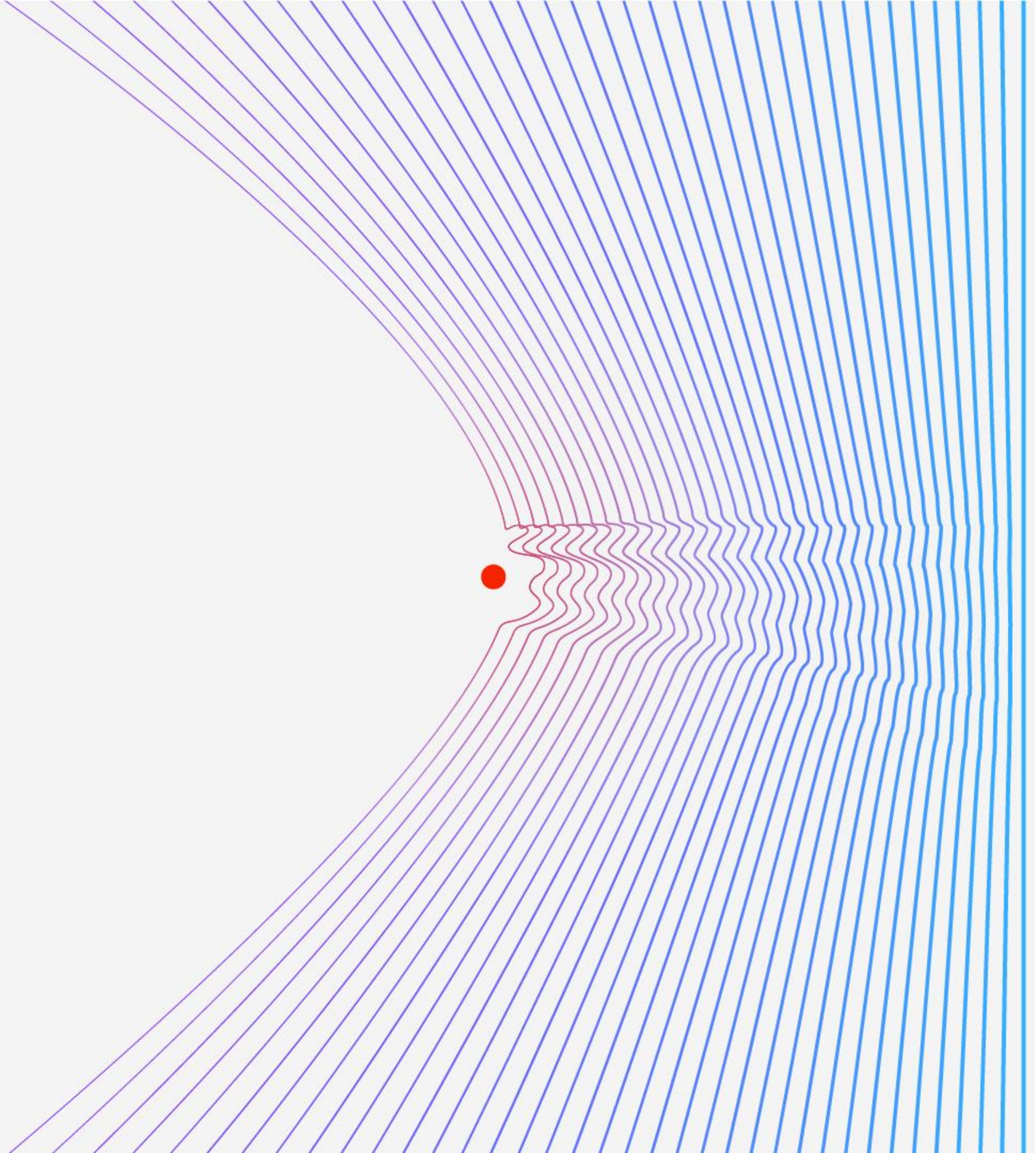
Cost of a Data Breach Report 2023

Enablement

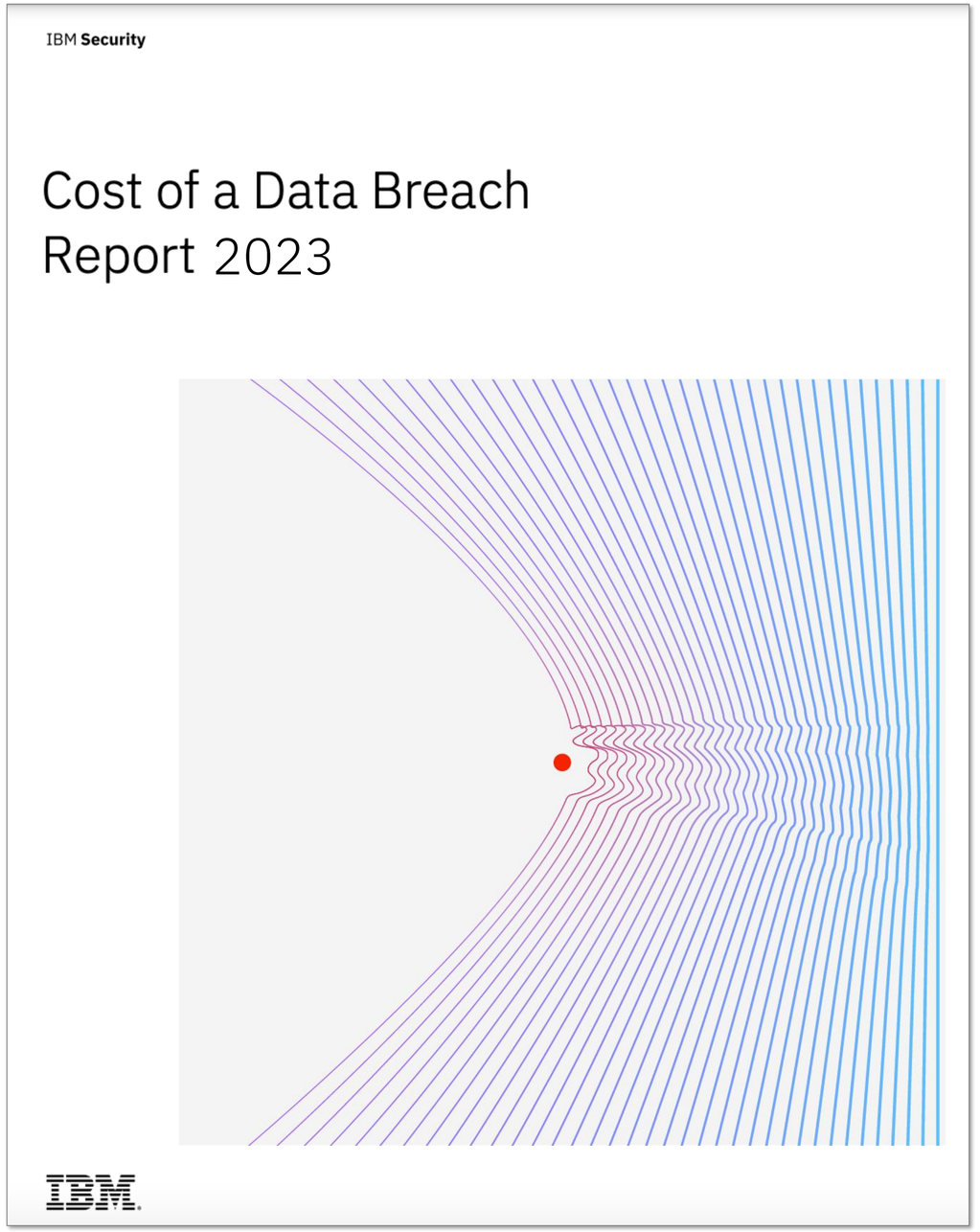


Cost of a Data Breach Report 2023

Launch Date: July 24

Offers a detailed investigation of factors that influence financial impacts to organizations. Organizations can learn what security measures can mitigate costs.

- ✓ #1 marketing asset for responses and revenue year over year
- ✓ Proprietary research, credible with buyers
- ✓ 3,600+ interviews, 550+ breaches analyzed, 16 countries/regions, 17 industries, 18th year



Client Facing Webinar- Register Here

Tues, Aug 1, 2023 11:00 AM EST

The Cost of a Data Breach 2023: Insights, Mitigators and Best Practices

Key findings

Average cost of a data breach reached a record high in 2023, but security investments at organizations are divided

USD 4.45 million

Average cost of a data breach

USD 10.93 million

Average cost of a breach in healthcare, the highest for 13 years in a row

51%

Organizations that planned to increase security investments as a result of a breach, with top investments in incident response (IR) planning and testing, employee training, and threat detection and response

Using a DevSecOps approach, deploying IR teams and security AI and automation produced large savings

USD 1.68 million

Savings for organizations using a DevSecOps approach at a high level compared to other organizations at a low level or no use of DevSecOps

USD 1.49 million

Savings for organizations with an IR team and regularly tested IR plan versus no IR team or IR testing

108 days

Breach response time saved for organizations with extensive use of security AI and automation

USD 1.76 million

Savings for organizations with extensive use of security AI and automation compared to organizations with no security AI or automation deployed

Industry-ranked. Report.

Key findings

Costs were highest and breaches took longer to contain when breached data was stored across multiple environments

