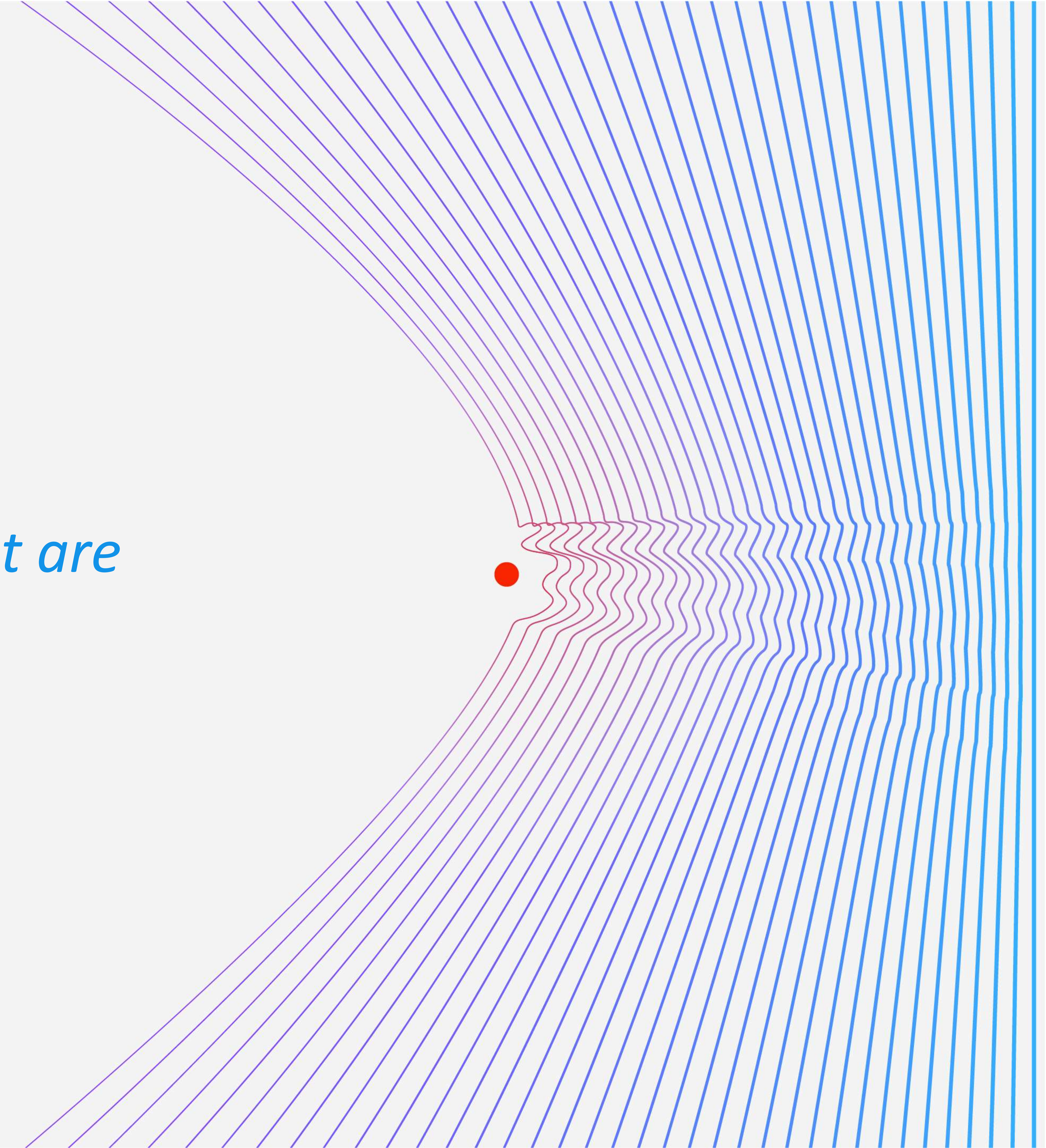
IBM **Security**

Cost of a Data Breach Report 2023

How costly is a data breach and what are the most effective countermeasures

