The 5 hidden costs of a hacking incident

In today's digital age, cybersecurity is not merely an IT concern but a core business risk. The consequences of a hacking incident can be severe, with lasting implications for a company's bottom line, operations, and brand reputation. Here are five ways in which a hacking incident can negatively impact your business:

1

Sensitive data

Theft of data: Cybercriminals can breach your systems to steal sensitive data which can be used for identity theft, fraud, or other malicious purposes.

Incidental costs: Businesses often incur significant expenses post-breach, including the cost of replacing stolen data, forensic investigations, and legal fees.

2

Disruption to operations

Loss of accessibility: If your website gets compromised, customers might be unable to access your services, leading to potential lost revenue.

Operational halt: Compromised computer systems could mean an inability to process orders, manage inventory, or communicate effectively, stalling daily operations.

3

Damage to reputation

Damaging trust: When a business suffers a breach, especially one where customer information is compromised, trust is broken. This can lead to a loss of current customers and difficulties in attracting new ones.

Negative publicity: Hacking incidents often attract media attention, which can cast a shadow over the company's reputation.

4

Compliance violations

Regulatory repercussions: Failing to protect sensitive data, especially of customers, might breach regulations like GDPR or CCPA, resulting in substantial fines and penalties.

Legal ramifications: Depending on the breach's nature and the data involved, businesses may face lawsuits from affected stakeholders.

5

Loss of intellectual property

Business secrets at risk: Hackers can target a company's core intellectual assets – be it proprietary software, product blueprints, or strategic plans.

Advantage to competitors: Stolen intellectual property can be sold or leaked, providing competitors with an unfair advantage and potentially undermining the company's market position.

About Intigriti

Global crowdsourced security provider trusted by the world's largest organizations

Intigriti's bug bounty platform provides continuous, real-world security testing to help companies protect their assets and their brand. Our community of ethical hackers challenge our customers' security against realistic threats: we test in precisely the same way malicious hackers do.

How vulnerability management works with Intigriti

1. Researcher tests and searches for a vulnerability
2. Researcher submits a report via Intigriti
3. Intigriti's triage begins communication with researcher
4. Intigriti's triage team applies quality assurance steps
5. In-scope, unique and well-written reports are submitted to client
6. Client accepts report, and payment is automatically processed

125.000+ researchers

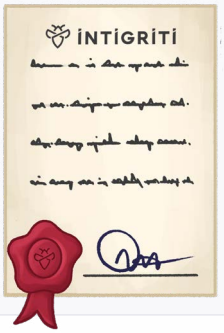
More than 125.000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs

Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.

GDPR compliant

We ensure compliance with the highest security and data security standards.



Strong global presence

Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in North America, Europe and Asia. In 2025, vulnerabilities were submitted from more than 180 countries.

A vulnerability reported and fixed is one less opportunity for a cybercriminal to exploit. Ready to talk about launching your first bug bounty program? We're here to help you launch successfully.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

YOU'RE IN GOOD COMPANY

Dropbox · Coca-Cola · Nestlé · Personio · NVIDIA · intel · Red Bull · Microsoft · UBISOFT