39%

Amount of breached data stored across multiple types of environments including public, private and hybrid clouds and on premises

292 days

Breach response time when data was stored across multiple environments, 15 days longer than the overall average for containing a breach

USD 750,000

Amount of higher breach costs when breached data was stored across multiple environments versus on premises only

Detecting the breach with internal security teams and involving law enforcement led to savings

33%

Percentage of organizations detected a breach using their internal security systems and teams, or their managed security service providers (MSSPs), versus disclosed by a benign third party or by the attacker

33 days

Average containment time saved by organizations that involved law enforcement in a ransomware attack

USD 1 million

Average savings for organizations that detected a breach internally versus having the breach disclosed by an attacker such as in extortion or ransomware

Need in response and containment

277 days

Time to identify and contain a data breach in 2023, same number of days as 2022

Solutions for speed

- Organizations with an extensive use of **security AI and automation** detected and contained an incident on average 108 days faster versus organizations that didn't use security AI and automation
- Breaches at organizations with **AI and automation** tools cost USD 1.76 million less than those with no AI and automation deployed
- Average breach cost savings associated with a regularly tested **IR plan** was USD 1.49 million, compared to no IR plan or IR testing
- Having an **attack surface management (ASM)** solution leads to breach containment that is 83 days faster than without an ASM solution
- In a **ransomware** attack, organizations that involved law enforcement saw breach containment times that were 33 days faster than without law enforcement involvement