Marcus Schmid
IBM Cybersecurity Strategy & Risk Leader



Agenda

01

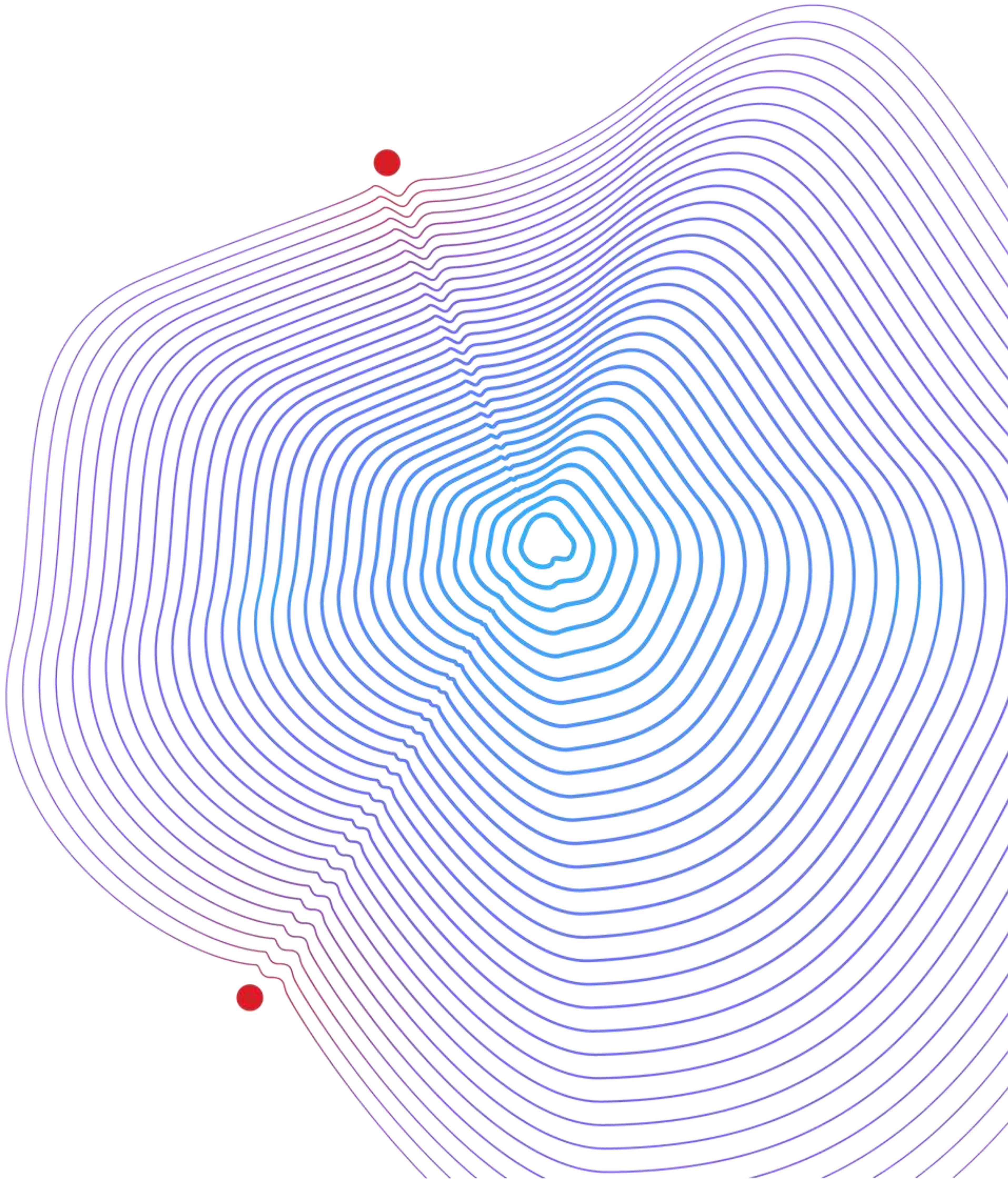
What do you get out of this report and what evidence is it based on?

