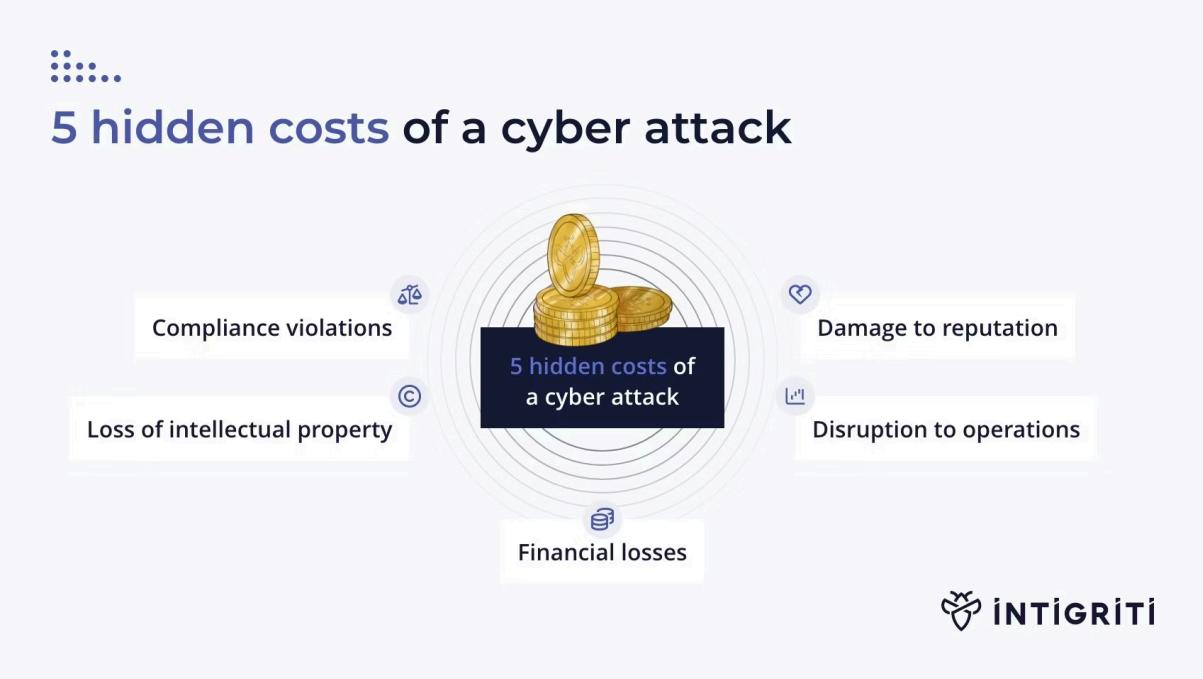
# Unveiling the 5 hidden costs of a cyberattack

BY INTI DE CEUKELAIRE · APRIL 26, 2024 · LAST UPDATED ON MARCH 6, 2025

Recent years have witnessed a dramatic surge in cyberattacks, with both the frequency and sophistication of attacks reaching unprecedented levels. Cybercrime is anticipated to cost companies all over the globe an estimated $10.5 trillion annually by 2025, and IoT attacks alone are expected to double by then too.

While the immediate (typically financial) impacts of a cyberattack are often evident, the hidden costs can be equally, if not more, damaging. This blog post aims to shed light on the lesser-known repercussions of cyberattacks, revealing the hidden costs that businesses need to be aware of.

## 5 hidden costs of a cyberattack




### 1. Financial losses

Okay, this cost isn't as 'hidden' as the others, but it certainly warrants a mention! When we think of the aftermath of a cyberattack, the first thing that comes to mind is often the financial impact. And rightly so, as the theft of data and subsequent incidental costs can quickly add up to significant financial losses for businesses. According to IBM's 2023 Cost of a Data Breach Report, for businesses with less than 500 employees, the average cost of a data breach is $3.31 million. That's a significant amount of money.

Cybercriminals are adept at breaching systems to steal sensitive data, which can then be used for identity theft, fraud, or other malicious purposes. Whether it's customer information, proprietary business data,

or financial records, the loss of such data has far-reaching consequences. Not only does it compromise the trust and privacy of customers, but it often results in substantial financial damages for the business.

Moreover, businesses typically incur significant expenses post-breach, including the cost of replacing stolen data, forensic investigations, and legal fees. These incidental costs can quickly escalate, further exacerbating the financial impact of a cyberattack.

## 2. Disruption to operations

In addition to financial losses, cyberattacks can also disrupt the normal operations of a business, leading to significant productivity losses and operational challenges.

One of the most common disruptions caused by cyberattacks is the loss of accessibility. If a business's website or online services are compromised, customers may be unable to access their services, leading to potential lost revenue and damage to the brand reputation. Moreover, compromised computer systems can lead to an inability to process orders, manage inventory, or communicate effectively, stalling daily operations and impacting the bottom line.

Targus, a well-known laptop bag and case manufacturer, experienced this recently. Following a cyberattack, the company implemented precautionary measures to disable significant portions of its infrastructure, resulting in disruptions to normal business operations.

## 3. Damage to reputation

Perhaps one of the most insidious hidden costs of a cyberattack is the damage it inflicts on a business's reputation. When a business suffers a breach, especially one where customer information is compromised, trust is broken. This loss of trust can lead to a loss of current customers and difficulties in attracting new ones, ultimately impacting the long-term viability of the business.

Furthermore, hacking incidents often attract media attention, which can cast a shadow over the company's reputation. Negative publicity surrounding a cyberattack can further erode customer trust and confidence in the business, compounding the damage to its reputation.

A well-known example of this happened back in 2018, when cybercriminals accessed the personal data of approximately 429,612 British Airways customers and staff. The brand was found to be processing its data without sufficient protection, and as a result, received huge reputational damage. This incident was even highlighted as a reason for their reputation falling to a four year low in 2019.

## 4. Compliance violations

Today, businesses are subject to a myriad of data protection and privacy regulations, such as GDPR or CCPA. Failing to protect sensitive data, especially that of customers, can result in regulatory repercussions and substantial fines and penalties.

Moreover, depending on the nature of the breach and the data involved, businesses may face lawsuits from affected stakeholders, further adding to the legal and financial burden of a cyberattack.

### 5. Loss of intellectual property

Last but not least, cyberattacks can result in the loss of valuable intellectual property, posing a significant threat to a company's competitive advantage and market position. Hackers may target a company's core intellectual assets, such as proprietary software, product blueprints, or strategic plans, putting its business secrets at risk.

Furthermore, stolen intellectual property can be sold or leaked, providing competitors with an unfair advantage and potentially undermining the company's market position. The loss of intellectual property can have far-reaching consequences, impacting innovation, market competitiveness, and ultimately, the bottom line.

## How Intigriti can help

Businesses looking to secure their assets and avoid all the above scenarios can rely on Intigriti to provide a comprehensive security testing solution. By leveraging the expertise of over 90,000 security researchers, businesses can proactively identify and address vulnerabilities in their systems before they can be exploited by malicious actors.

Moreover, Intigriti's commitment to compliance ensures that organizations can trust their data security standards are met while mitigating the risks associated with cyber threats.

To learn more about our bug bounty services, click here.