USD 1.02 million

Savings in average breach costs when the breach was contained in under 200 days

Industries ranked by cost

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

Countries ranked by cost

1. United States – USD 9.48 million

2. Middle East – USD 8.07 million

3. Canada – USD 5.13 million

4. Germany – USD 4.67 million (+1)

5. Japan – USD 4.52 million (+1)

6. United Kingdom – USD 4.21 million (-2)

7. France – USD 4.08 million
8. Italy – USD 3.86 million

9. Latin America – USD 3.69 million (+4)

10. South Korea – USD 3.48 million (-1)

11. Association of Southeast Asian Nations (ASEAN) – USD 3.05 million (+1)

12. South Africa – USD 2.79 million (-2)

13. Australia – USD 2.70 million (-2)

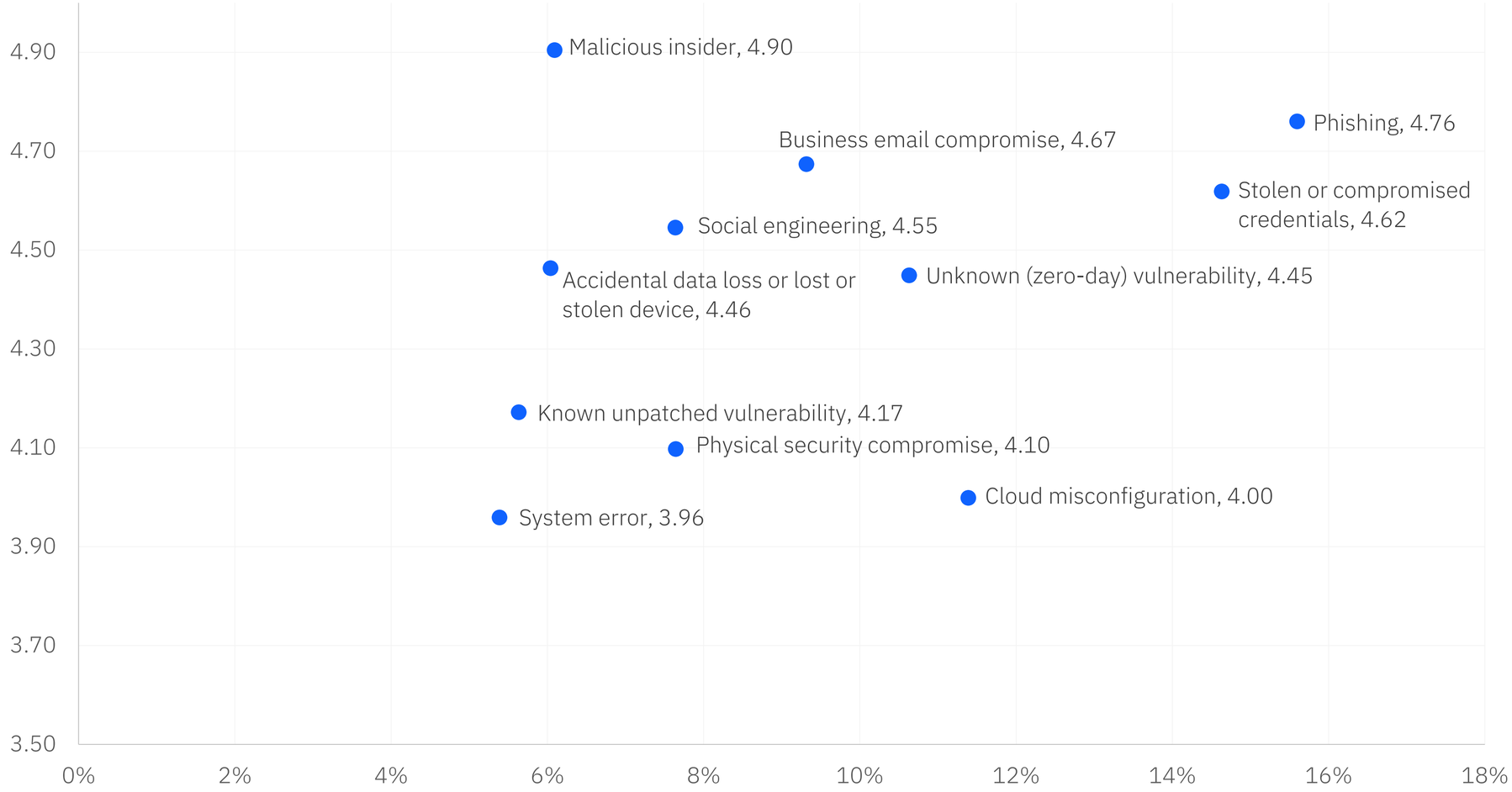
14. India – USD 2.18 million
15. Scandinavia – USD 1.91 million

