

THE FINANCIAL IMPACT OF CYBERSECURITY BREACHES

As cybercrime continues to evolve, the financial risks associated with inadequate cybersecurity measures highlight the urgent need for businesses to adopt proactive defense mechanisms and expedite response times to minimize both immediate and long-term costs.

DISCOVER THE TOTAL COSTS ASSOCIATED WITH CYBERATTACKS

CYBER BREACHES BY THE NUMBERS

\$10.5 Trillion
total costs worldwide in 2025 (Forbes Advisor, 2024)

\$9.36 Million
direct costs per U.S. incident (Forbes Advisor, 2024)

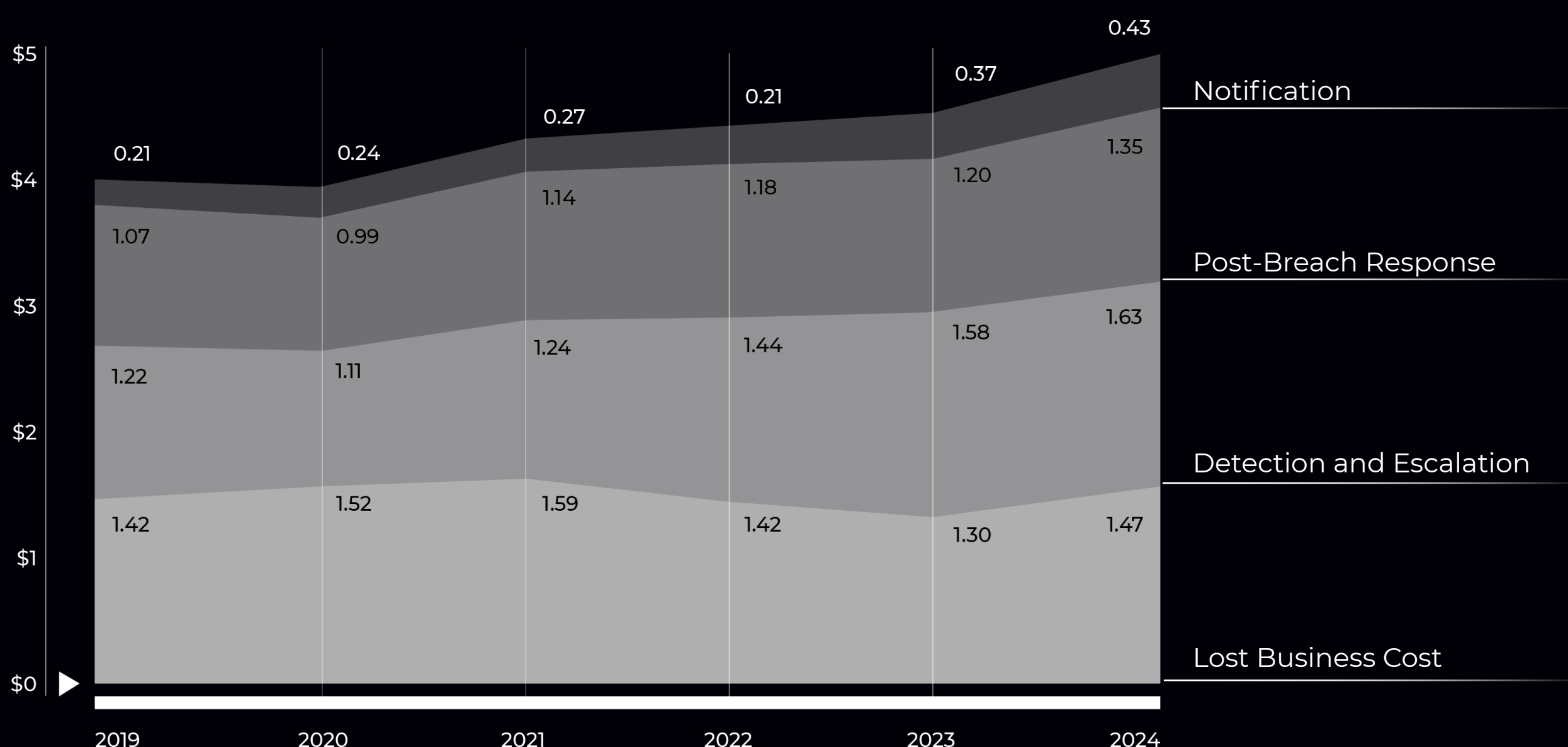
\$1.63 Billion
direct expenses in 2024 (IBM, 2024)

