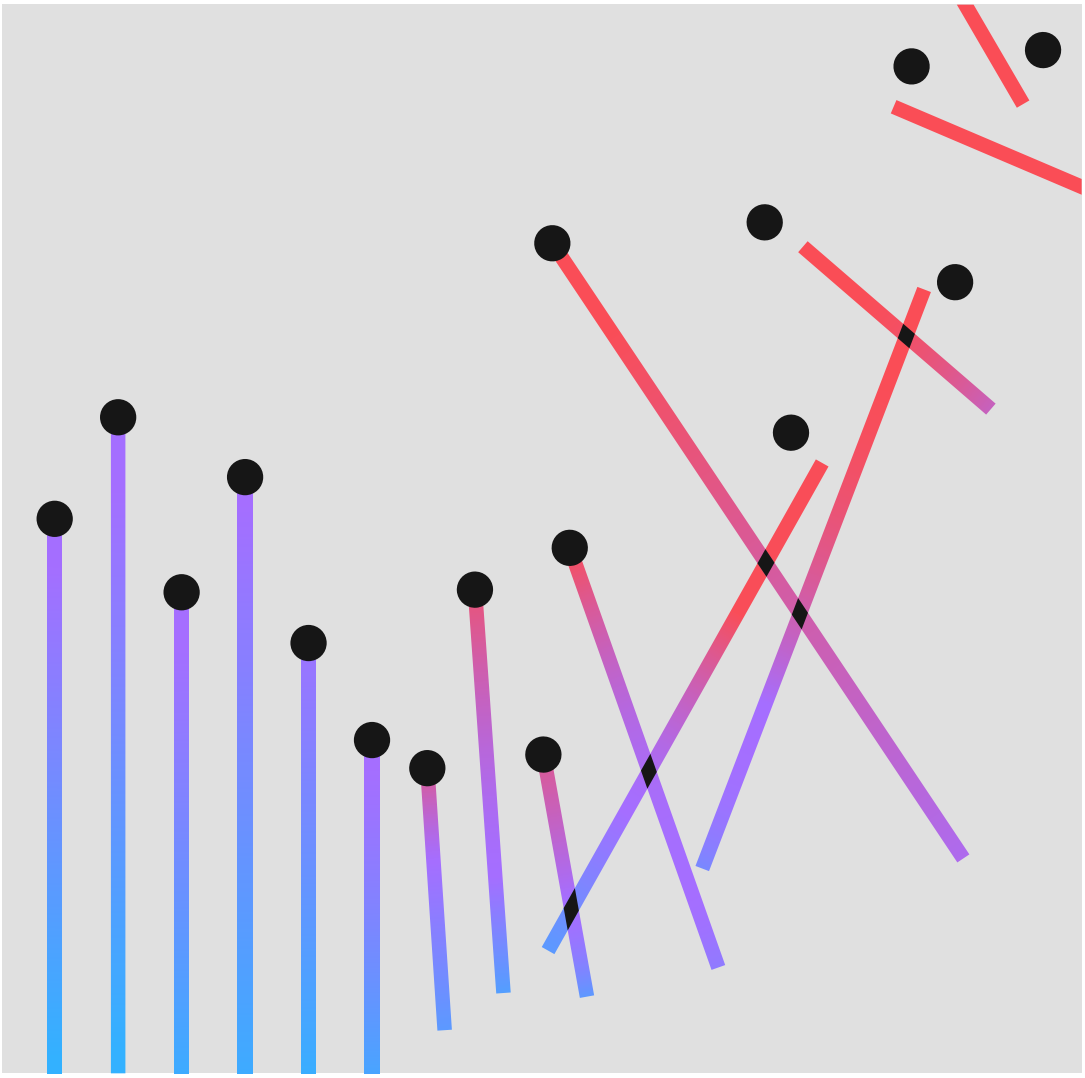
IBM **Security**

Cost of a Data Breach Report 2022: Executive Summary



IBM

Contents

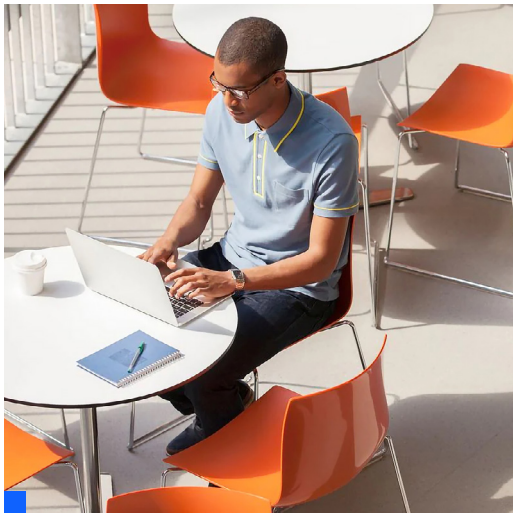
Executive summary

The Cost of a Data Breach Report offers IT, risk management and security leaders a lens into factors that can increase or help mitigate the rising cost of data breaches.

Now in its 17th year, this research — conducted independently by Ponemon Institute, and sponsored, analyzed and published by IBM Security® — studied 550 organizations impacted by data breaches that occurred between March 2021 and March 2022. The breaches occurred across 17 countries and regions and in 17 different industries.

We conducted more than 3,600 interviews with individuals from organizations that were impacted by the data breaches. During the interviews, we asked questions to determine the cost to organizations across different activities related directly to both the immediate and prolonged response to the data breaches.

As in previous years' reports, this year's data provides a view of how dozens of factors impact the costs that keep adding up after a data breach occurs. Additionally, the report examines root causes, short-term and long-term consequences of data breaches, and the mitigating factors and technologies that allowed companies to limit losses.



Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute.[1]

USD 4.35 million

Average total cost of a data breach

Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report.

83%

Percentage of organizations that have had more than one breach

Eighty-three percent of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach. Sixty percent of organizations studied stated that they increased the price of their services or products because of the data breach.

USD 4.82 million

Average cost of a critical infrastructure data breach

The average cost of a data breach for critical infrastructure organizations studied was USD 4.82 million — USD 1 million more than the average cost for organizations in other industries. Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries. Twenty-eight percent experienced a destructive or ransomware attack, while 17% experienced a breach because of a business partner being compromised.