16. Brazil – USD 1.22 million

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

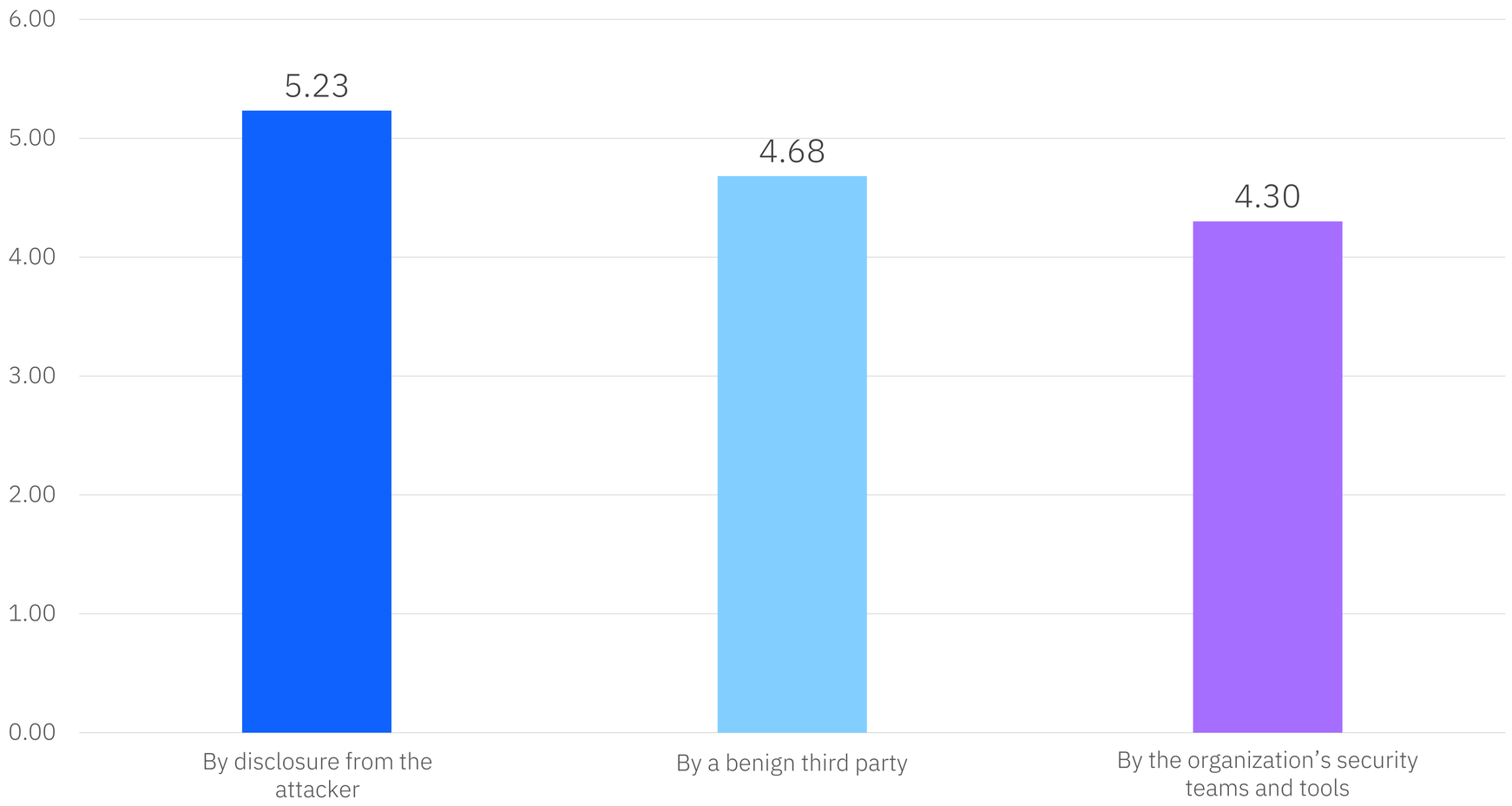
Average cost and frequency of data breaches by initial attack vector

USD millions



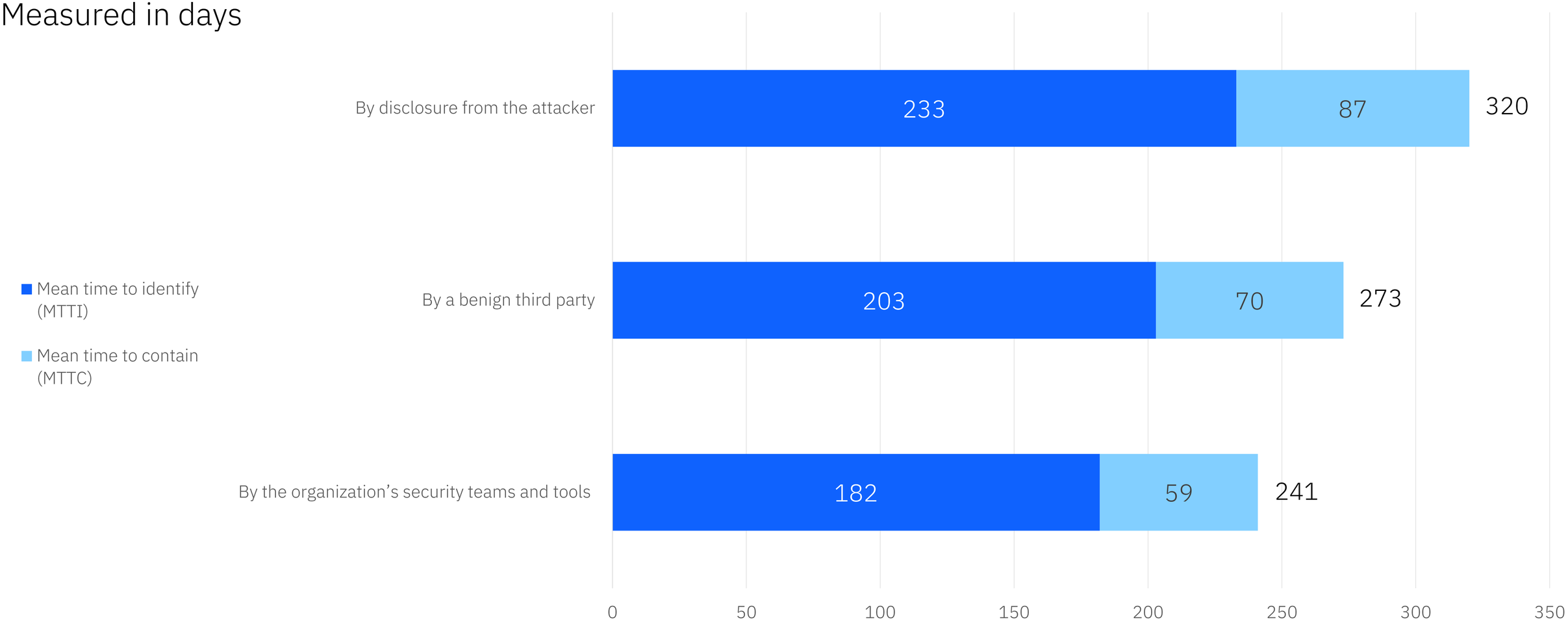
Average cost of a data breach by how the breach was identified

