




The ROI of a Modern Security Program



Modern security programs are critical to protect and manage data — unstructured and structured, in the cloud and on-prem — across the ever-evolving data landscape. Recent trends point to an increase in data breaches, data leaks, and compromised crown jewel data. Get the latest cybersecurity statistics on the cost of data breaches, security leaks, and more — and find out how a modern security program boosts ROI and drives innovation.

Table of contents

Introduction.....	2
The Cost of Security Breaches.....	4
Time Is Money.....	6
The Dollar Value of PII and Other Sensitive Data Records.....	7
Most Data Breaches Come From Malicious Attacks.....	9
Regulatory Compliance and ROI.....	11
Brand Trust and Indirect Benefits for ROI.....	13
What a Modern Security Program Looks Like.....	14

The Cost of Security Breaches

In 2020, the total cost of security breaches worldwide averaged \$3.86 million, with the United States leading the pack with an \$8.64 million average — or nearly twice the global figure — according to the annual IBM/Ponemon Institute study.

Of the types of records that carry the highest price tag for companies when compromised, customer PII — or personally identifiable information, which is often highly sensitive, vulnerable, and regulated — came in the highest at a \$150 cost per record.

By industry, healthcare is the hardest hit with \$7.13 million in breach-related costs, followed by the energy industry at \$6.39 million, and finance at \$5.85 million — all of which clock in significantly above that global \$3.86 million average.

If you look at what these industries have in common, they are both more frequently targeted by malicious attackers and more subject to strict regulatory requirements (due to the amount and types of sensitive data they process) than are less affected industries.

Highly regulated sectors not only face more fines and penalties from a breach, but are more likely to suffer damaged brand reputation and customer loss as a result of compromised sensitive or personal information.

Fortunately, there are ways to guard against direct and indirect costs due to security incidents — while unlocking insight and value from your data at the same time. Implementing security automation across an organization — while leveraging AI and automated analytics — shows the greatest potential for savings. Companies that have fully deployed security automation, versus those with no automation, show a potential savings of up to \$3.58 million due to reduced breach threat.

\$3.86M

potential savings of
companies that have fully
deployed security automation

BY THE NUMBERS

Highly regulated sectors not only face more fines and penalties from a breach, but are more likely to suffer damaged brand reputation and customer loss as a result of compromised sensitive or personal information.

\$3.86M

the average cost of
security breaches worldwide

\$8.64M

the average cost of
security breaches in the US

\$7.13M

the average breach-related
costs in the health care

\$6.39M

the average breach-related
costs in the energy industry

\$5.85M

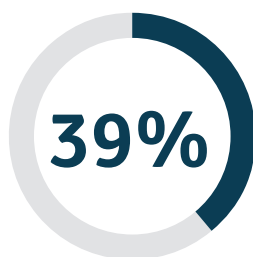
the average breach-related
costs in the finance industry

Time Is Money

The average time for a company to both identify and contain a data breach is 280 days. Companies that leverage automation to contain breaches in fewer than 200 days save a potential average of \$1.12 million.

Just as revenue lost to breach incidents varies by industry, so does breach lifecycle time. The average time frame to contain a breach in healthcare is 329 days — and 233 days in finance. Companies with fully deployed security automation bring their identification + containment time down by an average of 74 days.

While the financial consequences of compromised or exposed data is often immediate, the effects are also longstanding — especially when taking into account the loss of brand trust and customer loyalty. Organizations incur 39% of the financial loss from a breach — over a third — more than a year after the breach itself.



of the financial loss organizations
incur from a data breach

BY THE NUMBERS

Just as revenue lost to breach incidents varies by industry, so does breach lifecycle time.

280days

time for a company to both
identify and contain a data breach

\$1.12M

potential savings of companies
that leverage automation to contain
breaches in fewer than 200 days

329days

the average time frame to
contain a breach in healthcare

233days

the average time frame to
contain a breach in finance

74days

the average time that companies
bring down with fully deployed
security automation

The Dollar Value of PII and Other Sensitive Data Records

The types of data records that are most often exposed or compromised in breaches contain:

- **customer PII**: compromised in 80% of data breaches
- **intellectual property (IP)**: compromised in 32% of data breaches
- **anonymized customer data**: compromised in 24% of data breaches
- **employee PII**: compromised in 21% of data breaches

An alarming **80% of compromised data contains PII** — which is often highly sensitive, vulnerable, and regulated. Additionally, all of these types of records may be sensitive either on their own or in combination with other data and data types — and are regulated differently by various compliance requirements a company faces.

Different types of records also carry different average costs for a company when exposed. The most “expensive” data type to become compromised is, again, customer PII. Average costs per type of data record are:

- **customer PII**: \$150 per record
- **intellectual property (IP)**: \$147 per record
- **anonymized customer data**: \$143 per record
- **employee PII**: \$141 per record

The takeaway? Organizations need to put particular emphasis on safeguarding customer PII, which is highly regulated, sensitive, costly when compromised — and at much higher risk than any other type of corporate data.

