



# FAMIS

Daryl Williams  
Rosa Alaia

June 11<sup>th</sup> 2024

# IBM - Latest Updates in Cyber Resilience and AI

Question - What do these two topics have in common??

# IBM - Latest Updates in Cyber Resilience and AI

Answer – Its All about the



DATA!!

# Group Exercise

- Current Cost of a Data Breach?
- Are you Resilient?

## EXERCISE GROUND RULES

Top two (2) thoughts – go with your gut  
1 Minute!

If table – combine into top three (3)  
2 Minutes!



---

<https://www.ibm.com/downloads/cas/E3G5JMBP>

# CHANGE HEALTHCARE CYBER ATTACK

- The hack of Change Healthcare reportedly affected [billing and care authorization portals](#). It's led to [prescription backlogs](#) and [missed revenue](#) for providers, posing potential threats to worker paychecks and even patient care.
- The attack also prompted high-level calls for action from the likes of [Senate Majority Leader Chuck Schumer](#) of New York and leading medical organizations. The American Medical Association called on the Department of Health and Human Services to “use all its available authorities to ensure that physician practices can continue to function, and patients can continue to receive the care that they need.”
- “This massive breach and its wide-ranging repercussions have hit physician practices across the country, risking patients’ access to their doctors and straining viability of medical practices themselves,” the AMA’s president, Dr. Jesse Ehrenfeld, said in a March 4 [statement](#). “This is an immense crisis demanding immediate attention.”

### Total cost of a data breach

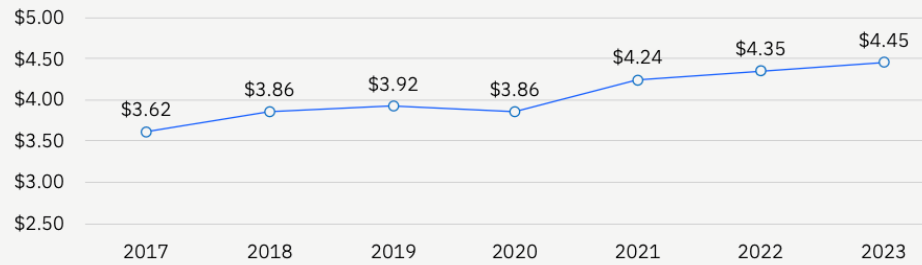
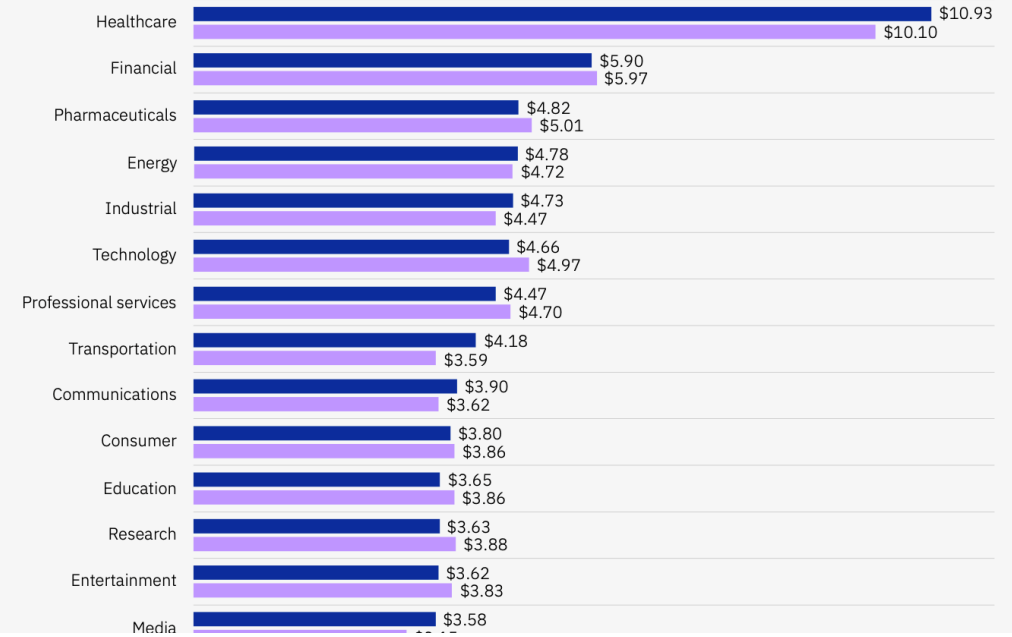