02

Key findings

03

Recommendations to help reduce the cost of a data breach



What do you get out of this report and what evidence is it based on?

Offers a detailed investigation of factors that influence financial impacts of a data breach to organizations

Organizations can learn what security measures can mitigate costs

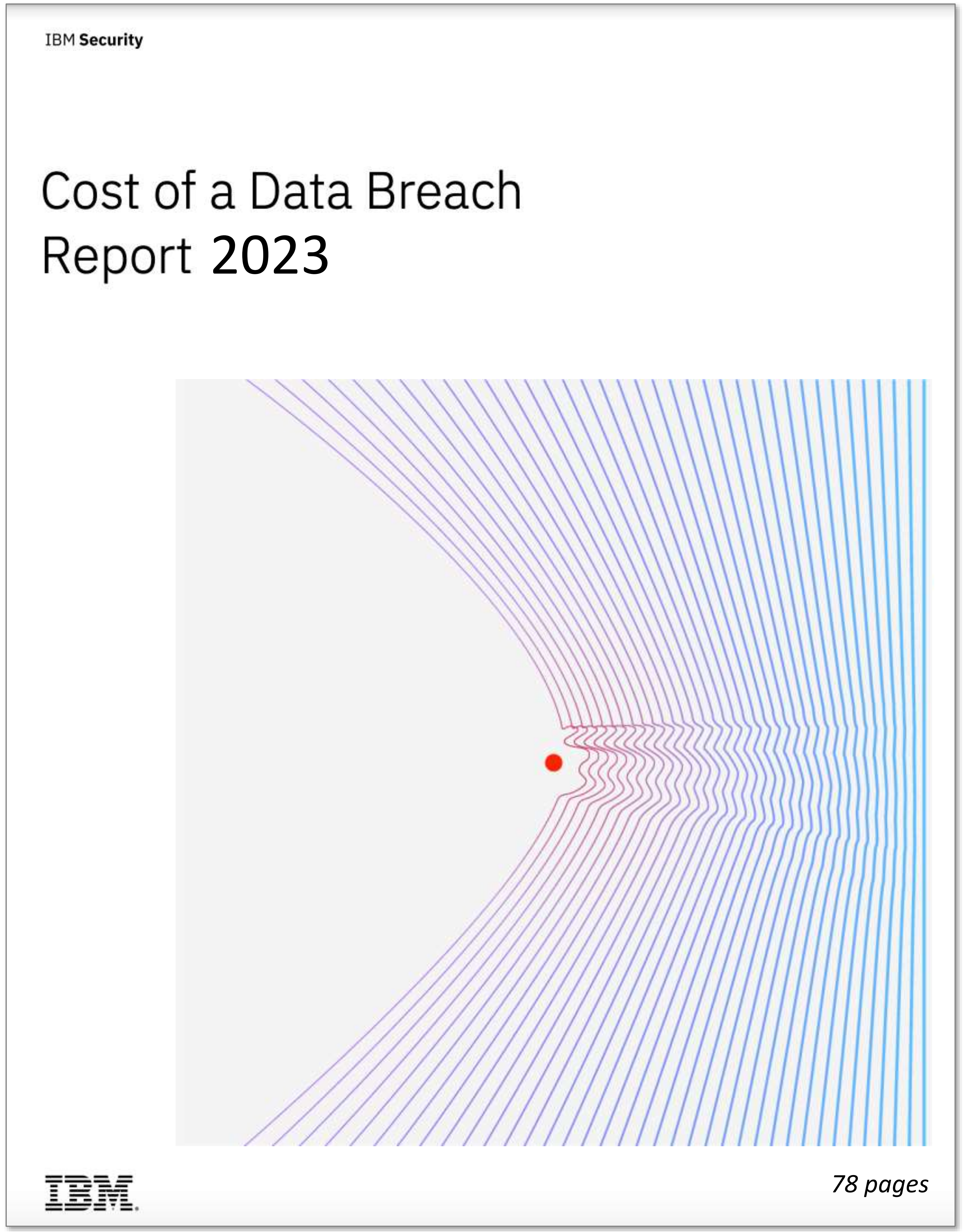
550+ real world breaches analyzed between March 2022 and March 2023

