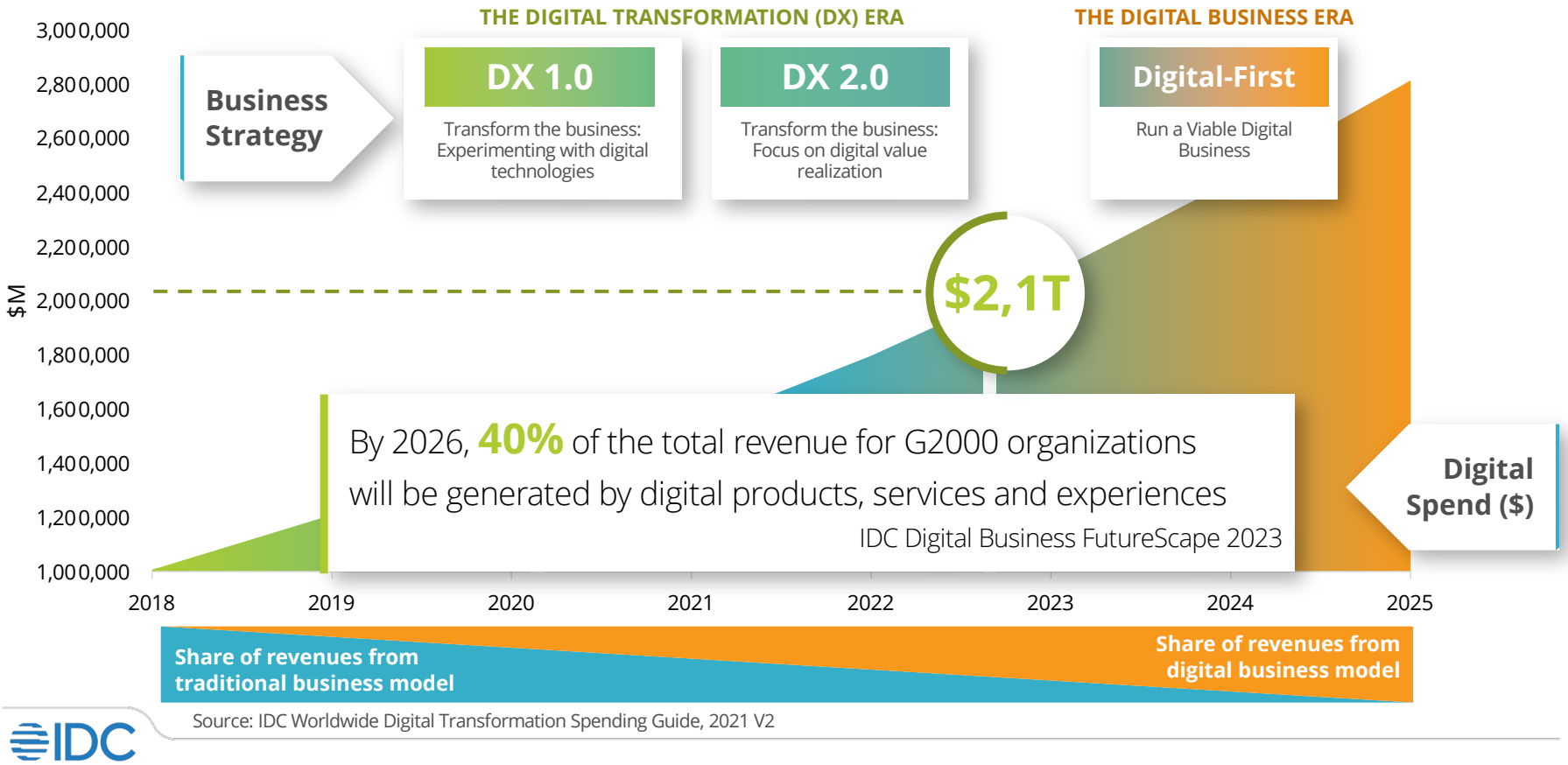
The Digital First CISO

Frank Dickson
Group Vice President, Security & Trust

IDC

What do we mean by Digital First Organizations?

The Shift to the Digital Business Era

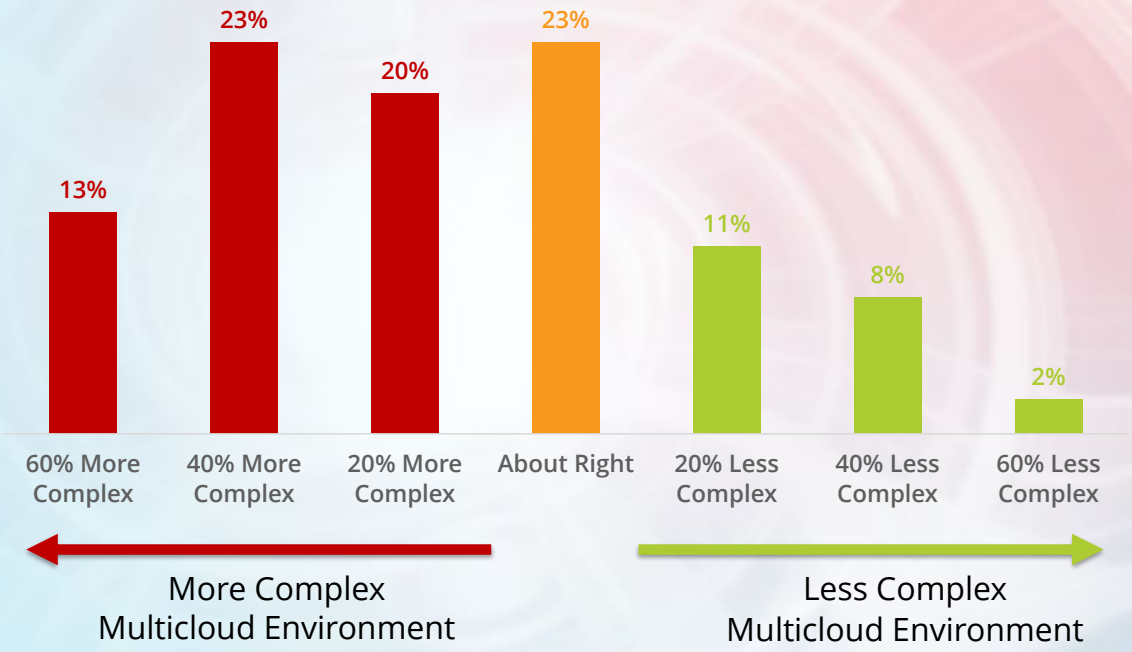


Source: IDC Worldwide Digital Transformation Spending Guide, 2021 V2

From [redacted] GEMENT

SCALE

56% of organizations have a more complex multicloud environment than expected



Source: Security ServicesView, February 2022 , IDC

Artificial Intelligence

Artificial intelligence comprises a grouping of machine-based technologies that perceive and synthesize data to infer information and insight to create systems that learn, reason, adapt, and self-correct.

