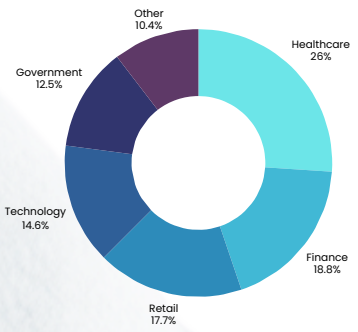
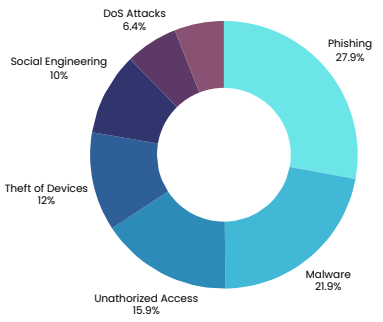
Lepide 'A decade of digital disaster' Infographic - October 2024



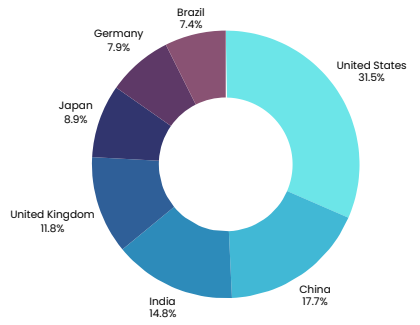
A Decade of Breaches by Industry

The data suggests that sectors handling sensitive personal information, such as healthcare and finance, are more likely to be targeted by cyberattacks. However, technology and retail industries also face significant risks due to their reliance on digital infrastructure and customer data. The visualization provides an overview of the relative vulnerability of different industries to data breaches.



A Decade of Breaches by Threat Type

Phishing and malware attacks emerge as the primary threats, followed by unauthorized access, loss of devices, and social engineering. The visualization offers insights into the techniques used by cybercriminals to compromise data security and highlights the need for organizations to implement robust defenses against these threats.

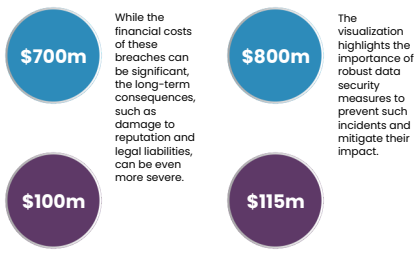


A Decade of Breaches by Country

The United States, China, and India emerge as the top three countries in terms of the number of reported breaches. This is likely due to their large populations, advanced economies, and high levels of digitalization. However, data breaches can occur anywhere, and even smaller countries may face significant risks. The visualization highlights the global nature of the cyber threat landscape.

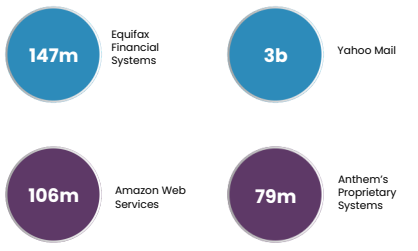
Top 4 Data Breaches by Estimated Financial Loss

The infographic presents a breakdown of the top four data breaches in terms of estimated financial losses over the past decade.



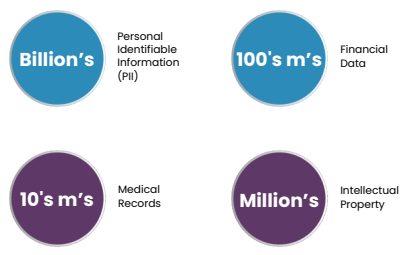
Top 4 Data Breaches by Software Breached

The infographic presents a breakdown of the top four data breaches in terms of the software compromised and the number of records affected.



Top 4 Types of Content Stolen from Data Breaches (2014-2024) with Approximate Number of Records.

The infographic presents a breakdown of the most common types of data compromised in data breaches over the past decade (2014-2024).