Measured in
USD millions



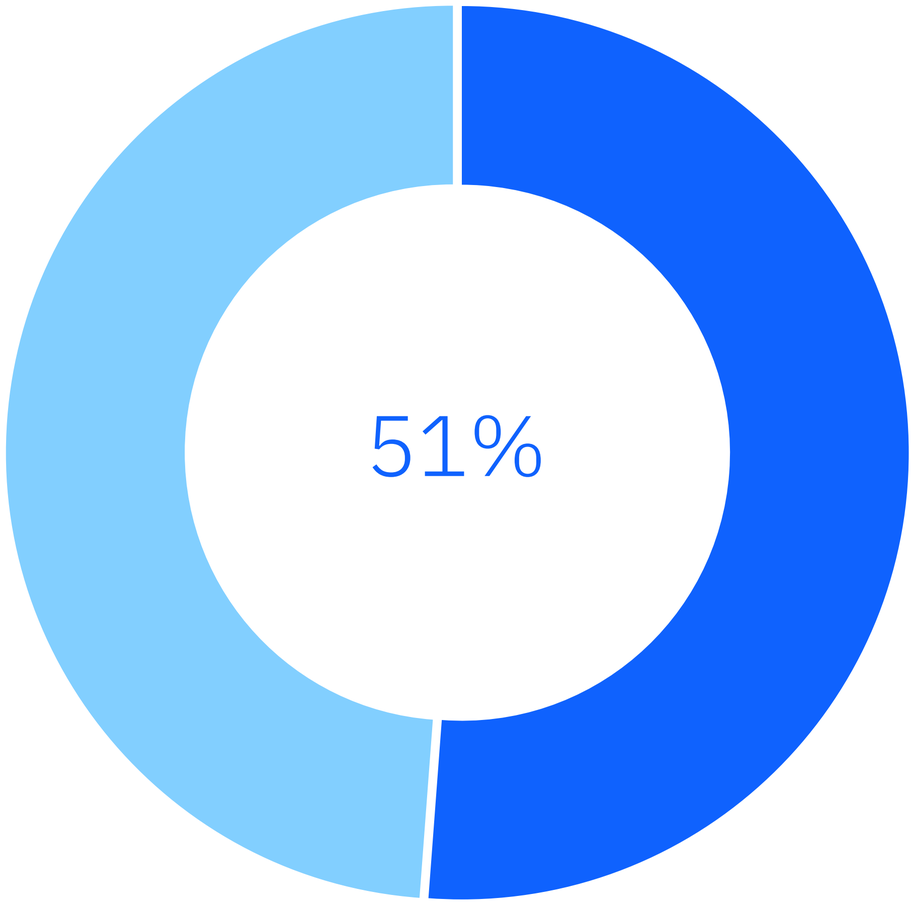
Average time to identify and contain a breach by how the breach was identified

Measured in days



Following the data breach, will your organization increase its security investment?

Percentage that responded yes

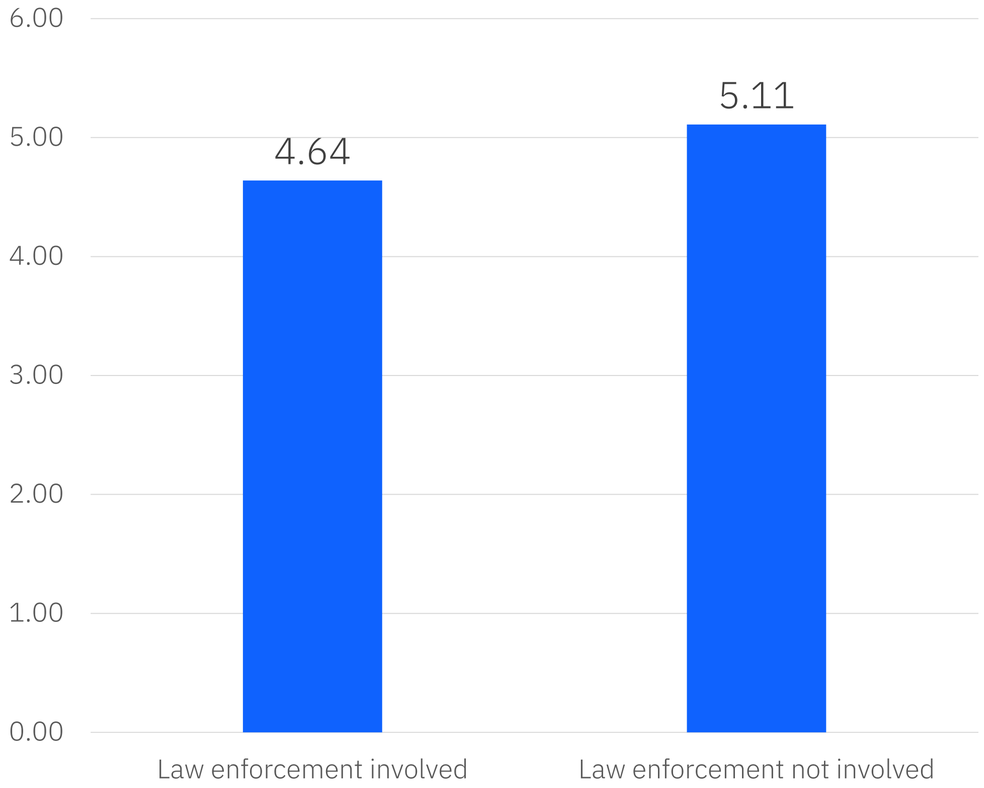


Share of organizations increasing types of security investment following a data breach