Artificial Intelligence builds on itself

4

GENERATIVE AI

Learns from data and uses it to create artifacts that preserve a likeness to original data

3

PREDICTIVE AI

Analyzes existing data for prediction or automation, ie Blocking or Risk-based response

2

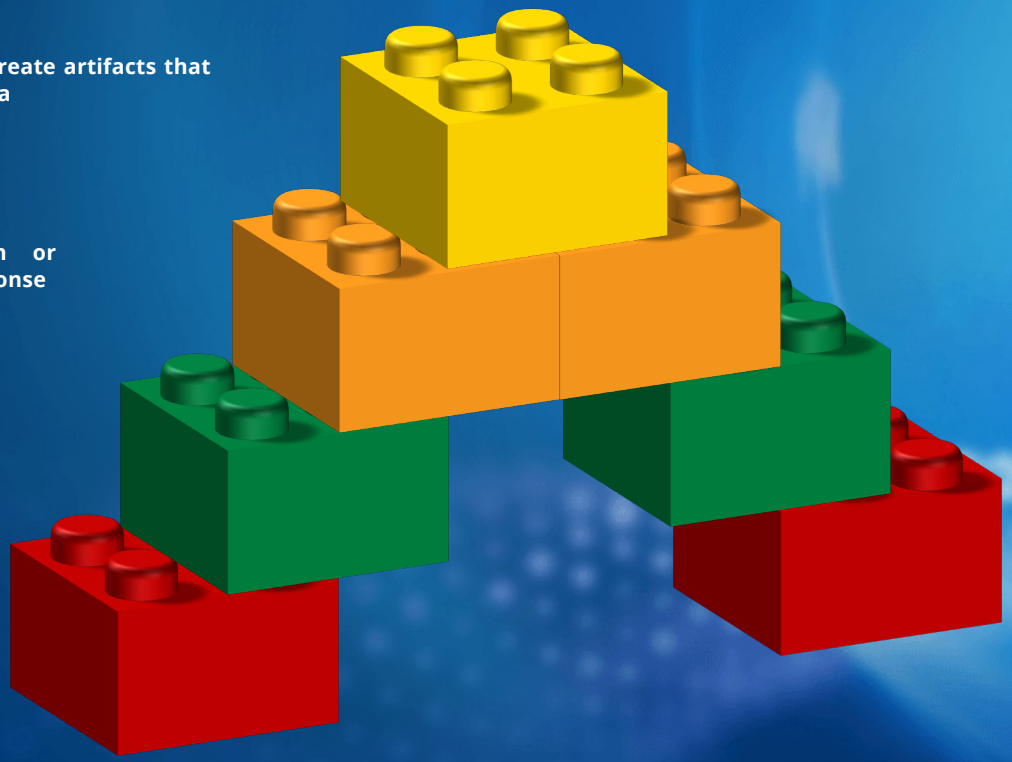
DEEP LEARNING

ML techniques that make computational multilayer neural networks feasible such as Convolutional neural networks

1

MACHINE LEARNING

Subset of AI techniques that enable computer systems to learn without programing by a human



IDC

GenAI: Almost 2 Years Later

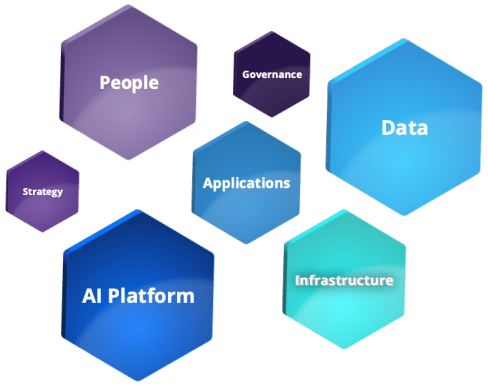
Source: Future Enterprise Resiliency & Spending Survey Wave 4, IDC, April, 2024. N.A. = 288

What Will it Take?