USD 3.05 million

Average cost savings associated with fully deployed security AI and automation

Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. This 65.2% difference in average breach cost — between USD 3.15 million for fully deployed versus USD 6.20 million for not deployed — represented the largest cost savings in the study. Companies with fully deployed security AI and automation also experienced on average a 74-day shorter time to identify and contain the breach, known as the breach lifecycle, than those without security AI and automation — 249 days versus 323 days. The use of security AI and automation jumped by nearly one-fifth in two years, from 59% in 2020 to 70% in 2022.

1. Cost amounts in this report are measured in US dollars (USD).

USD 4.54 million

Average cost of a ransomware attack, not including the cost of the ransom itself

Eleven percent of breaches in the study were ransomware attacks, an increase from 2021, when 7.8% of breaches were ransomware, for a growth rate of 41%. The average cost of a ransomware attack went down slightly, from USD 4.62 million in 2021 to USD 4.54 million in 2022. This cost was slightly higher than the overall average total cost of a data breach, USD 4.35 million.

19%

Frequency of breaches caused by stolen or compromised credentials

Use of stolen or compromised credentials remains the most common cause of a data breach. Stolen or compromised credentials were the primary attack vector in 19% of breaches in the 2022 study and also the top attack vector in the 2021 study, having caused 20% of breaches. Breaches caused by stolen or compromised credentials had an average cost of USD 4.50 million. These breaches had the longest lifecycle — 243 days to identify the breach, and another 84 days to contain the breach. Phishing was the second most common cause of a breach at 16% and also the costliest, averaging USD 4.91 million in breach costs.