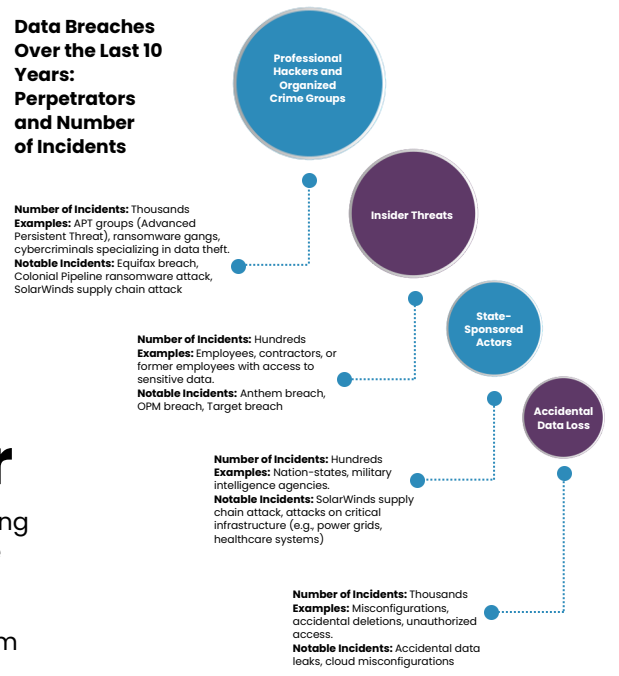
Brian Krzanich, former CEO of Intel Corporation

"Data breaches are a fact of life in the digital age. The question is not whether they will happen, but when."

Mark Zuckerberg, CEO of Meta (formerly Facebook)

"Security is a never-ending battle. We're constantly investing in new technologies and working with experts to protect our users' data."

Data Breaches Over the Last 10 Years: Perpetrators and Number of Incidents



Top 4 Types of Content Stolen from Data Breaches (2014-2024) with Approximate Number of Records.

The infographic presents a breakdown of the most common types of data compromised in data breaches over the past decade (2014-2024).

Data Breach Breakdown: A Decade of Digital Disaster

In the digital age, data is the new currency. Its value is immeasurable, driving innovation and fueling economies. However, with this value comes a grave responsibility: safeguarding it from malicious actors. This infographic dives deep into the alarming landscape of data breaches over the past decade, examining the trends, costs, and consequences of these cyberattacks. From the magnitude of corporate breaches to the vulnerabilities exploited, this visual exploration sheds light on the evolving threat landscape and the urgent need for robust data security measures.

46%

Small businesses (SMBs) bear the brunt of cybercrime, accounting for over 40% of all business-related attacks.

50%

A staggering 50% of small businesses lack a comprehensive cybersecurity plan, leaving them vulnerable to cyberattacks.

33%

Nearly a third of small businesses rely on free cybersecurity tools, compromising their data security compared to professional-grade solutions.

The Cybersecurity Blind Spot: SMBs Face Growing Threats

Cybersecurity Crisis: Billions Lost, Workforce Strained

$12.2 billion

Cybercriminals netted $12.3 billion in the United States alone during 2023, highlighting the escalating financial toll of cyberattacks.

4.2 million

In 2023, there were 4.2 million cybersecurity pro's worldwide. Cybersecurity experts are in high demand due to the increasing threat of cyberattacks.

32% increase

The U.S. cybersecurity workforce is projected to expand by 32% by 2032, creating approximately 53,000 new jobs.

Major Corporate Data Breaches (2014-2024)

1 — Adobe, October 2013

Hackers stole millions of customer records, including encrypted passwords and credit card numbers.

2 — Ashley Madison, July 2015

The extramarital dating website suffered a data breach, exposing the personal information of millions of users.

3 — Yahoo, September 2016

A massive data breach affected over 500 million user accounts, compromising email addresses, passwords, and security questions.

4 — Uber, November 2018

Hackers stole the personal information of 57 million users and 250,000 drivers, including names, email addresses, phone numbers, and driver's license numbers.

5 — Twitter, July 2020

A coordinated attack allowed hackers to gain control of high-profile accounts, including those of President Obama, Joe Biden, Elon Musk, and Bill Gates.

6 — MS Exchange SV, March 2021

A series of vulnerabilities in Microsoft Exchange Server were exploited by hackers to launch attacks on organizations worldwide.

7 — LastPass, December 2022

A data breach exposed the encrypted vault files of some LastPass users, potentially compromising their passwords and other sensitive information.

8 — Roblox, October 2023

A data breach affected up to 500,000 customers, exposing personal and financial information.

Barack Obama, former President of the United States

"Cybersecurity is one of the most serious challenges we face as a nation. It's a threat to our economy, our national security, and our way of life."

Angela Merkel, former Chancellor of Germany

"The digital age is a great opportunity for humanity, but it also brings new risks. Cybercrime and cyber warfare are serious threats that we must address together."

Common Reasons for Data Breaches

Misconfigurations

Incorrect settings or configurations can expose sensitive data.