Figure 1. Measured in USD millions



# Today's Cost for Cyber Attack

# Malicious Attacks

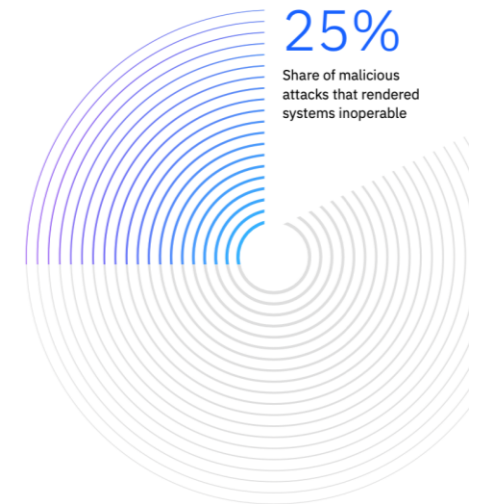
Malware — or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking, and any other type of malware attack that leverages software in a malicious way.

## Complete findings

### Ransomware and destructive attacks

This year, ransomware and destructive attacks<sup>3</sup> accounted for 24% and 25% of malicious attacks, respectively.

As in the 2022 report, we looked at the lifecycle of these types of breaches and the impact of paying a ransom compared to not paying a ransom. This study doesn't include the cost of the ransom in calculating the total cost of the breach. In the 2023 report, for the first time, we examined the influence of involving law enforcement in the effort to contain a ransomware attack.





EPA warning  
on Cyber  
attacks

USA TODAY TRUMP TRIAL Inside courtroom HISTORIC MOMENTS College protests NEWS TO YOUR INBOX Start the day smarter


U.S. Elections Sports Entertainment Life Money Tech Travel Opinion

# EPA urges water utilities to protect nation's drinking water amid heightened cyberattacks

**Thao Nguyen**  
USA TODAY

Published 12:04 a.m. ET May 21, 2024 | Updated 12:57 p.m. ET May 21, 2024

[f](#) [X](#) [✉](#) [➔](#)



and **change chemical levels** to dangerous amounts.

### EPA issues cyberattack warning for water utilities

The Environmental Protection Agency issued a nationwide alert urging water utilities to take immediate action to safeguard drinking water from cyberattacks. *Wibbitz - News*

# Types of Recovery and Resilience

**Cyber Security is not  
Cyber Resiliency**

Security – The Moat  
Pre-Attack

Resiliency – Time to Recover  
Post - Attack

PSPDFKit Cyber recovery is very different from Disaster recovery

Category	Disaster Recovery	Cyber Recovery
Recovery Point	Known Point in time	Not known...yet
Recovery Time	RPO/RTO	Trusted and Verified first
Nature of Disaster	Flood, power outage, weather	Targeted
Impact of Disaster	Regional	Global
Recovery	Failback	Based on situation
Data to Recover	Known	Unknown
Topology	Connected Data Centers	Isolated and away from production
Data Volume	Comprehensive, all data	Super selective
Probability	Low	High

# IBM - Cyber Resiliency Assessment

The Cyber Resiliency Assessment is a no-cost, two-hour virtual workshop with IBM security experts and storage architects. The analysis and recommendations are confidential, vendor neutral and non-invasive without the need to install anything or run scripts. We will work with your team to:

- Review data backup, protection, and restoration procedures,
- Identify safeguards to prevent becoming a cyberattack victim, and
- Understand critical business outcomes and connect them to targeted cyber resiliency strategies.

In the final report, you'll come away with:

- Detailed assessment report of findings,
  - Roadmap of recommended improvements and considerations, and
  - Management presentation, connecting practical methods to achieve your business outcomes.
-

# AI in Public Sector

- The expanding use of Artificial Intelligence (AI) in government is triggering numerous opportunities for governments worldwide. Traditional forms of service provision, policy-making, and enforcement can change rapidly with the introduction of AI-technologies in government practices and public-sector ecosystems. For example, governments can use AI-technologies to improve the quality of public services, to foster citizens' trust, and to increase efficiency and effectiveness in service delivery. AI may also be used by governments to generate more accurate forecasts and to simulate complex systems that allow experimentation with various policy options.
- At the same time, AI use in government creates challenges. While the use of AI in government may increase citizens' trust towards governments, it may also *reduce* citizens' trust in government and government decisions.

<https://www.sciencedirect.com/journal/government-information-quarterly>

# AI Group Exercise

- Top Uses of AI in Your Organization?
- What is your biggest concern about AI?

## EXERCISE GROUND RULES

Top two (2) thoughts – go with your gut  
1 Minute!

If table – combine into top three (3)  
2 Minutes!