59%

Percentage of organizations that don't deploy zero trust

Just 41% of organizations in the study said they deploy a zero trust security architecture. The other 59% percent of organizations that don't deploy zero trust incur an average of USD 1 million in greater breach costs compared to those that do deploy. Among critical infrastructure organizations, an even higher percentage of 79% doesn't deploy zero trust. These organizations experienced on average USD 5.40 million in breach costs, more than USD 1 million higher than the global average.

USD 1 million

Average difference in cost where remote work was a factor in causing the breach versus when it wasn't a factor

When remote working was a factor in causing the breach, costs were an average of nearly USD 1 million greater than in breaches where remote working wasn't a factor — USD 4.99 million versus USD 4.02 million. Remote work-related breaches cost on average about USD 600,000 more compared to the global average.

45%

Share of breaches that occurred in the cloud

Forty-five percent of breaches in the study occurred in the cloud. Yet breaches that happened in a hybrid cloud environment cost an average of USD 3.80 million, compared to USD 4.24 million for breaches in private clouds and USD 5.02 million for breaches in public clouds. The cost difference was 27.6% between hybrid cloud breaches and public cloud breaches. Organizations with a hybrid cloud model also had shorter breach lifecycles than organizations that solely adopted a public or private cloud model.

USD 2.66 million

Average cost savings associated with an incident response (IR) team and regularly tested IR plan

Nearly three-quarters of organizations in the study said they had an IR plan, while 63% of those organizations said they regularly tested the plan. Having an IR team and an IR plan that was regularly tested led to significant cost savings. Businesses with an IR team that tested its IR plan saw an average of USD 2.66 million lower breach costs than organizations without an IR team and that don't test an IR plan. The difference of USD 3.26 million versus USD 5.92 million represents a 58% cost savings.

29 days

Savings in response time for those with extended detection and response (XDR) technologies

XDR technologies were implemented by 44% of organizations. Those organizations with XDR technologies saw considerable advantages in response times. Those organizations with XDR deployed shortened the breach lifecycle by about a month, on average, compared to organizations that didn't implement XDR. Specifically, organizations took 275 days to identify and contain a breach with XDR deployed versus 304 days without XDR deployed. This figure represents a 10% difference in response times.

12 years

Consecutive years the healthcare industry had the highest average cost of a breach

Healthcare breach costs hit a new record high. The average breach in healthcare increased by nearly USD 1 million to reach USD 10.10 million. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% since the 2020 report. Financial organizations had the second highest costs — averaging USD 5.97 million — followed by pharmaceuticals at USD 5.01 million, technology at USD 4.97 million and energy at USD 4.72 million.

USD 9.44 million

Average cost of a breach in the United States, the highest of any country

The top five countries and regions for the highest average cost of a data breach were the United States at USD 9.44 million, the Middle East at USD 7.46 million, Canada at USD 5.64 million, the United Kingdom at USD 5.05 million and Germany at USD 4.85 million. The United States has led the list for 12 years in a row. Meanwhile, the country with the fastest growth rate over last year was Brazil, a 27.8% increase from USD 1.08 million to USD 1.38 million.

Recommendations to help minimize financial impacts of a data breach

In this section, IBM Security outlines steps organizations can take to help reduce the financial cost and reputational consequences of a data breach. These recommendations include successful security approaches taken by organizations in the study.

Adopt a zero trust security model to help prevent unauthorized access to sensitive data.
Results from the study showed that while just 41% of organizations had implemented a zero trust security approach, they had a potential breach cost saving of USD 1.5 million with a mature deployment. As organizations incorporate remote work and hybrid multicloud environments, a zero trust strategy can help protect data and resources by limiting their accessibility and requiring context.

Security tools that can share data between disparate systems and centralize data security operations can help security teams detect incidents across complex hybrid multicloud environments. You can gain deeper insights, mitigate risks and accelerate response with an open security platform that can advance your zero trust strategy. At the same time, you can use your existing investments while leaving your data where it is, helping your team become more efficient and collaborative.

