



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. Financial Losses

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.



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.

In conclusion, in a world increasingly driven by digital transactions and data, safeguarding one's digital assets is paramount. Businesses must invest in robust cybersecurity measures, continuous training, and vigilant monitoring to protect themselves from the multifaceted threats posed by hackers.





About Intigriti

Agile security testing, powered by the crowd

Intigriti's bug bounty platform provides continuous, realistic 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.



90,000+ researchers

More than 90,000 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 European presence

Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in America, Europe and Asia. In 2021, vulnerabilities were submitted from more than 170 countries.

TAKE YOUR FIRST STEPS

-  Request a demo www.intigriti.com/demo
-  Visit the website www.intigriti.com
-  Get in touch hello@intigriti.com

How vulnerability management works on Intigriti



You're in good company

Revolut



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.

Speak to our team today.