3,475 interviews

16 countries/regions

17 industries

18th consecutive year



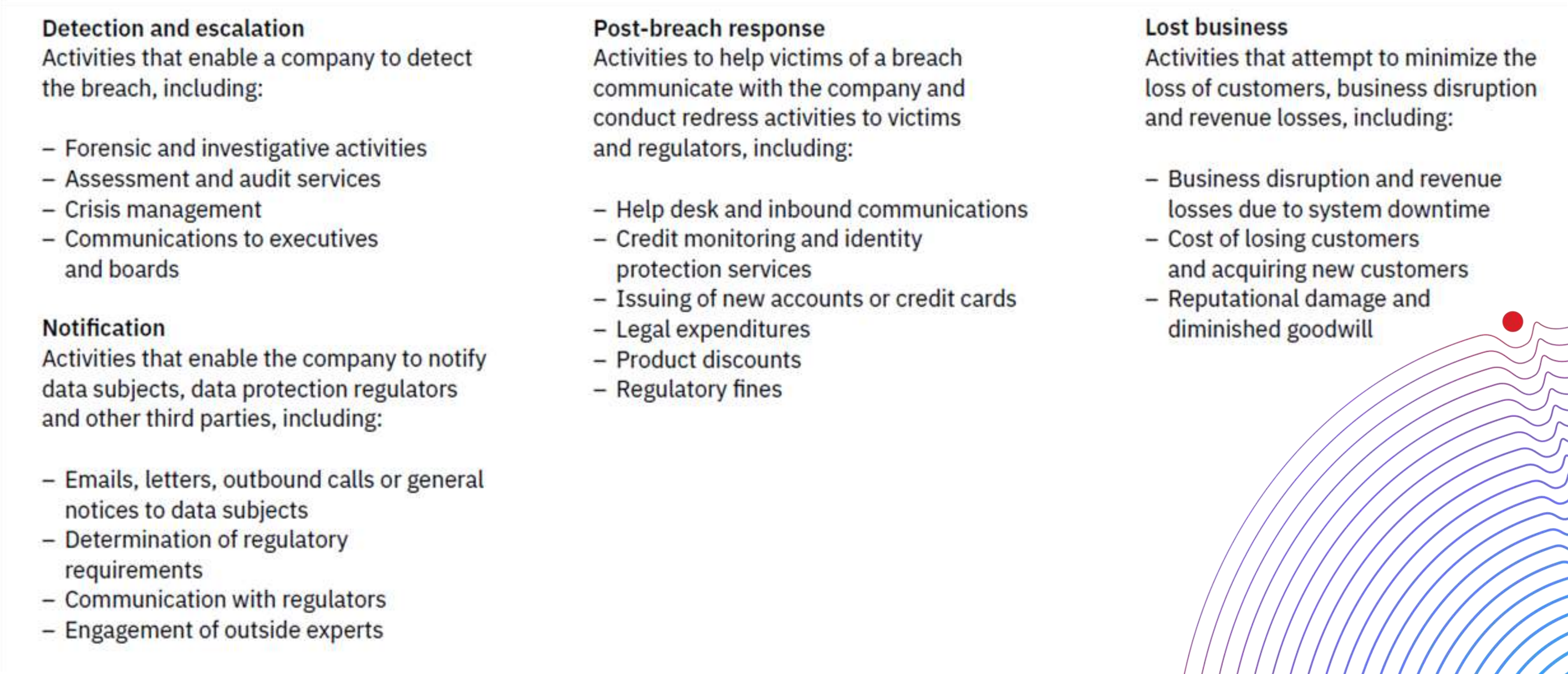
IBM Security

Cost of a Data Breach Report 2023

IBM

78 pages

How is the cost of a data breach calculated?