Protect sensitive data in cloud environments using policy and encryption.
With the increasing amount and value of data being hosted in cloud environments, organizations should take steps to protect cloud-hosted databases. Mature cloud security practices were associated with breach cost savings of USD 720,000 compared to no cloud security practices. Use data classification schema and retention programs to help bring visibility into and reduce the volume of sensitive information that's vulnerable to a breach. Protect sensitive information using data encryption and fully homomorphic encryption. Using an internal framework for audits, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve your ability to detect a data breach and escalate containment efforts.

Invest in security orchestration, automation and response (SOAR) and XDR to help improve detection and response times.
Along with security AI and automation, XDR capabilities can help significantly reduce average data breach costs and breach lifecycles. According to the study, organizations with XDR deployed shortened the breach lifecycle by 29 days on average compared to organizations that didn't implement XDR, with a cost savings of USD 400,000. SOAR and security information and event management (SIEM) software, managed detection and response services and XDR can help your organization accelerate incident response with automation, process standardization and integration with your existing security tools.

Use tools that help protect and monitor endpoints and remote employees.
In the study, breaches where remote work was a factor in causing the breach cost nearly USD 1 million more than breaches where remote work wasn't a factor. Unified endpoint management (UEM), endpoint detection and response (EDR) and identity and access management (IAM) products and services can help provide security teams with deeper visibility into suspicious activity. This oversight involves bring your own devices (BYOD) and company laptops, desktops, tablets, mobile devices and IoT, including endpoints the organization doesn't have physical access to. UEM, EDR and IAM speed investigation and response time to isolate and contain the damage in breaches where remote work was a factor.

Create and test incident response playbooks to increase cyber resilience.
Two of the most effective ways to mitigate the cost of a data breach are forming an incident response (IR) team and extensive testing of the IR plan. Breaches at organizations with IR teams that regularly test their plan saw USD 2.66 million in savings compared to breaches at organizations with no IR team or testing of the IR plan. Organizations can respond quickly to contain the fallout from a breach by establishing a detailed cyberincident playbook. Routinely test that plan through tabletop exercises or run a breach scenario in a simulated environment such as a cyber range.

Adversary simulation exercises, also known as red team exercises, can enhance the effectiveness of IR teams by uncovering attack paths and techniques they might miss and identifying gaps in their detection and response capabilities. An attack surface management solution can help organizations improve their security posture by locating previously unknown exposure points through simulations of an authentic attack experience.

Recommendations for security practices are for educational purposes and don't guarantee results.

About Ponemon Institute and IBM Security

Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards, and doesn't collect any personally identifiable information from individuals or company identifiable information in business research. Furthermore, strict quality standards ensure that subjects aren't asked extraneous, irrelevant or improper questions.

IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than 4.7 trillion events per month in more than 130 countries, IBM holds over 10,000 security patents. To learn more, visit ibm.com/security. Join the conversation in the IBM Security Community.

If you have questions or comments about this research report, including for permission to cite or reproduce the report, please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

Take the next steps

Zero trust security solutions
Wrap security around every user, device and connection.
Learn more

Identity and access management
Connect every user, API and device to every app securely.
Learn more

Data security
Discover, classify and protect sensitive enterprise data.
Learn more

Security orchestration, automation and response
Accelerate incident response with orchestration and automation.
Learn more

Security information and event management
Gain visibility to detect, investigate and respond to threats.
Learn more

Cloud security
Integrate security into your journey to hybrid multicloud.
Learn more

Endpoint security
Protect devices, users and organizations against sophisticated attacks.
Learn more

Cybersecurity services
Reduce risk with consulting, cloud and managed security services.
Learn more

Incident response and threat intelligence
Proactively manage and respond to security threats.
Learn more

Schedule a one-on-one consultation with an IBM Security X-Force expert
Schedule now

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2022