Vulnerabilities

Software updates and patches may not be applied promptly, leaving systems vulnerable to exploits.

User Error

Employees may inadvertently share sensitive data or fall victim to phishing attacks.

Third-Party Integrations

Integrations with other software or services may introduce vulnerabilities.

5 Clear Steps for Protecting Your Data

1 Identify Your Sensitive Data

Use Lepide Identify to automatically scan and classify your data, helping you locate sensitive information and prioritize its protection.

2 Manage User Access

Use Lepide Trust to analyze user permissions and identify those with excessive access who might be potential insider threats.

3 Monitor User Activity

Use Lepide Audit to monitor user interactions with data and access controls, helping you investigate incidents and breach scenarios.

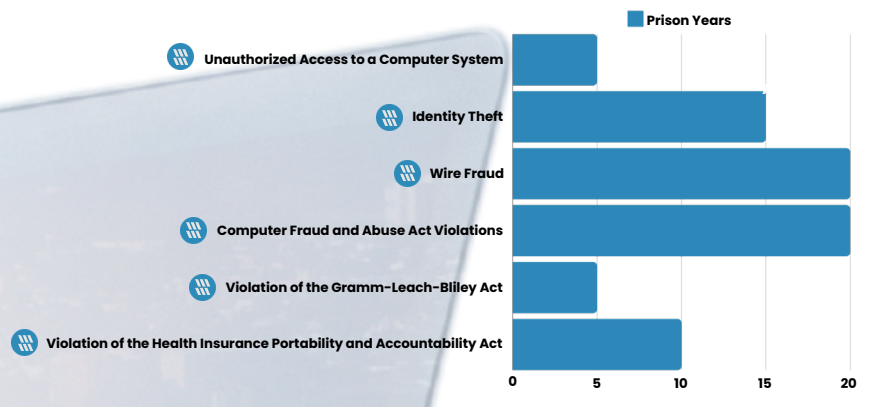
4 Detect Anomalous Behavior

Leverage Lepide Detect's machine learning capabilities to identify anomalous behavior and trigger automated responses to mitigate threats.

5 Respond Quickly and Effectively

Have a plan in place to respond to data breaches quickly and efficiently. This includes isolating the incident, notifying affected individuals, and taking steps to prevent future breaches.

Common Data Breach Types and Potential Penalties



Common Reasons for Data Breaches and Their Motivations with Approximate Percentages

Breach Type	Motivation	%
Phishing	Monetary gain, espionage, identity theft	30%
Malware	Monetary gain, espionage, disruption of services	25%
Ransomware	Monetary gain, extortion	15%
Unpatched Vulnerabilities	Monetary gain, espionage, disruption of services	10%
Insider Threats	Personal gain, revenge, espionage	5%
Third-Party Vendor Breaches	Monetary gain, espionage, supply chain disruption	5%
Weak Password Security	Monetary gain, espionage, identity theft	5%
Cloud Misconfigurations	Accidental data exposure, negligence	3%
Physical Security Breaches	Theft, vandalism, espionage	2%
Social Engineering	Monetary gain, espionage, identity theft	2%

Top Countries Suspected of Using Cyberattacks for State-Sponsored Purposes

China

Widely considered one of the most advanced and active state-sponsored cyber actors. Chinese state-backed groups have been implicated in a variety of cyberattacks, including espionage, intellectual property theft, and critical infrastructure disruption.

Russia

Russian state-sponsored cyber actors have been linked to numerous high-profile attacks, including interference in elections, attacks on critical infrastructure, and espionage against Western governments and businesses.

North Korea

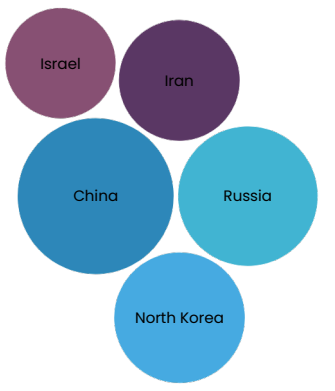
North Korea's state-sponsored cyber actors have been responsible for a number of high-profile attacks, including the WannaCry ransomware attack and attacks on financial institutions.

Israel

While Israel is known for its strong cybersecurity capabilities, it has also been accused of conducting offensive cyber operations against its adversaries.

Iran

Iranian state-sponsored cyber actors have been implicated in attacks targeting Israeli and Western interests, including critical infrastructure and government agencies.



Lepide