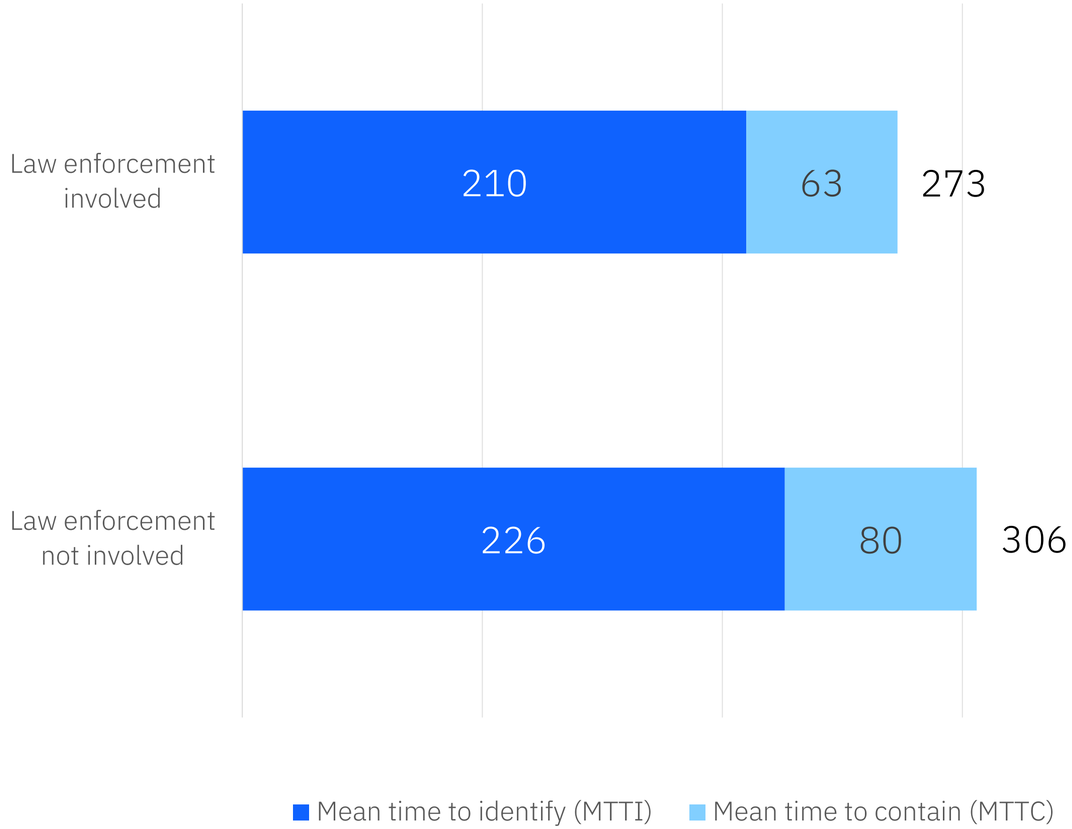
More than one response permitted

Ransomware attacks with law enforcement involved

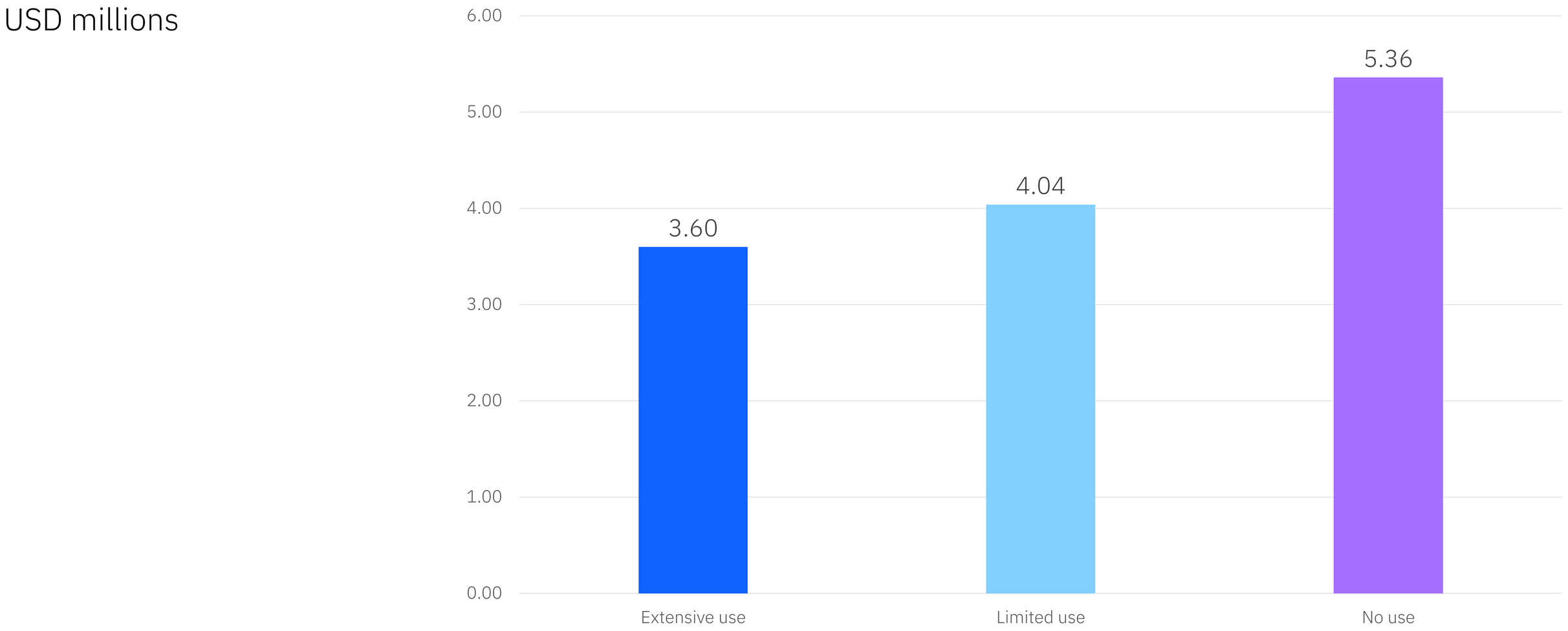
Average cost measured in USD millions



Average time to identify and contain measured in days

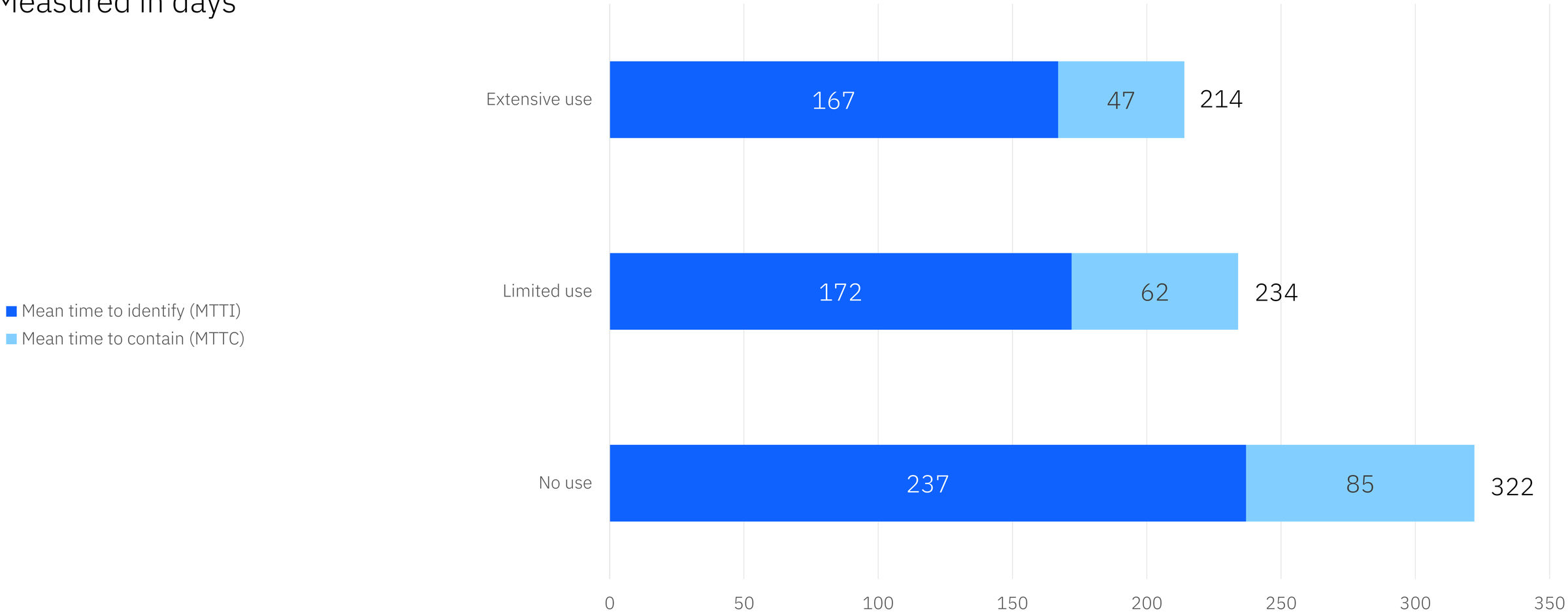


Average cost of a data breach by security AI and automation deployment level



Average time to identify and contain a data breach by level of security AI and automation

Measured in days



Recommendations

Build security into every stage of software and hardware development and test regularly:

- Employing a DevSecOps approach, which was the top cost mitigator in the 2023 report, is crucial for integrating security into organizational tools and platforms.
- Application developers should adopt secure by design and secure by default principles for security during the initial design phase of digital transformation projects.
- Apply the same principles to cloud environments to protect user privacy and minimize attack surfaces.
- Conduct application testing or pen testing from an attacker's perspective to identify and patch vulnerabilities before they result in breaches.

Protect data across hybrid cloud environments:

- 82% of data breaches involved data stored in cloud environments, with 38% spanning multiple environments.
- Make it a top priority to gain visibility and control over data in hybrid cloud environments.
- Seek data security and compliance technologies that work across platforms to protect data as it moves between databases, applications and services.
- Utilize data activity monitoring solutions to enforce controls and detect suspicious activity in real

Recommendations

Use security AI and automation to increase speed and accuracy:

- Only 28% of organizations extensively used AI and automation in their security operations, highlighting an opportunity for improvement.
- Extensive use of AI and automation resulted in significant cost savings and faster breach identification and containment.
- Embed AI and automation throughout security tool sets to enhance threat detection, response and investigation.
- Use mature AI technologies with demonstrated accuracy, effectiveness and transparency to eliminate bias and blind spots.
- Integrate core security technologies for seamless workflows and shared insights, using threat intelligence reports for pattern recognition and threat visibility.

Strengthen resiliency by knowing your attack surface and practicing incident response:

- Understand your industry and organization's exposure to relevant attacks and prioritize security accordingly.
- Use ASM tools or adversary simulation techniques for an attacker-informed perspective on risk profile and vulnerabilities.
- Establish a team well-versed in IR protocols and tools to reduce costs and breach containment time.
- Develop IR plans, conduct regular testing, and consider having an IR vendor on retainer for quicker breach response.