\$1.47 Billion
in recovery measures in 2024 (IBM, 2024)

UNDERSTAND YOUR FINANCIAL RISK

AVERAGE COST OF A DATA BREACH BY PHASE, BY YEAR

(Measured in USD millions; Source: IBM, 2024)



TOP 3 CYBER BREACH DIRECT EXPENSES IN 2024

Largest direct expense = cost of investigating breaches

Second largest direct expense = recovery measures

Third largest direct expense = Immediate loss of revenue due to operational disruption

TYPES OF CYBER BREACH EXPENSES

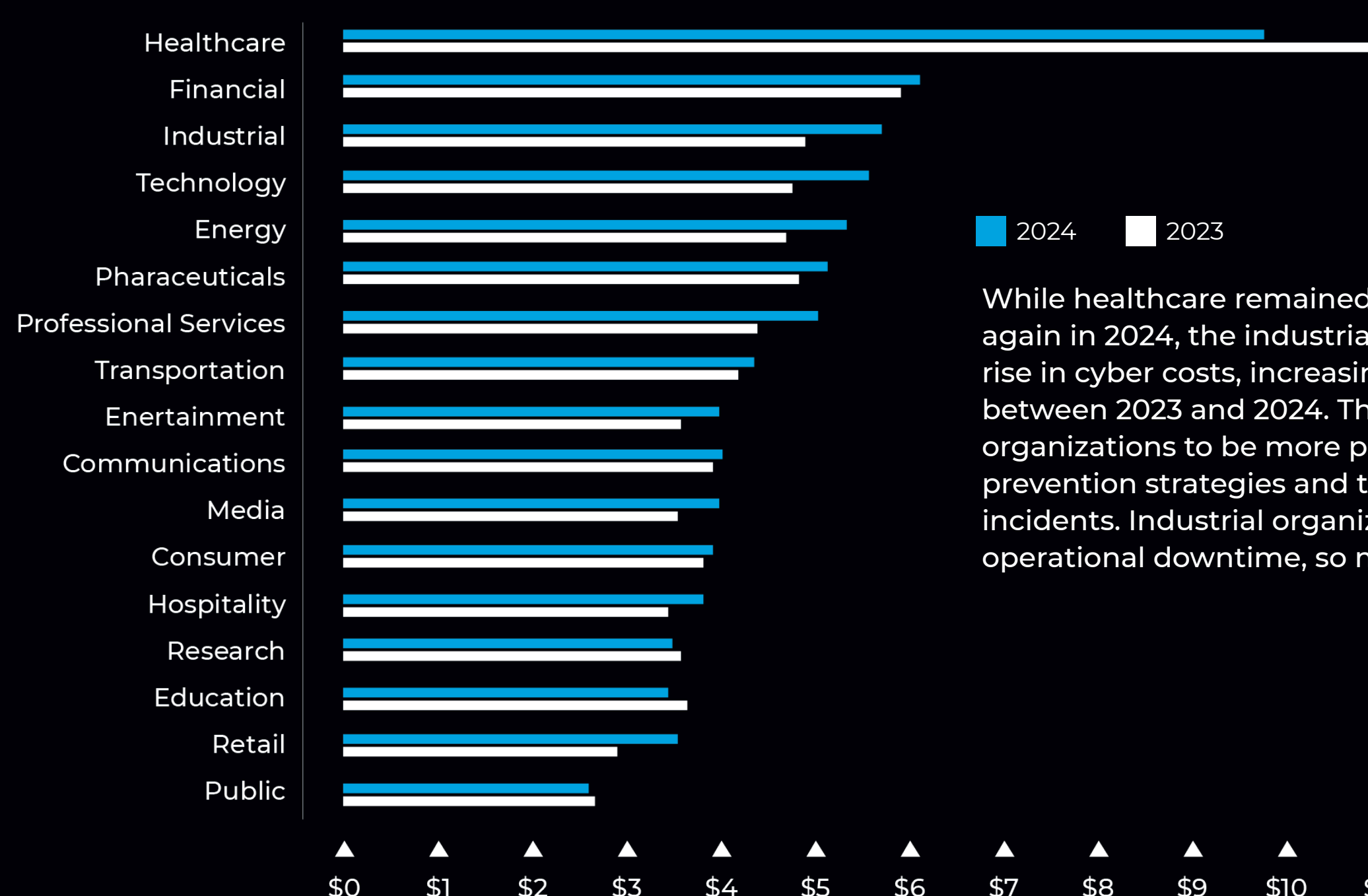
DIRECT COSTS
Investigating breaches
Recovery measures
Operational disruption

INDIRECT COSTS
Customer trust
Reputational damage
decline in market value.