Experimentation
The GenAI Scramble

2023-2024

Adoption
The AI Pivot



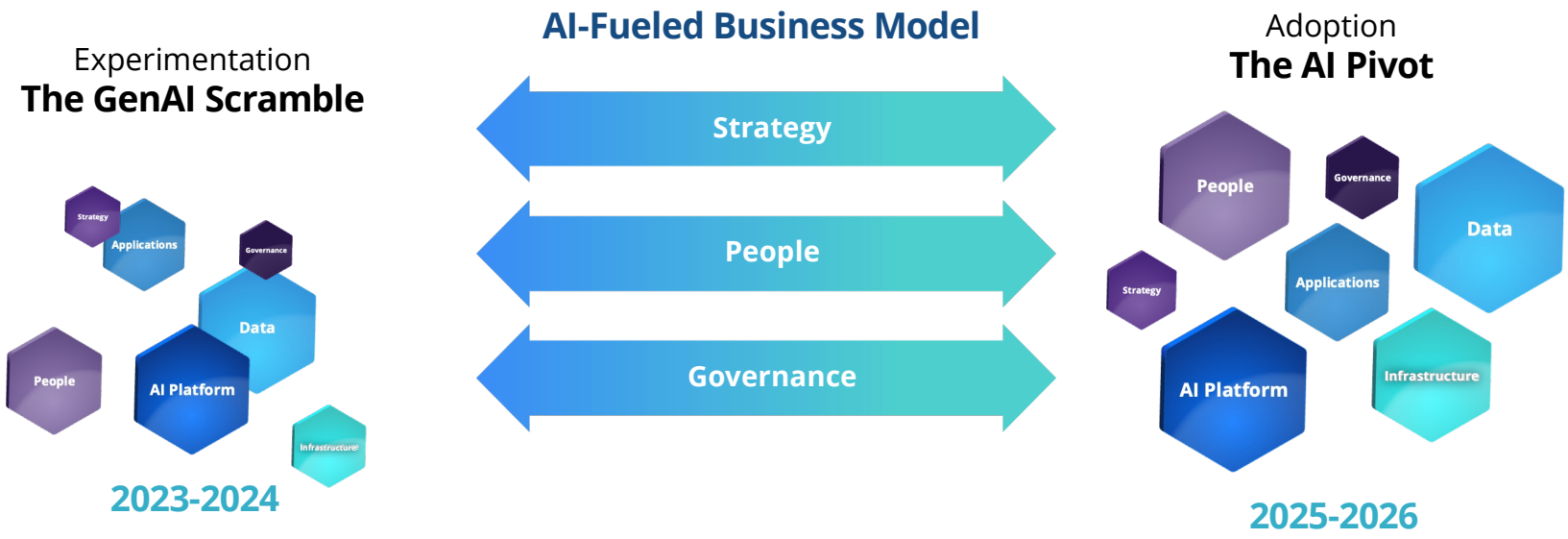
2025-2026

Acceleration
The AI-Fueled Business

2027+

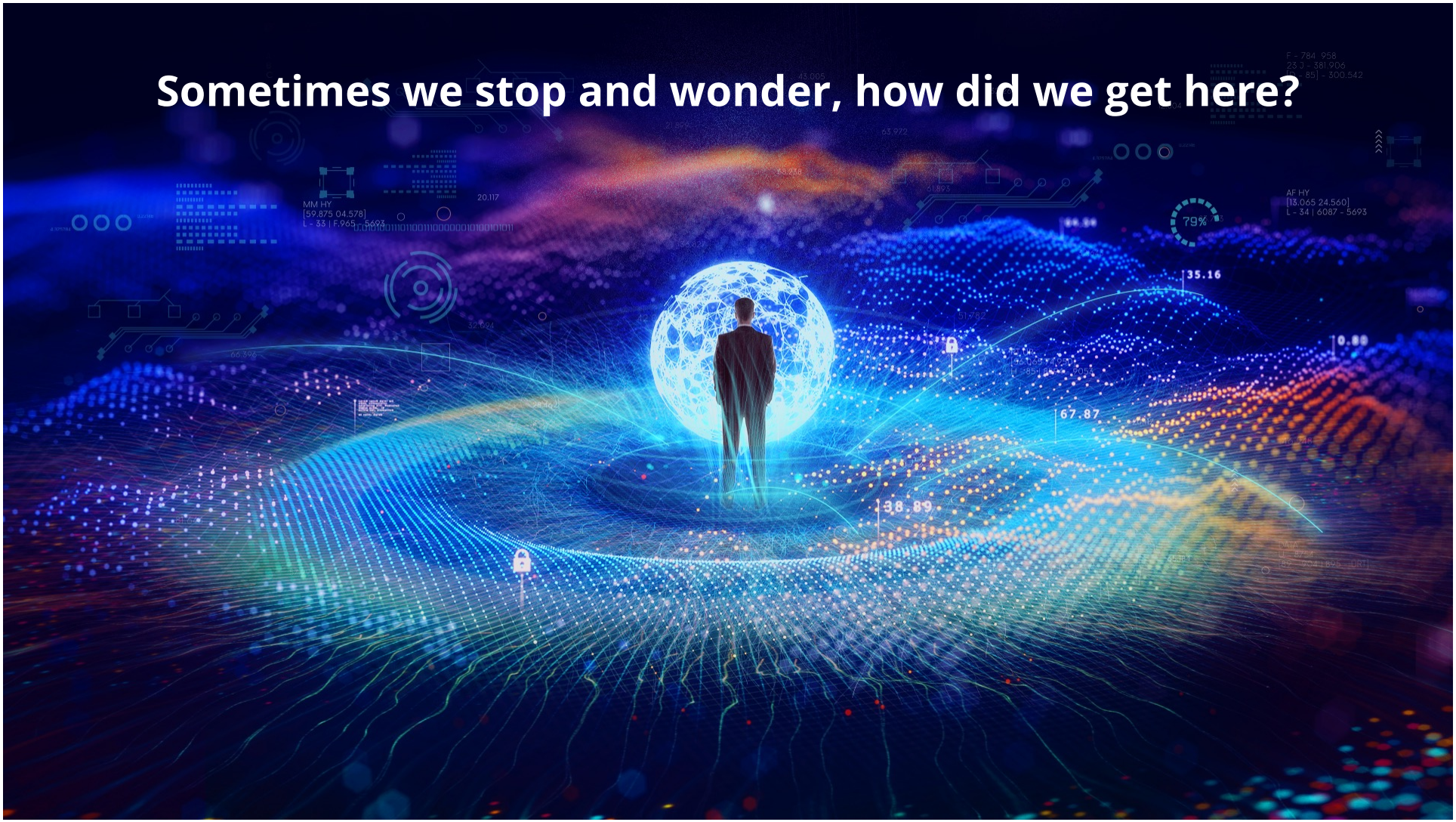
Source: IDC AI Adoption Model, 2024.

Business Model Blockers

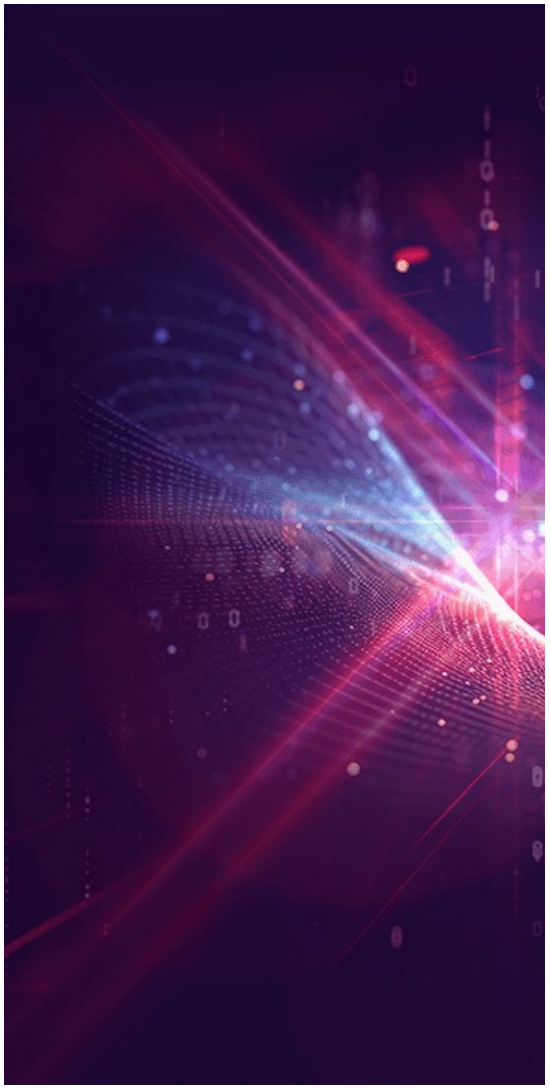


Source: IDC AI Adoption Model, 2024.

Sometimes we stop and wonder, how did we get here?



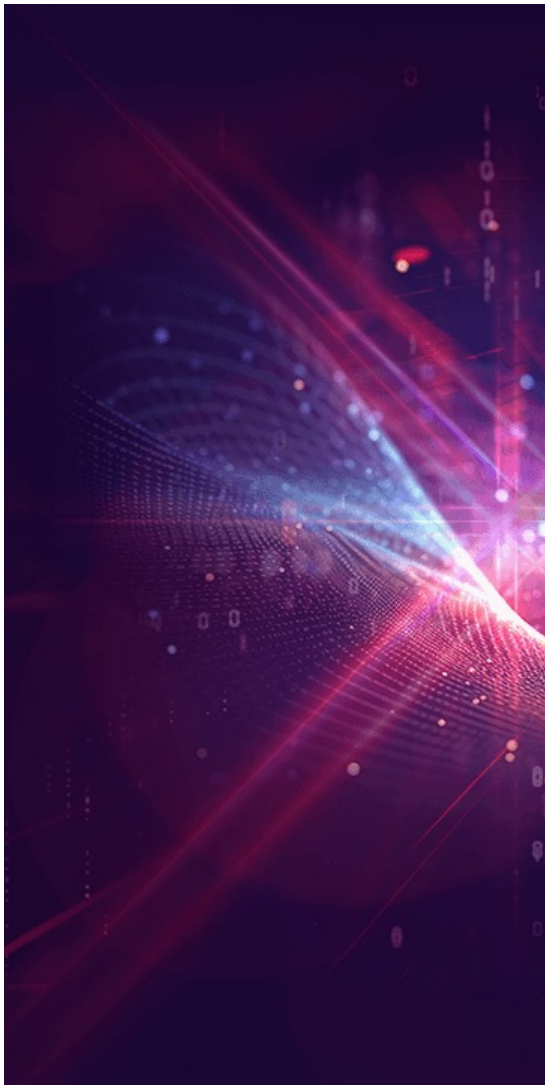
What are the 1st key implication of Digital First organizations on the CISO?



We evaluate CISOs based on cybersecurity prowess.

How important do you think is the role of the CISO in positively driving the results of the following business outcomes, technology priorities, and digital initiatives?

Source: CISO Thought Leadership Survey, IDC, November, 2023



We evaluate CISOs based on cybersecurity prowess.