# 10 Things Governments Should Know About Responsible AI

1. AI is Highly Relevant in Public Sector
  2. Government is a Data Billionaire
  3. Data Flows based on Trust
  4. Humans are at the Heart of Responsible AI
  5. Responsible AI has Five (5) Characteristics
  6. Trusted Data must be the Foundation
  7. Differentiate the Risks of Responsible AI
  8. Responsible AI requires AI Governance
  9. Tools embed Responsibility in AI
  10. Governments can build AI now
-

# The speed, scope, and scale of generative AI impact is unprecedented

Massive early adoption

80% of enterprises are working with or planning to leverage foundation models and adopt generative AI

Broad-reaching and deep impact

Generative AI could raise global GDP by 7% within 10 years

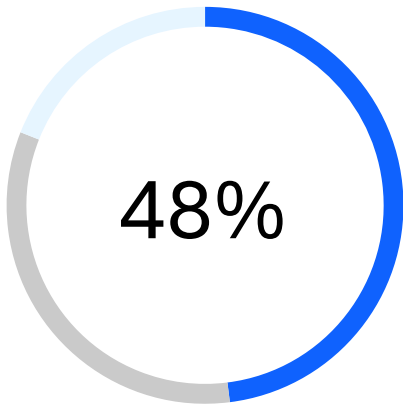
Critical focus of AI activity and investment

Generative AI expected to represent 30% of overall market by 2025

## Business leaders face challenges in scaling AI across the enterprise with trust

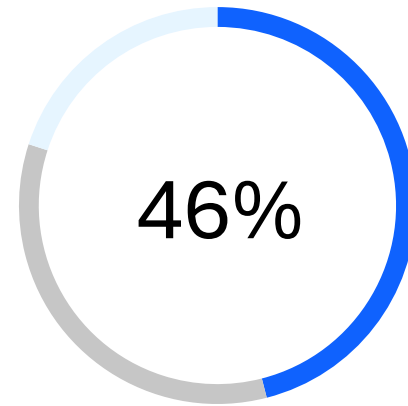
80% of surveyed business leaders see at least one of these ethical issues as a major concern<sup>1</sup>

### Explainability



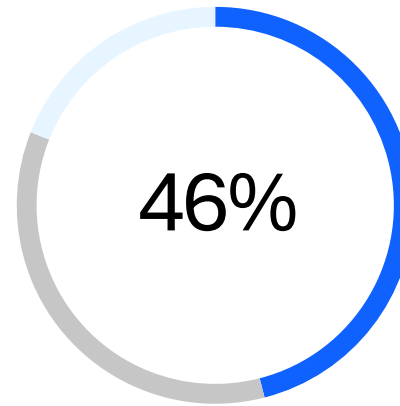
believe decisions made by generative AI are not sufficiently **explainable**

### Ethics



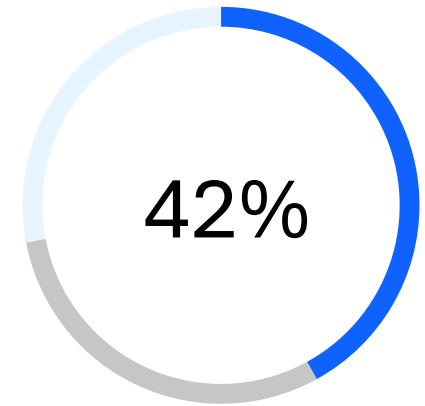
concerned about the safety and **ethical** aspects of generative AI