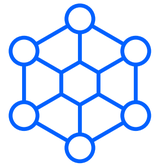
IBM solutions that can help

Proactively plan for attacks. With the increase in ransomware, ensure you have an incident response plan and team that can address blended ransomware and data theft extortion techniques and rehearse your plan. IBM Security X-Force Incident Response Retainer can help you with building and testing plans, simulated attack exercises like the IBM Cyber Range, "surge assistance" on speed dial and boots-on-the-ground fast response to incidents.

Get in front of the threat rather than react to it. Get a better understanding of threat actor motivations and tactics to prioritize security resources by leveraging IBM Security X-Force Threat Intelligence. Discover attack patterns and techniques that are more likely to be exploited by a real-world attacker with IBM Security Randori Recon.

Improve detection and response times. Reinvigorate internal detection programs to find and stop exploitation attempts quickly and effectively utilizing AI by investing in:

- IBM Security QRadar Suite
- IBM Security Managed Detection and Response Services.



Harden your infrastructure. Data shows ransomware was a top threat type and phishing and vulnerability exploitation were the most common infection vectors. Be sure to have backups, test them often and store them offline. Check your patch management structure to uncover risky vulnerabilities with IBM Security X-Force Red Vulnerability Management Services.

IBM solutions that can help (cont.)

Protect your data. Provide comprehensive data protection for on-prem and cloud data stores with IBM Security Guardium Data Protection. As your attack surface grows from migrating to the cloud, develop a data-centric cybersecurity program with comprehensive protection, centralized visibility, and monitoring against unauthorized access, exposure or data theft with IBM Data Security Services .

Security by design. Build security into every stage of your digital transformation by charting your journey with an iterative framework that guides you from ideation, to build, to scale using IBM Garage™

Apply rigorous best practices to cloud security. With cybercriminals moving to the cloud, develop a unique incident response plan, tools and team designed specifically to respond to cloud attacks with help from IBM Security Cloud Security Services.

Starting the conversation

#1 call-to-action/goal:

Drive clients/prospects for 1:1 briefing via ibm.biz/book-a-consult or reach out to Jeff Soukup to schedule.

Before the call/meeting, read the Cost of a Data Breach Report or executive summary and frame your conversation around top insights:

- Average cost of a data breach has reached a record high of USD 4.45 million
- When breached data was stored across multiple environments costs were $0.75M higher and breaches took 15 days longer to contain
- Using a DevSecOps approach, deploying incident response teams and AI/automation produced large savings
- As a result of breaches, 51% of organizations plan to increase their security investment with top investments planned for incident response (IR) planning and testing, employee training, and threat detection and response.
- Detecting the breach with internal security teams led to savings of up to $1M and involving law enforcement led to savings of $0.47M and 33 days in breach containment

Conversation starters

- We just released the 2023 Cost of a Data Breach Report, one of our top research pieces
- This report can help organizations understand what factors increase or mitigate the cost of breaches
- Based on data and insights from the research, the report offers recommendations to help strengthen your security posture
- I'd be happy to talk through the top insights and recommendations

Narrowing it down

- This report highlights a few trends like (include a few report top insights listed on left).
- What types of threats are you seeing in your organization or industry?
- Have you had any challenges in defending against recent threats?
- The Cost of a Data Breach Report also includes a few best practices based on the research data. Would you like me to walk you through some of those tips to see if you have any thoughts on where you might want to learn more on where IBM can help?

Hot Links:

Report main page:
ibm.biz/breach-report

External webinar
ibm.biz/breach-webinar

Book a consult w/ X-Force expert
ibm.biz/book-a-consult

Security Intelligence blog
ibm.biz/breach-blog (to be updated at launch)

Seismic page for CODB
ibm.biz/CODB-Seismic
(client deck, 2 pager, seller email template, enablement recording, geo & industry slides and more!)

Marketing contact:

Sarah Dudley
Sr. Product Marketing Manager, Cyber Threat Mgmt, IBM Consulting Cybersecurity Services
sdudley@us.ibm.com

Launch calendar

IBM Sec + IBM Consulting actions

Launch | **Internal** Communications | **External** Communications | **Ongoing** Communications

LAUNCH DAY

- Full report, action guide & web experience launches
- Launch blog (SI and IBM.com), IBM Newsletter
- IBM Security Community pages & newsletter
- Press release + media outreach
- Email campaign
- Paid + owned social (Twitter, LinkedIn, YouTube) + social enablement kit
- CTA on IBM Homepage and several IBM Security and Consulting web pages
- Partner Plus outbound email + social push
- Comms launch announcement across BUs
- All top Slack channels
- w3 internal blog + email from Chris McCurdy
- IBMer News
- Sales enablement materials on Seismic & Content Plus (inc. seller email, client deck, 1-pager, geo/industry slides, reasons to call, call script, etc)

IBM Sec + Consulting leadership launch call

IBM Consulting Americas LCP briefing

Sales enablement live session at 11am EST

June 28 | July. 3 | July 5 | July 12 | July 13 | July 18 | July 20 | July 24 | **July/August** | **Ongoing drum beat and measurement**

Final report from Blue Studio complete

Webinar email push #1

IBM Champions briefing

Webinar email push #2

- Paid Search
- IBM Blog series: Product demos
- IBM Tech Now video announcement

- IBM Consulting Client Partner Calls (LCP)
- Geo leader calls
- External Webinar 8/1
- Black Hat
- Owned Social Push #2 & #3
- Lighthouse/Content+ comms (Spotlight, newsletter, slack channels)

- IBM SME POV blog/IBM blog series
- Event activations: CISO ExecNets, Cyber Security Summits, Gartner IAM, Evanta events

Questions?