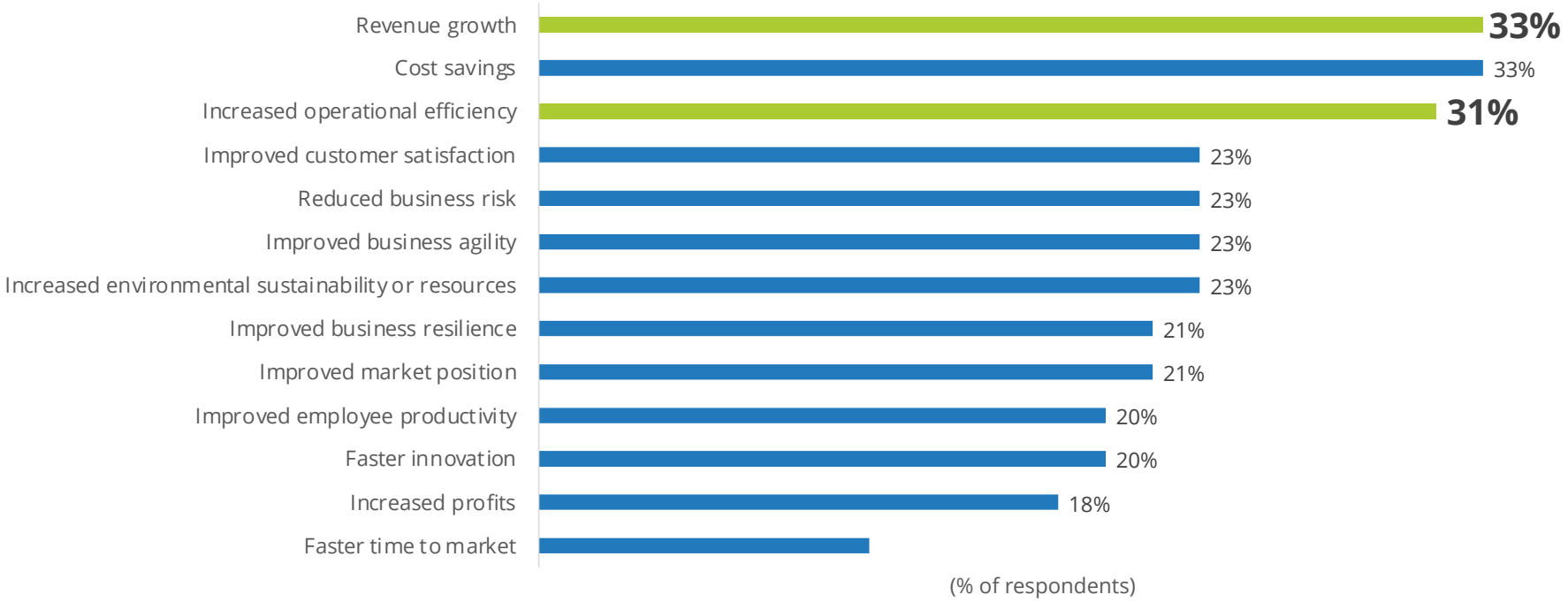
How important do you think is the role of the CISO in positively driving the results of the following business outcomes, technology priorities, and digital initiatives?

1. Investing in cybersecurity technologies
2. Improving IT support
3. Improving digital skills across the organization

Source: CISO Thought Leadership Survey, IDC, November, 2023

Revenue growth and increased operational efficiency are #1 and #3 in CISO business outcomes.

Please rank the three most important business outcomes that your organization (entire company) was trying to achieve from technology initiatives in the past 12 months.

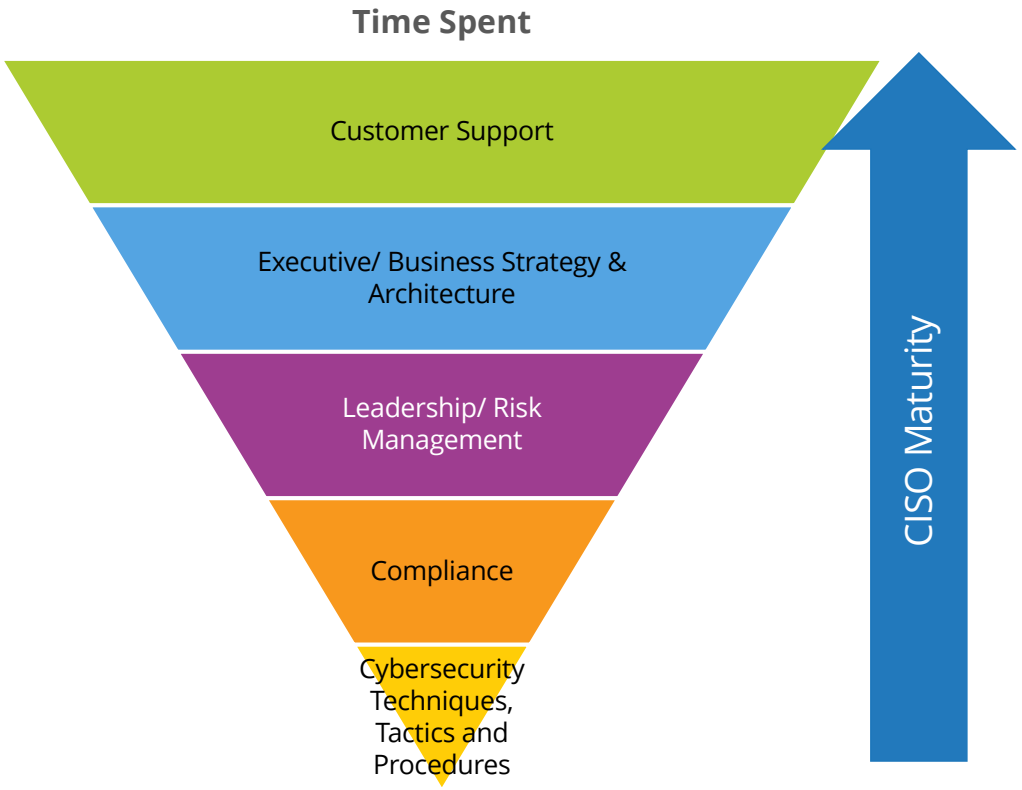


Source: CISO Thought Leadership Survey, IDC, November, 2023

Even with GenAI, revenue growth is the priority.

Over the next 3 to 5 years, what are the most important business outcomes the executive team within Security looking to achieve with Generative AI initiatives?

As a CISO matures in the role, the time spent on tasks changes.



Key Point: We evaluate CISOs based on cybersecurity prowess, but customer support demands much of their actual job.

How important do you think is the role of the CISO in positively driving the results of the following business outcomes, technology priorities, and digital initiatives?