Detection and escalation
Activities that enable a company to detect the breach, including:

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

Notification
Activities that enable the company to notify data subjects, data protection regulators and other third parties, including:

- Emails, letters, outbound calls or general notices to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

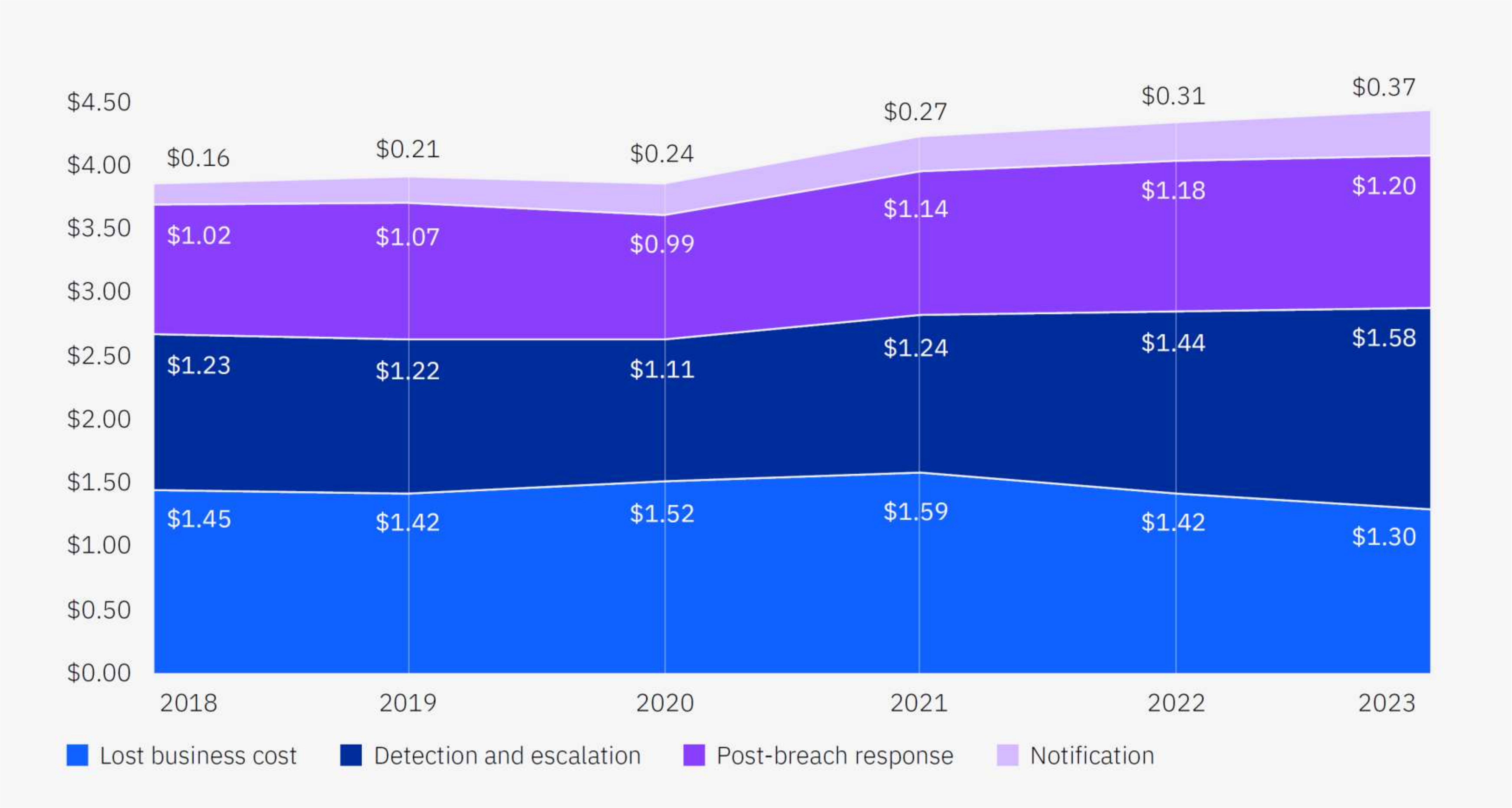
Post-breach response
Activities to help victims of a breach communicate with the company and conduct redress activities to victims and regulators, including:

