CyberProof®
A UST Company

How to keep cyberattacks from tanking your balance sheet

According to a recent Forrester report, last year saw:

1
BILLION
records exposed in the top 35 breaches

$2.6
BILLION
stolen in the top nine cryptocurrency breaches

$2.7
BILLION
in fines levied to the top 35 violators

Recent breaches:

Lapsus$ claimed to have stolen 1 terabyte of crucial data from semiconductor chip company Nvidia and demanded a **$1 million** ransom.

A DDoS attack on a Google Cloud Armor customer, that Google compared to **"receiving all the daily requests to Wikipedia in just 10 seconds."**

Company shares plunged when authentication company OKTA announced that around **2.5% of its customer records** were exposed in a supply chain attack.

A new high was recorded for phishing, with more than **1,270,00 attacks** recorded in the third quarter of 2022 alone.

Costs of a data breach

$4.35M
The average cost of a data breach reached $4.35 million in 2022.

$1.85M
For ransomware, costs are different: The average payment in 2021 was approximately $1.85 million.

And these are just direct costs; indirect costs are greater. They include:

- Lost business
- Lost customers
- Reputation losses
- Regulatory and legal expenses

Cybersecurity is a key business risk

The threat of attack is greater than ever before, partly because:

1. **Rising geopolitical tensions,** particularly around the Russia-Ukraine conflict and U.S.-China relations, created a knock-on effect.
2. **State-sponsored cyber warfare** is impacting the private sector.
3. **Enterprises** often become collateral damage.

Against this backdrop, it becomes increasingly crucial for corporate boards to align their organizations' cyber-risk management with their business needs.

Cyber-risk balance sheets can provide insight

According to the World Economic Forum's Principles for Board Governance of Cyber Risk, 37% of organizations strongly agree that quantifying risk leads to better management of cyber risks.

A cyber risk balance sheet includes:

- **Standardization**
- **Prioritization**
- **Mapping**

Lowering costs

Organizations deploying AI and automation incurred $3 million less, on average, in breach costs. Those deploying AI and automation detected breaches faster, minimizing the impact on operations.

Advanced cloud solutions that save dramatically on data ingestion and storage costs.

Viewing cybersecurity as a strategic business enabler

By illustrating the business case for cybersecurity — **aligning cyber-risk management with business objectives** — it becomes possible to make current and future decisions about the organization's cyber health in terms that the board can understand.

This information was first published by CyberProof President Yuval Wollman in Harvard Business Review. To learn more about how to mitigate the risk of attack, contact us.

SPEAK WITH AN EXPERT →

CyberProof®
A UST Company