Source: CISO Thought Leadership Survey, IDC, November, 2023

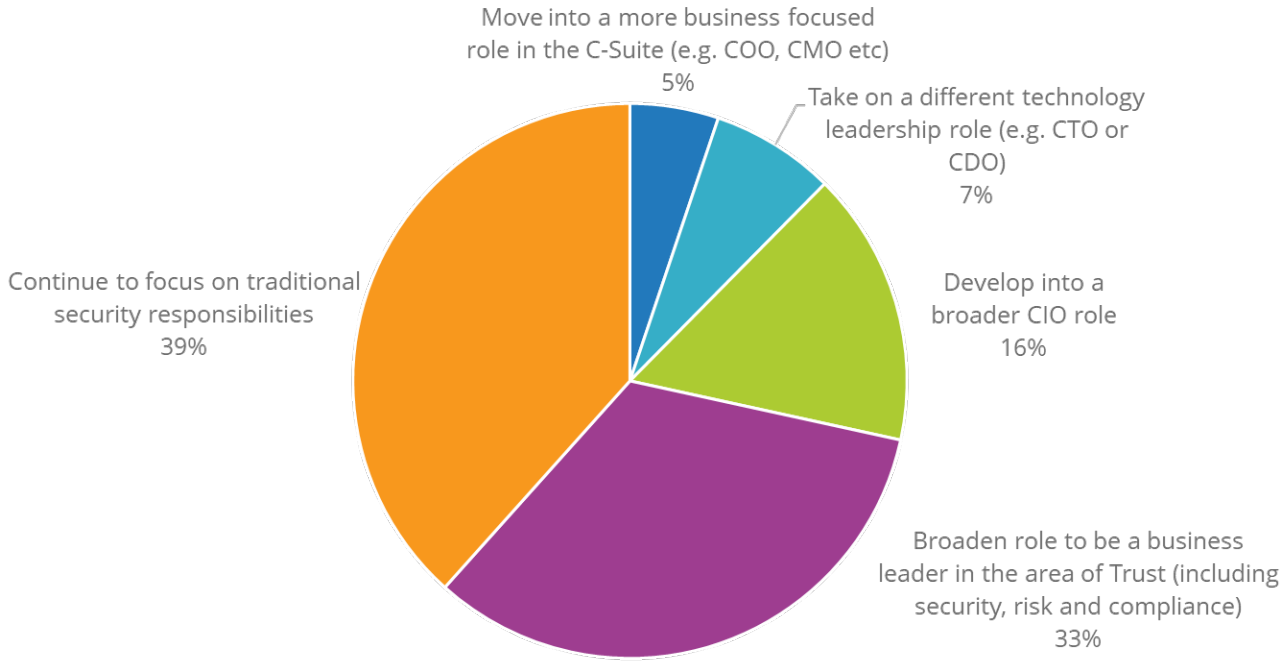
Topical Evolution of Skills Knowledge of a CISO

IDC Survey Spotlight

Does a CISO need to worry about the goals of the business or just focus on security?

Frank Dickson

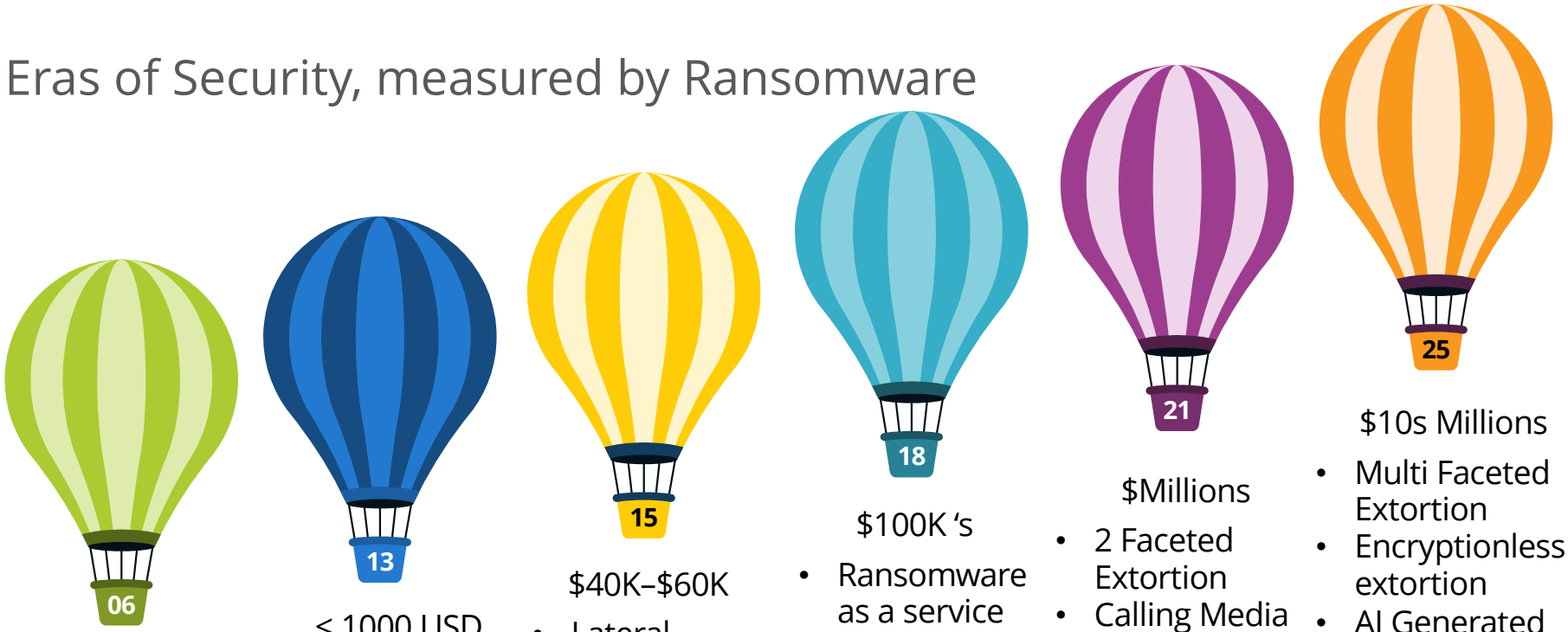
What is the most important way you see your role evolving over the next 12-24 months?



IDC #US51249523 (September 2023)
Source: WW C-Suite Tech Survey, IDC, August, 2023, n = 89

What are the 2nd key implication of Digital First organizations on the CISO?

Eras of Security, measured by Ransomware



$100–$200

660-bit RSA public key

< 1000 USD

- C&C
- Encryption
- Cryptocurrency

$40K–$60K

- Lateral movement
- Privilege escalation

$100K 's

- Ransomware as a service
- Evasion
- Backdoor
- Identity theft

$Millions

- 2 Faceted Extortion
- Calling Media
- Data theft
- Shaming

$10s Millions

- Multi Faceted Extortion
- Encryptionless extortion
- AI Generated Phish
- Deep fakes