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing of new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines

Lost business
Activities that attempt to minimize the loss of customers, business disruption and revenue losses, including:

- Business disruption and revenue losses due to system downtime
- Cost of losing customers and acquiring new customers
- Reputational damage and diminished goodwill

The average cost of a data breach is at an all-time high of 4.45 M$ and has increased by 15.3% over the last 3 years



Cost segments of a data breach [in MUSD]

The average cost varies intensely by industry. Healthcare and financial are consistently on top

1. Healthcare – USD 10.93 million

2. Financial – USD 5.90 million

3. Pharmaceuticals – USD 4.82 million

4. Energy – USD 4.78 million (+1)

5. Industrial – USD 4.73 million (+2)

6. Technology – USD 4.66 million (-2)

7. Services – USD 4.47 million (-1)

8. Transportation – USD 4.18 million (+5)

9. Communications – USD 3.90 million (+3)

10. Consumer – USD 3.80 million (-1)

11. Education – USD 3.65 million (-1)

12. Research – USD 3.63 million (-4)

13. Entertainment – USD 3.62 million (-2)

14. Media – USD 3.58 million (+1)

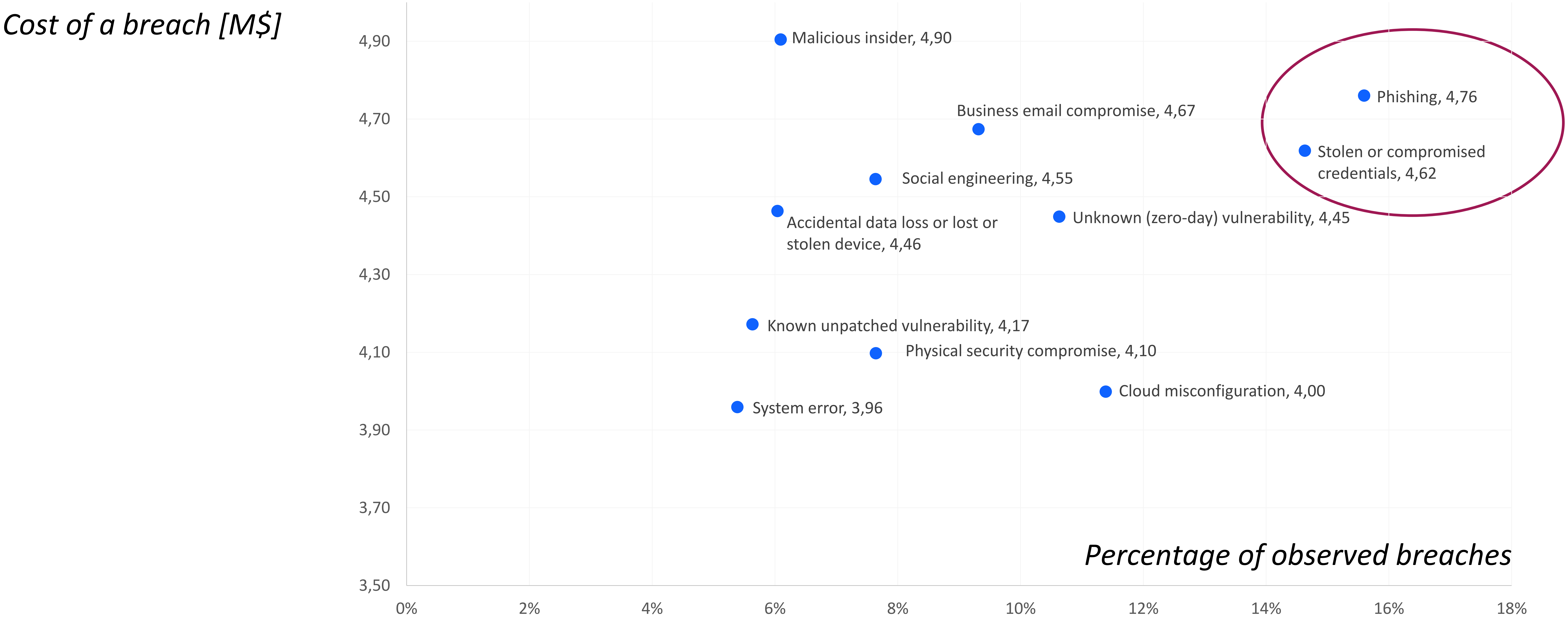
15. Hospitality – USD 3.36 million (+1)