BY THE NUMBERS

The types of data records that are most often exposed or compromised in breaches

80%

of data breaches
compromise a customer PII

32%

of data breaches compromise
an intellectual property (IP)

24%

of data breaches compromise
an anonymized customer data

21%

of data breaches
compromise an employee PII

Most Data Breaches Come From Malicious Attacks

Fifty-two percent (52%) of all data breaches come from malicious attacks — and that's 2% more than from system glitches and human error combined, as shown in the following breakdown of root causes for data breaches:

- malicious attacks — **52% of data breaches**
- system glitches — **25% of data breaches**
- human error — **23% of data breaches**

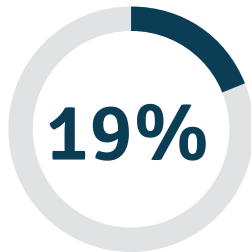
Breaches from malicious attacks are nearly \$1 million more expensive on average than those that stem from human error or glitches — and have consistently remained the costliest type of breach over the past five years. These root causes carry the following average costs:

- malicious attacks — **\$4.27 million**
- system glitches — **\$3.38 million**
- human error — **\$3.33 million**

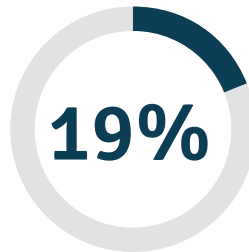


of all data breaches come
from malicious attacks

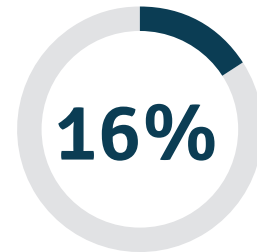
Of all breaches due to malicious attacks, the most prominent root causes include:



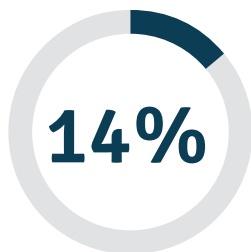
from stolen or
compromised credentials



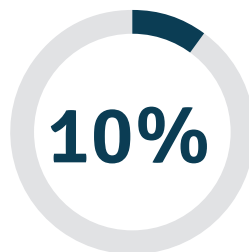
from cloud
misconfiguration



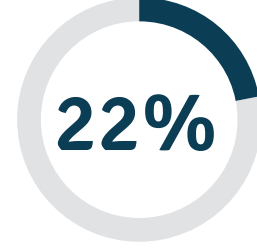
from third-party
software vulnerabilities



from phishing



from a physical
security compromise



from insider attacks,
email compromises,
social engineering, etc.

The remaining 22% come from insider attacks, email compromises, social engineering, and other misconfiguration causes, combined. Malicious attacks by destructive malware and ransomware prove more expensive — at \$4.52 million and \$4.44 million, respectively — than the cost of an average breach.

The percentage of malicious attacks also varies by location and industry. The highly regulated technology and finance industries have a higher incidence rate of malicious attacks than the average of 52% — specifically, 59% for technology and 56% for finance. In the US, 54% of incidents stem from attacks.

Regulatory Compliance and ROI

There are several ways businesses that implement a security program that will see significant returns on their investment.

Investing in **AI-driven security technology** enables companies to avoid heavy regulatory fines and penalties for potential violations. These companies are not only more likely to avoid or mitigate a costly breach incident in the first place — but are in a better position to recover in the event that one occurs.

Specific regulations that companies face run the gamut depending on the company's size, what type of data it processes, where it does business, and its industry. Highly regulated industries like finance and health see more significant returns based on the amount of sensitive, personal, critical, and vulnerable data they collect, store, and process — not to mention the fact that they are more targeted by malicious attacks.

A financial firm operating in the US, for example, needs to adhere to protection requirements put forth by regulations that include — but are not limited to:

- the federal Gramm-Leach-Bliley Act (GLBA), which is specifically designed for financial services
- the Sarbanes-Oxley Act (SOX)
- the General Data Protection Regulation (GDPR) if they do business in Europe
- state regulations like New York SHIELD and NYDFS
- the California Consumer Privacy Act (CCPA) — as well as its upcoming companion law, the stricter California Privacy Rights Act (CPRA).



“

Investing in AI-driven security technology enables companies to avoid heavy regulatory fines and penalties for potential violations. These companies are not only more likely to avoid or mitigate a costly breach incident in the first place — but are in a better position to recover in the event that one occurs.

”

Brand Trust and Indirect Benefits for ROI

Safeguarding customers' sensitive data, personal information, and personally identifiable information — which is compromised in around 80% of data breaches — helps an organization build customer trust and loyalty — and avoid inevitable financial ramifications if that trust is damaged or lost.

Security breach disclosures have a critical impact on a brand's reputation. Compromised businesses typically must share details about a breach incident with:

- regulators
- customers and clients who have been affected by the breach
- often third parties, suppliers, and even the press

Negative outcomes from disclosure affect customer loyalty, recommendations to other potential customers, and the public's overall perception of the brand.

A security program based on deep data intelligence and machine learning boosts ROI by facilitating operational efficiency, reducing reporting time on incidents, ensuring safer cloud migrations that will cut costs down the line, establishing access controls that guard against internal unauthorized access and human error, and much more.

“

Security breach disclosures have a critical impact on a brand's reputation.

”

What a Modern Security Program Looks Like

No matter what potential business impact your organization faces in terms of compromised security — from financial costs to reputational damage to total data loss — the cost of a security breach is higher than the cost of protecting your business from that breach.

BigID's extensible data intelligence technology is based on a deep discovery foundation that offers businesses full visibility into all their data. Advanced machine learning techniques classify and tag all the data you collect and process across your entire enterprise — both on the cloud and on-premise.

Identify and map data by customer and employee PII, intellectual property, crown jewel data, critical data, and more — so you can know where your most vulnerable data lives and how to best protect it. Prioritize high-risk data with open access issues, regulatory requirements, and by retention policy. Reduce notification and response time on data breaches, avoid adverse reputational consequences from an incident, and empower your organization to uncover valuable insights from your data.

BigID's platform incorporates modular apps that are fit-for-purpose and designed to create actionable solutions for your business needs. Integrate apps like risk scoring, file access intelligence, data remediation, and breach data investigation into your security framework to take swift action on vulnerable and exposed data — and measurably reduce risk for your entire organization.

Schedule a BigID demo to learn more about how your company can fully leverage an adaptable, actionable data security program based on deep discovery and classification — and maximize your return on investment.