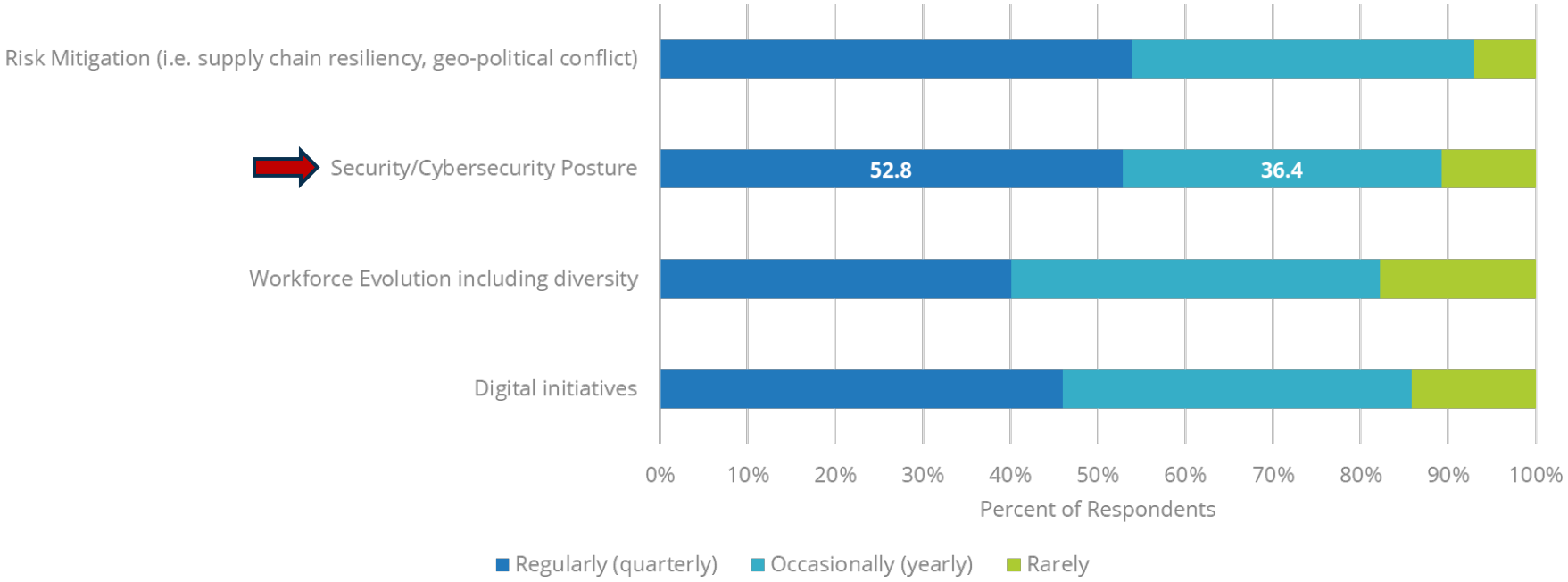
Do we need a CISO?

Should the CISO report to the CEO?

Should the CISO report to the Board?

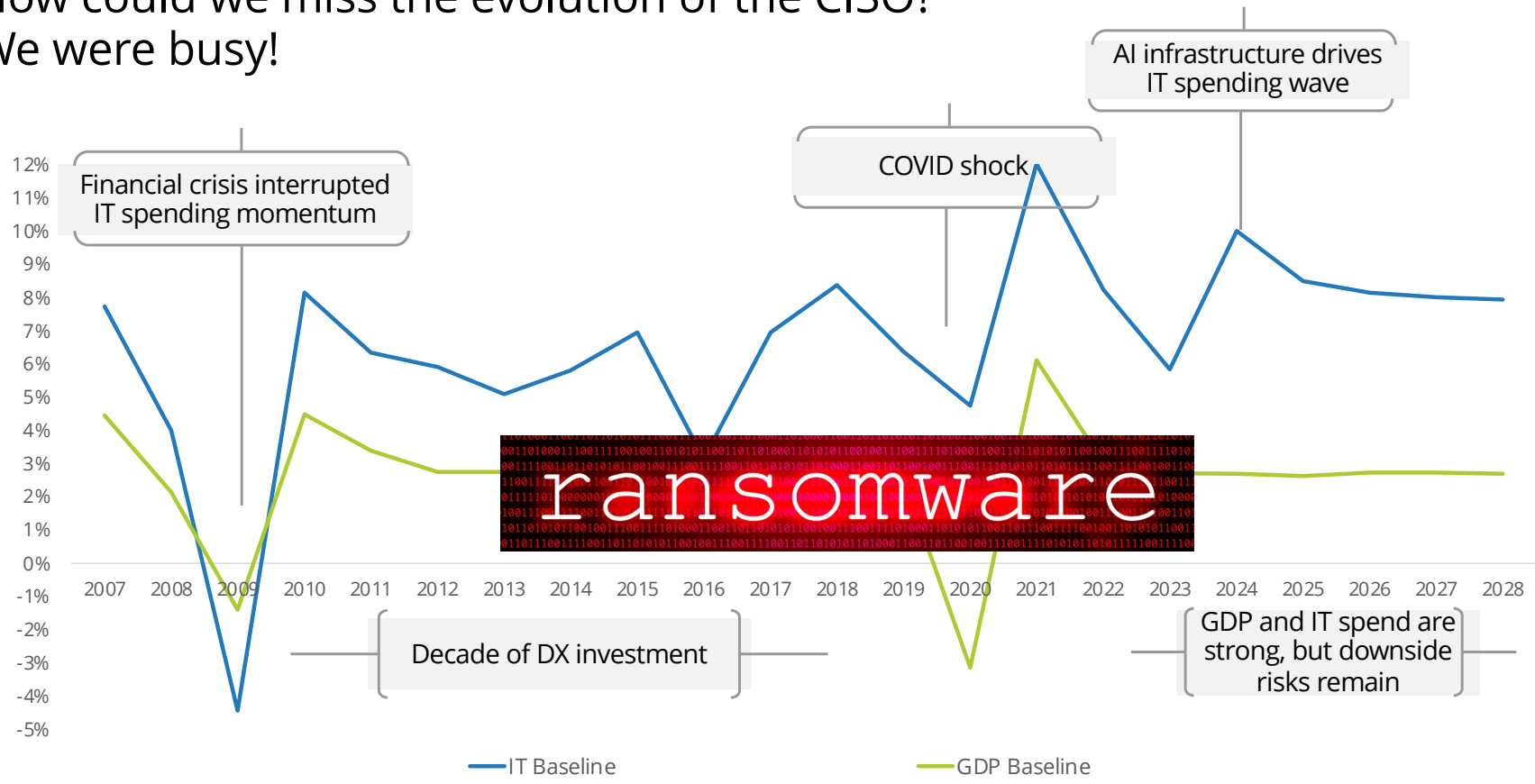
More than half of organizations report on cybersecurity posture to the board of directors at least quarterly; 89% report at least annually.

Beyond financial results, how often are you required to present on the following topics to the board?



IDC # US52306324 (May 2024)
Source: IDC Worldwide CEO Survey, February 2024, n = 354

How could we miss the evolution of the CISO? We were busy!



Source: IDC Worldwide Black Book (September 2024) growth in constant currency; excludes telecom spending and business services

Cybersecurity Metrics Need to be Appropriate for the Audience. Don't deliver the wrong metrics to the board.