16. Retail – USD 2.96 million (-2)

17. Public sector – USD 2.60 million

- Avg breach cost increased YtY
- Average breach cost decreased YtY
- +/- indicates movement of rank

Average cost and frequency of data breaches vary by initial attack vector – phishing and stolen credentials are top entry points



More quantitively evidenced findings

1 in 3

Only 1 out 3 breaches are identified by an organization’s own security teams or tools

Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. 67% of breaches were reported by a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection.

USD 470,000

Additional cost experienced by organizations that didn’t involve law enforcement in a ransomware attack

This year’s research shows that excluding law enforcement from ransomware incidents led to higher costs. While 63% of respondents said they involved law enforcement, the 37% that didn’t also paid 9.6% more and experienced a 33-day longer breach lifecycle.

USD 1.76M

The effect of extensive security AI and automation on the financial impact of a breach

Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches. Organizations that used these capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. They also reported USD 1.76 million lower data breach costs compared to organizations that didn’t use security AI and automation capabilities.

USD 1.68M

Cost savings from high levels of DevSecOps adoption

Integrated security testing in the software development process (DevSecOps) showed sizable ROI in 2023. Organizations with high DevSecOps adoption saved USD 1.68 million compared to those with low or no adoption. Compared to other cost-mitigating factors, DevSecOps demonstrated the largest cost savings.

USD 1.49M

Cost savings achieved by organizations with high levels of IR planning and testing

In addition to being a priority investment for organizations, IR planning and testing emerged as a highly effective tactic for containing the cost of a data breach. Organizations with high levels of IR planning and testing saved USD 1.49 million compared to those with low levels.

Most effective recommend-dations that reduce the cost of a data breach

1	Strengthen resiliency by knowing your attack surface and **practicing incident response**	- 1.49 M$
2	Build security into **every stage of software development** and deployment—and test regularly	- 1.68 M$
3	Use security AI and **automation** to increase speed and accuracy	- 1.76 M$
4	Keep **employee training** on a high level	- 1.50 M$

