider of offshore financial services when it was breached in 2016. The release of confidential information in the "Panama Papers" forced the firm to close its doors in 2018.

Large companies suffer consequences as well. Research shows an average decrease in market capitalization of 5 percent after a breach and a permanent decrease of 1.8 percent. This is in addition to direct costs such as lost revenue, lost productivity, incident response, and regulatory penalties.

How to protect brand reputation

Protecting brand reputation requires organizations to maintain the trust of their customers and partners, including trust that sensitive information will remain protected. Where network security and perimeter defenses were once the focus of security teams, web applications define the perimeter today. Committing to secure development at the start of the development lifecycle makes this task simpler.

Understand the threats

Building an application then testing for security is a backwards approach. By anticipating threats to an application, controls to mitigate risk can be assigned as part of the development process. This turns testing into an exercise to validate that the controls were properly implemented.

Enumerating threats to an application does not require weeks-long traditional threat models. Up to 90 percent of the threats to an application are directly related to an application's technology stack and deployment environment. By identifying these up front, it is possible to build a secure application in nearly the same amount of time as if no security planning occurred.

Reasonable security is the standard

The goal of a security program is not to eliminate all risk, as residual risk always remains. Instead, the goal should be to reduce risk to a level commensurate with the risk appetite of the organization.

Regulatory standards can help in some projects. The Payment Card Industry Data Security Standard is quite granular and can be mapped to development tasks. Other standards are less specific and can be summarized as a) understanding the risks present in the environment, and b) following a plan to address those risks.

The US Federal Trade Commission defines this as "reasonable security," and actions under Section 5 of the FTC Act often cite the absence of "reasonable security." The General Data Protection Regulation (GDPR) in Europe and the UK also looks at the appropriateness of the controls used, and considers the size of the organization and breach when assessing penalties. According to U.K. Information Commissioner Elizabeth Denham "Our focus is whether or not there was adequate, reasonable, consistent, effective data security to protect people's data."

Be honest in the event of a data breach

Honesty builds trust. In the event of a breach, do not obfuscate or cover up. Inform victims and regulators promptly. This is the most direct way to minimize reputational damage now and in the future.

> **"You will be held accountable for what you did or didn't do in the months and years leading up to a crisis."**
>
> **Prof. Daniel Diermeier**
> **IBM Professor of Regulation and Competitive Practice**
> **Kellogg School of Management**

Balanced Development Automation enables organizations to inject security throughout the application development process without delaying delivery timelines. Assurances about information safety and advanced safeguards for applications can go a long way in building your brand image in the customers' eyes.

SecurityCompass

Go Fast. Stay Safe.™

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001