BOARD OF DIRECTORS

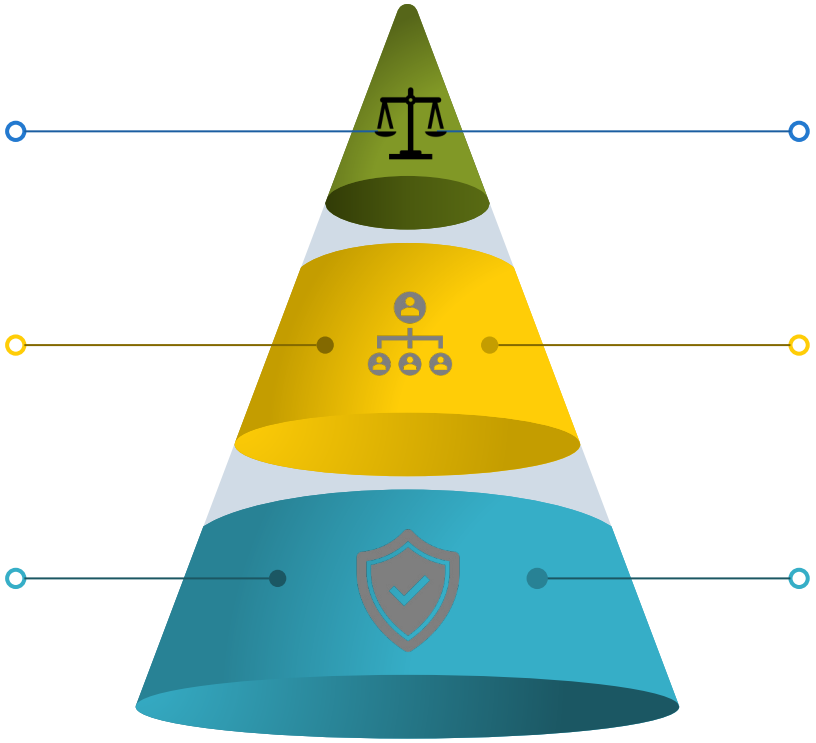
Looking to translate cyber risk into business risk

CEO & C-SUITE

Executing on the strategic objectives for the organization

CISO & CYBER LEADS

Tactical technical details of the day-to-day operations of cybersecurity throughout the organization
Efficiency often trumps effectivness



GOVERNANCE

- Overview of effectiveness
- Risks Affecting the Organization
- Overall Risk & Compliance Scores
- Trends

MANAGERIAL

- Overall Risk & Compliance Scores
- Incident Management
- Cost of Incidents
- General Program Metrics

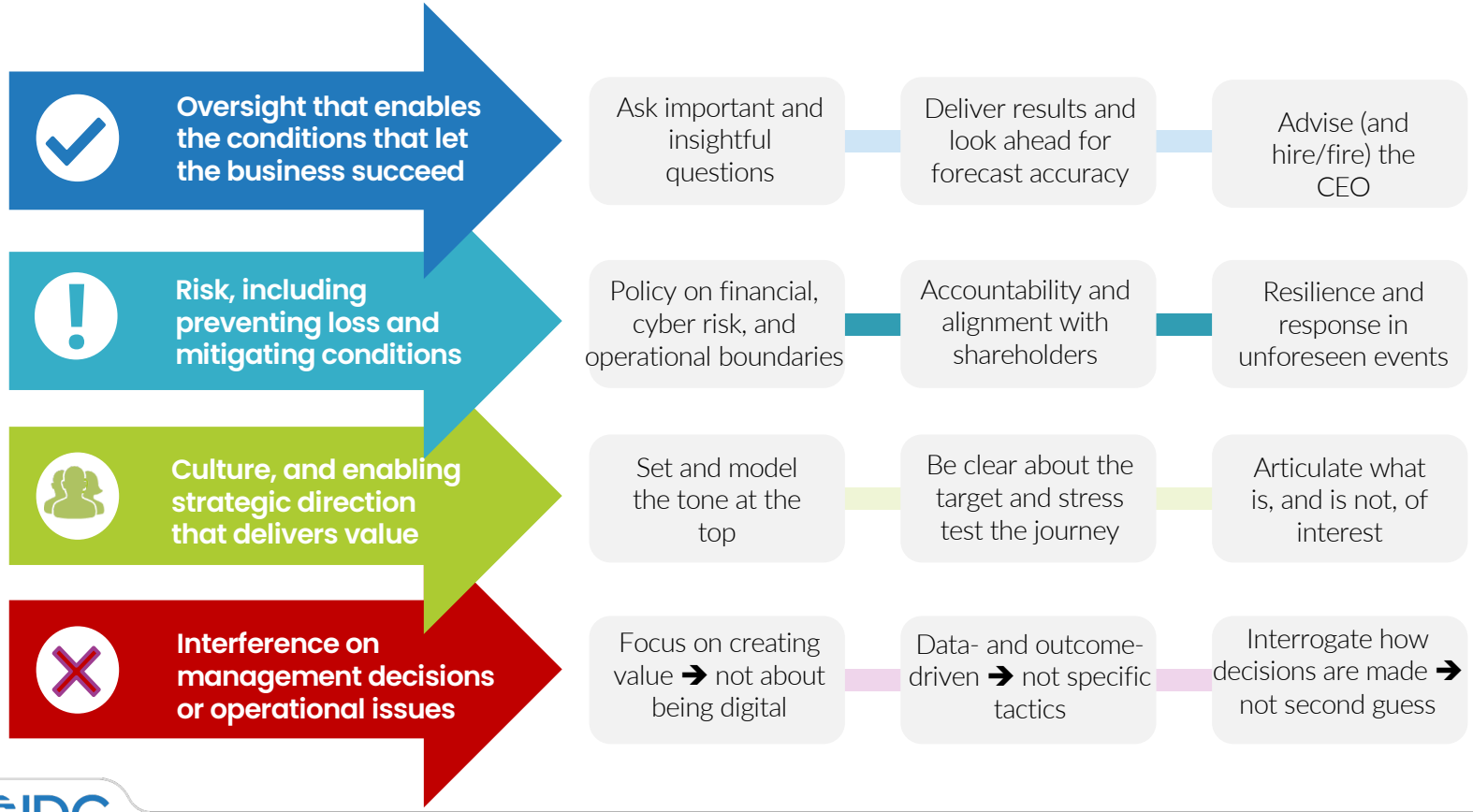
OPERATIONAL

- Governance (Policies, Metrics, Reporting, Education, TPRM, Projects)
- Risk Management
- Compliance Management
- Identity & Access Management
- Servers, Endpoints & Mobile
- Network
- Security Operations Center (SOC)
- Incident Management