### Bias



believe that generative AI will propagate established **biases**

### Trust



believe generative AI cannot be **trusted**

Agree Neutral Disagree



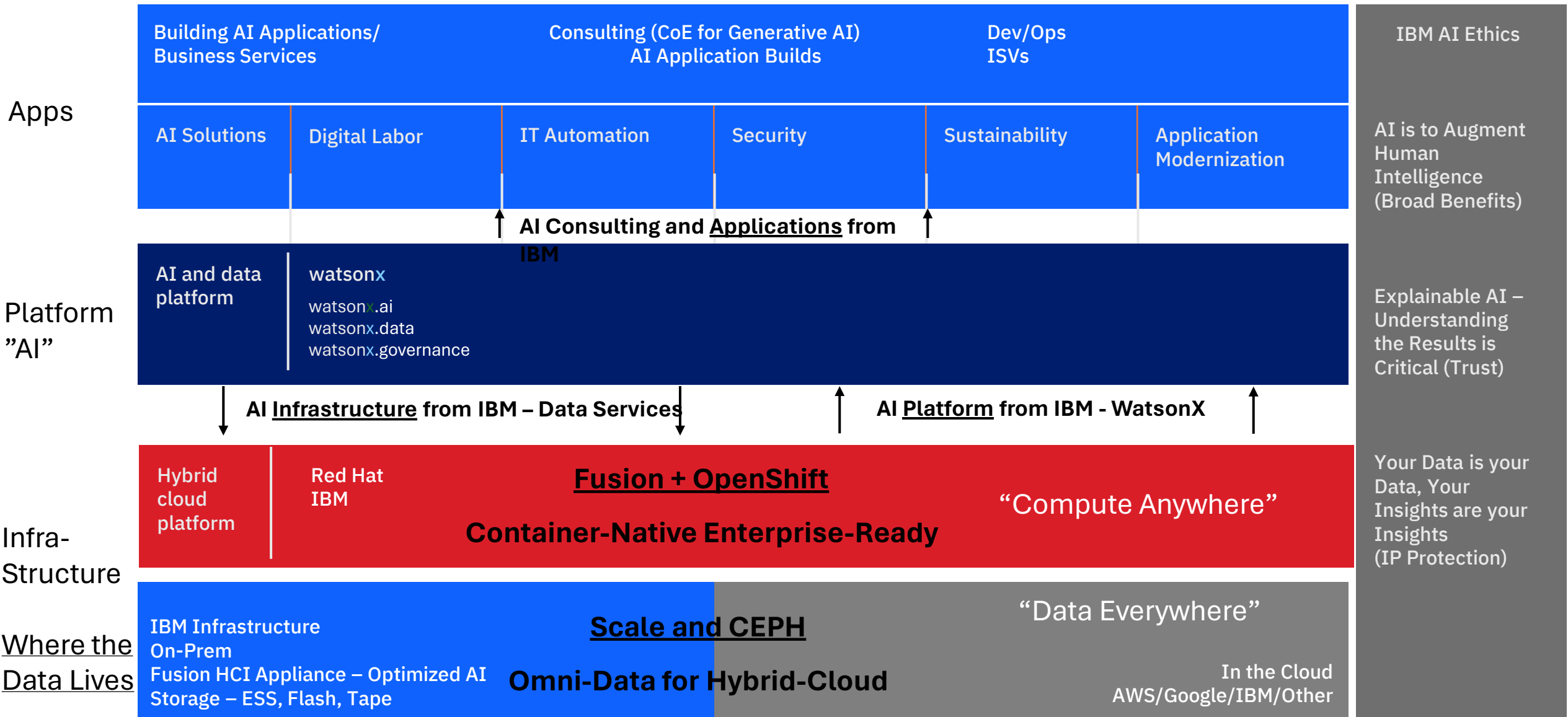


# IBM in AI World?



# Hybrid Cloud for AI

## AI Layers - Application, Platform, and Infrastructure – An End-to-End View



# AI ETHICS

## IBM AI Ethics

AI is to Augment  
Human  
Intelligence  
(Broad Benefits)

Explainable AI –  
Understanding  
the Results is  
Critical (Trust)

Your Data is your  
Data, Your  
Insights are your  
Insights  
(IP Protection)

Augment Human Intelligence

Understand the Results

IP and Data Rights Protection



Trust will become the Key AI Differentiator in Public Sector

# GOVERNANCE

## Bills on artificial intelligence filed in lead-up to Florida legislative session

*Legal and AI experts say it's a complicated area to regulate.*

Tallahassee Democrat

## Govern AI models anywhere

IBM® watsonx.governance™ was built to direct, manage and monitor the artificial intelligence (AI) activities of your organization by using IBM watsonx™, one integrated platform, which can be deployed on cloud or on-premises.

- Govern generative AI (gen AI) and machine learning (ML) models from any vendor including IBM® watsonx.ai™, Amazon Sagemaker and Bedrock, Google Vertex and Microsoft Azure.
- Evaluate and monitor for model health, accuracy, drift, bias and gen AI quality.
- Access powerful governance, risk and compliance capabilities featuring workflows with approvals, customizable dashboards, risk scorecards and reports.
- Use factsheet capabilities to collect and document model metadata automatically across the AI model lifecycle.

[Get the ebook: Build responsible AI workflows with AI governance →](#)

Report

IBM is named a leader in the IDC MarketScape: Worldwide AI Governance Platforms 2023.

[Read the excerpt →](#)

THINK 2024 Announcement

[IBM expands watsonx portfolio on AWS](#)



# Group Exercise Review

# Things to do Today

1

Resiliency  
Assessment – Know  
Where You Are

2

Data Infrastructure –  
Your Data is Your Gold  
– Use it; Protect it

3

AI – Learn, Leverage,  
Govern (Compliance)

IBM is Happy to Help

**THANK YOU**