HIDDEN COSTS
Loss of intellectual property
Future security investments
Insurance premiums
Legal expenses

CYBER BREACH EXPENSES BY INDUSTRY

(Measured in USD millions; Source: IBM, 2024)



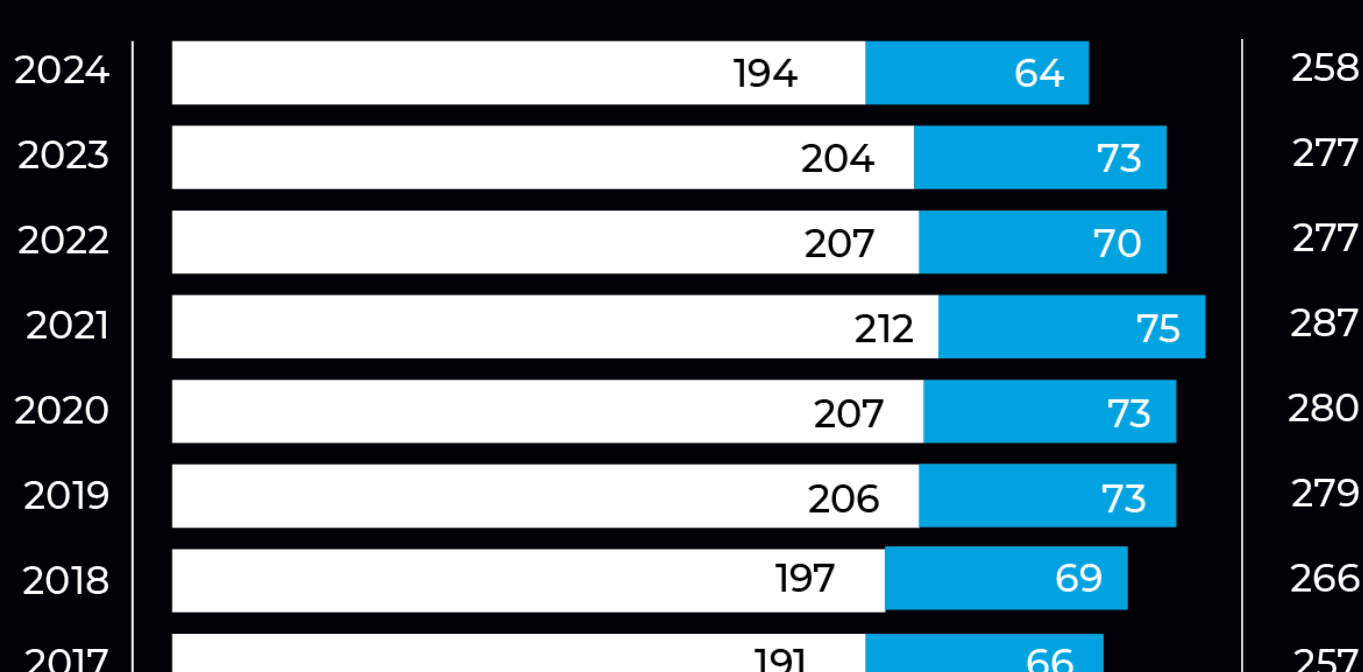
While healthcare remained at the top of the industry costs again in 2024, the industrial market suffered from the largest rise in cyber costs, increasing by an average of \$830,000 between 2023 and 2024. This marks the need for industrial organizations to be more proactive with cybersecurity prevention strategies and to respond quicker to cyber incidents. Industrial organizations are particularly sensitive to operational downtime, so mitigation is of the essence.

AVERAGE TIME TO IDENTIFY A BREACH

(Measured in Days; Source: IBM, 2024)

The old adage, "Time is Money," has never been more true than when speaking about the cost of cybersecurity. The longer the response time, the higher the costs due to the potential for more damage to occur. While the overall time to respond decreased from 2023 to 2024, with the mean time identifying a breach dropping to 258 days, some markets experienced an increase in response time year-over-year. Clearly, there needs to be mechanisms in place to be able to identify security breaches immediately when they occur, as well as the expectation that immediate intervention will be made to mitigate organizational – and perhaps community-wide – risk from these breaches.

Mean Time to Identify (MTTI) Mean Time to Contain (MTTC)



Mitigate financial impacts of cybercrime in your organization.
Request a cybersecurity assessment today.

Read More at:
qaconsultants.com/services/application-security

REQUEST NOW