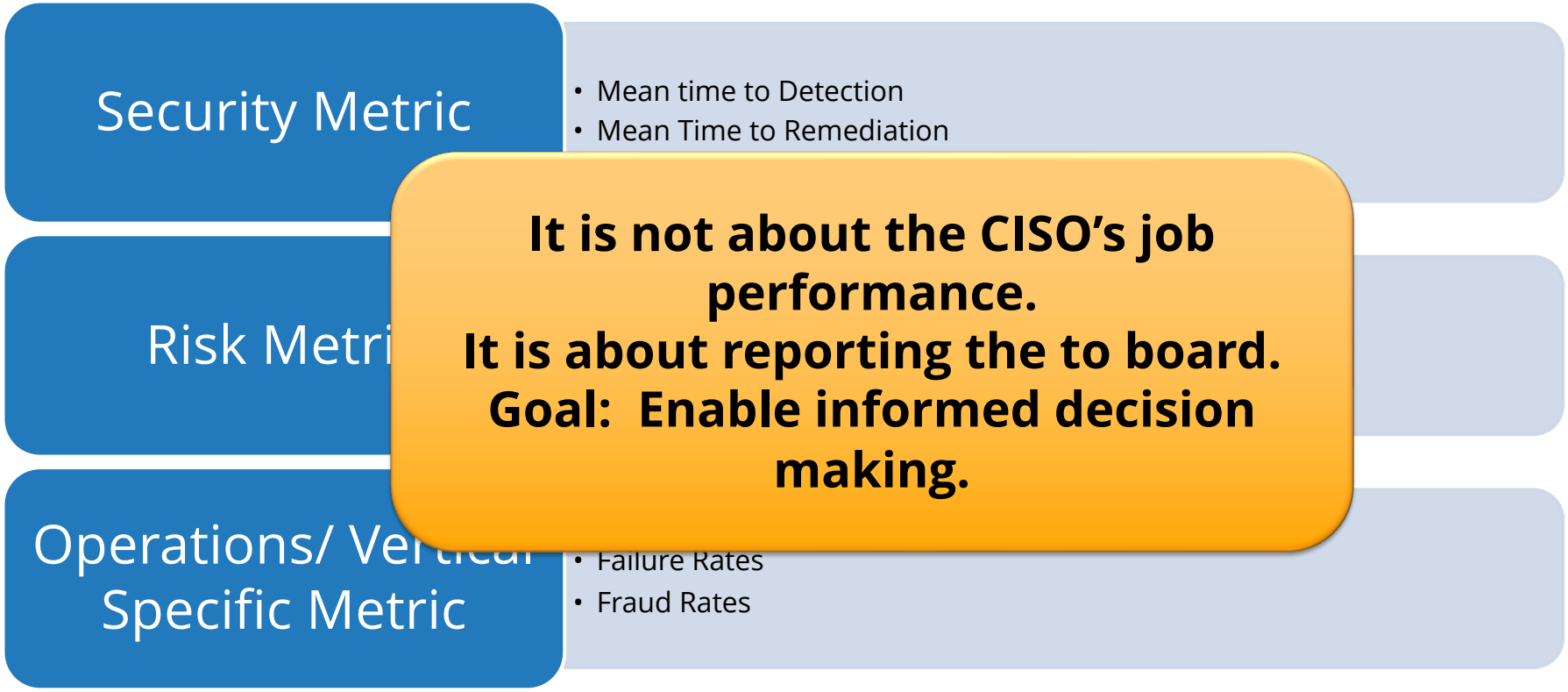
IDC

Board Scope

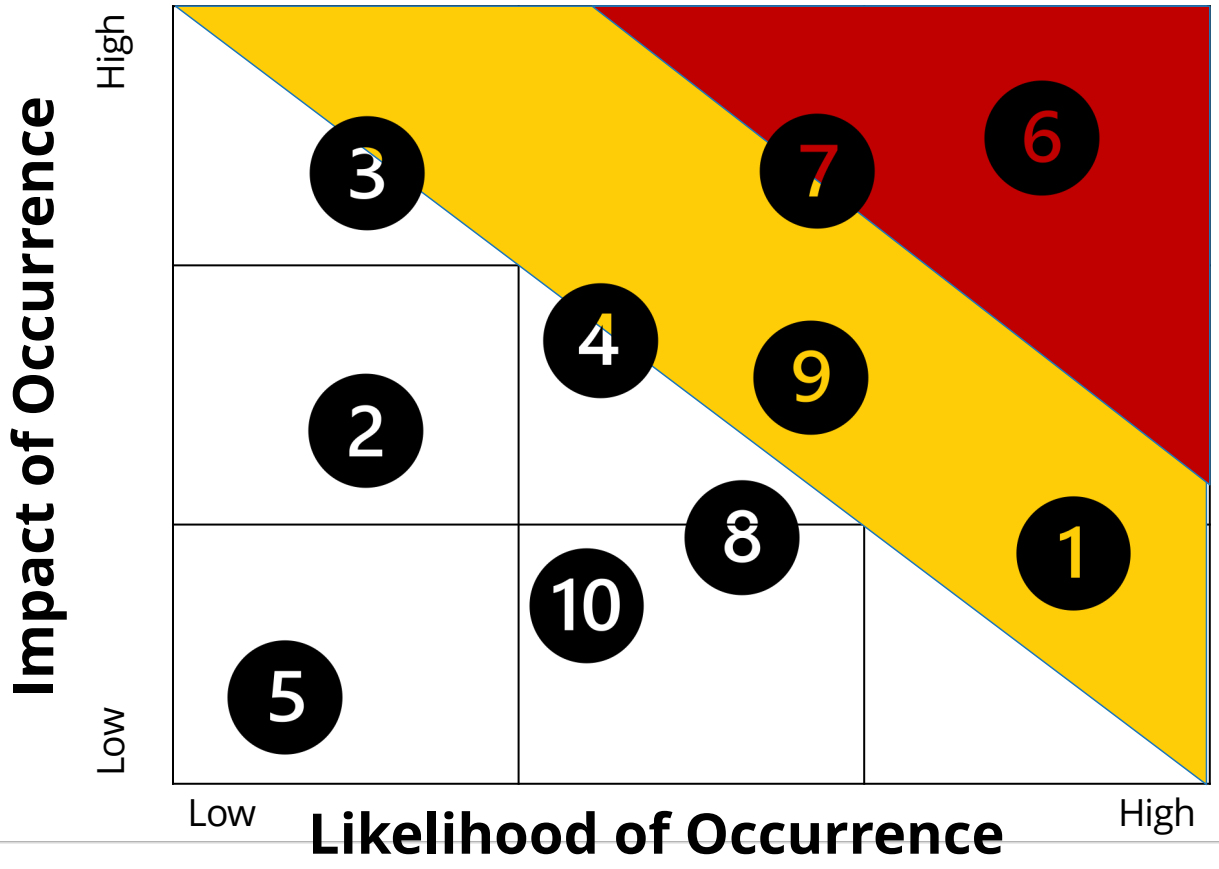
Understand what the board cares about



Choose 6 to 10 metrics critical to your organization across 3 categories.



Boards Care about Business Risk; Be Careful with Colors.



Source: Building Leverage in Board-Level Digital Strategy Conversations #US49689022

Boards Don't 'Do,' They 'Direct'; Help Them Help You

The board has a duty-of-care obligation to ensure proper cybersecurity governance

- Answer the questions that they should be asking

The board's role is to ensure that risk is managed in accordance with its approved risk appetite

- Focus on avoiding surprises and opportunities for mitigation

The board's primary strategic tool is in policy and procedures defined to manage cyber-risk

- Help them identify gaps and opportunities to improve the "tone at the top"

Focus on the questions the board needs to ask "management"

- Respect the roles of the CEO and "management"
- Guide board inquiries to management through honest focus on continuous improvement

Career advise: Tell the CEO what he/she should know BEFORE the board meeting.

What do Boards ask about their CISO and Cybersecurity?

Shamelessly Plagiarized from Kevin Mandia, mWise 2024 Keynote

1. How good are we? How secure are we? What are the odds something bad happens?
2. How good at cybersecurity do we need to be? What are the benchmarks that we need to be above?
3. What should boards worry about?
4. What are the best practices to supervise the work?
5. How do we know that the company is doing all that is possible?
6. What are the questions we the board should ask to the CISO? (how good is the CISO?) The CISO needs a security mindset. Questions need to evaluate that mindset.
7. What do CEOs wish they did before a breach?
8. How does AI impact us from a risk perspective? How should we be thinking about AI?
9. Latest headline questions
10. Other: Supply chain, threats, geopolitical conditions, deep fakes
11. What are other boards asking you?

For Additional Information

Frank Dickson
fdickson@idc.com
https://www.linkedin.com/in/frankdickson/
@fdickson777

 IDC.com

 linkedin.com/company/idc

 twitter.com/idc

 blogs.idc.com