Where to find more information

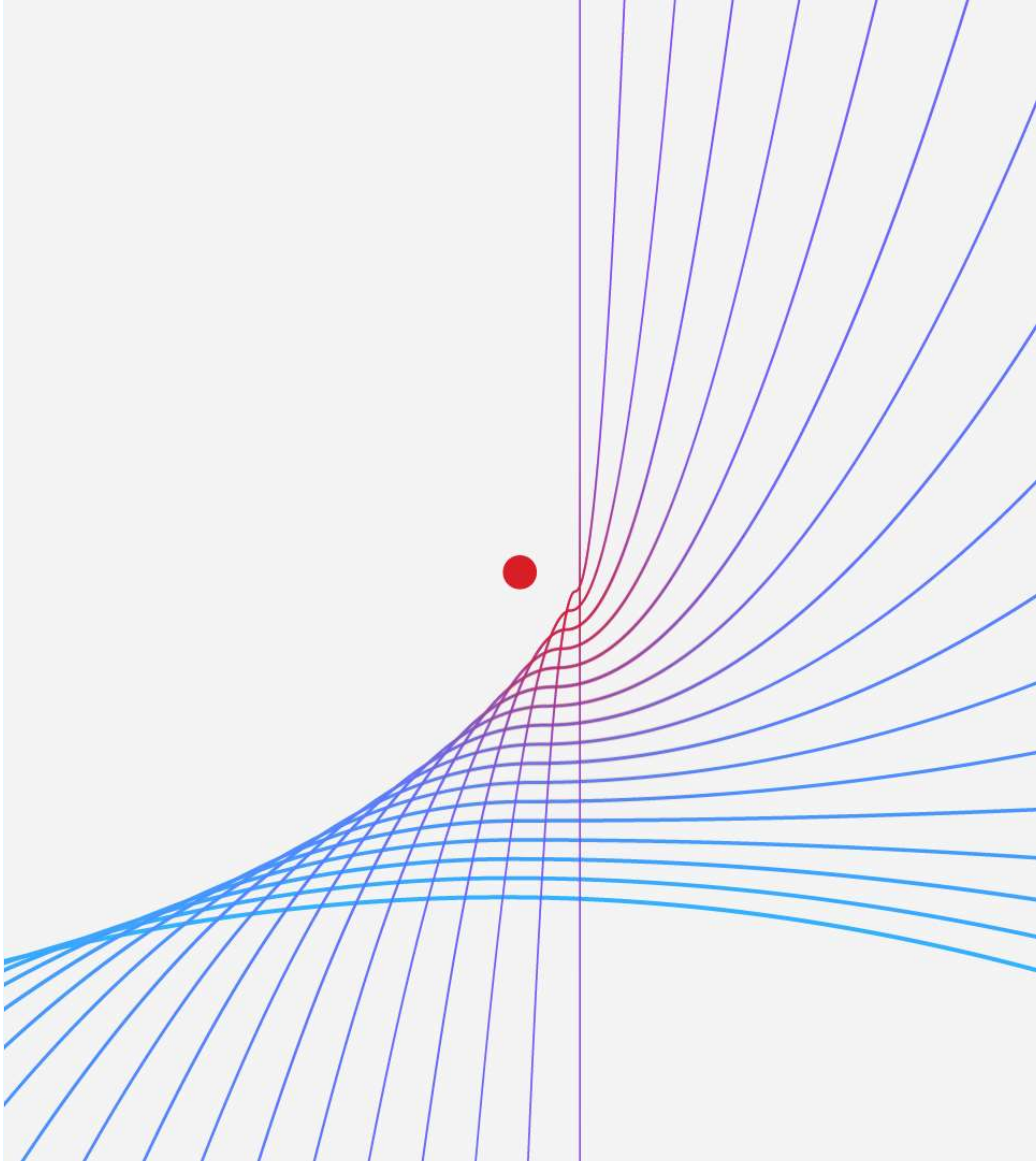
Report website
ibm.biz/breach-report

Top findings and recommendations webinar
ibm.biz/data-breach-webinar

Security Intelligence overview blog
ibm.biz/breach-blog

IBM Security® X-Force® expert consultation
ibm.biz/book-a-consult

Cost of a Data Breach Action Guide
ibm.biz/CODBActionGuide



Thank you.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Generally expected results cannot be provided as each client's results will depend entirely on the client's systems and services ordered. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.