ET *CISO Intelligence*

Beyond the *Breach*

India's Cyber, AI & Governance Benchmark 2026

Foreword

"Is it AI for security or security for AI?"

The world today is shaped by data, the new battlefield. Cyber elements now permeate every dimension of our existence. AI for Security and Security for AI are distinct but interconnected: the first strengthens protection technologies, from vulnerability assessment and XDR to SIEM, threat hunting, and fraud detection; the second keeps AI itself trustworthy, safe, and responsibly governed, with models protected, usage monitored, and governance frameworks embedded.

The ETCISO Intelligence Report reveals how deeply this challenge cuts: supply chain and vendor attack vectors remain a top adversary tactic in manufacturing, cited by over 32% of organisations, while data privacy and compliance tools have emerged as long-term budget priorities alongside cloud security, Zero Trust, and IAM. As India's digital economy surges, projected to contribute 20% of GDP by 2026, defending this growth will demand resilient strategies, sharper governance, and the courage to evolve faster than the adversary.

Table of contents

04 Executive Summary

06 Introduction

12 Industry snapshot

16 Chapter 1
Where AI already delivers value

26 Chapter 2
Governance and the CISO's mandate

34 Chapter 3
DPDP: confident, not evidenced

40 Chapter 4
The post-quantum clock

44 Chapter 5
The workforce dividend

49 What Cybersecurity Leaders
Should Do Next

51 Appendix 1
About the research

52 Appendix 2
About ETCISO Intelligence

Executive summary

India's AI adoption has outpaced the governance built to control it. Most organisations run AI in only 10–25% of security operations, and just over a quarter can show a meaningful cut in response time.

Frontrunners, 16% of the sample, use AI across the largest share of security operations and get sharper results. Governance shows the same gap: 78% of cybersecurity leaders lead or co-own AI governance, but only 21% keep most AI under formal control.

DPDP confidence sits at 71%, but mapping trails at 45%. Data leakage remains the top AI risk at 67%. AI-driven automation is changing where security work is concentrated.

At a glance

44% plan to raise AI security spend by more than a quarter next year, led by BFSI (47%) and IT/ITES (46%).

74% of Manufacturing respondents run AI-based threat detection in at least a quarter of their security operations, yet reports the lowest security budget intent of any sector.

67% name data leakage as their top AI security concern, ahead of shadow AI (50%) and third-party AI risk (46%).

78% of CISOs own AI governance, but only 21% govern most of their AI estate.

71% are confident in DPDP readiness, but only 45% have mapped more than half of their personal data.

92% have no dedicated post-quantum budget line, even though half expect board attention within 12 months.



Adoption is ahead of control

16%

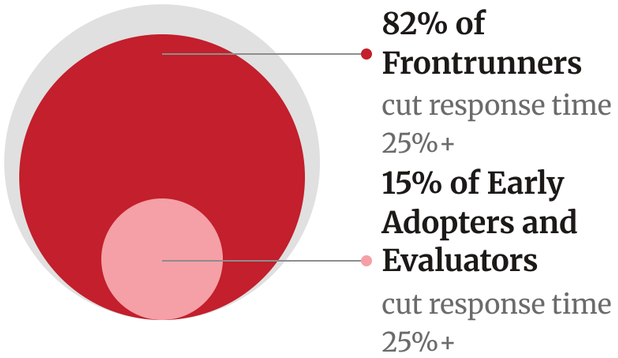
of organisations are AI Security Frontrunners, running AI across most of their security operations

AI use has expanded beyond pilots in Indian security operations, but governance has not kept up. Most organisations still cannot say how much of their AI estate sits under formal security control.

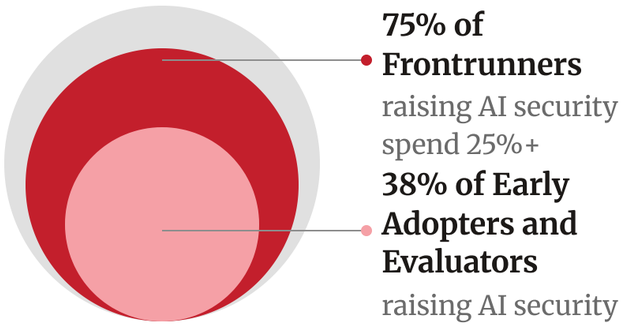
Over 200 senior security leaders across India took part. 45% run AI in more than a quarter of security operations; 16% past half.

We call that leading group **AI Security Frontrunners**. Everyone else, 84% of the sample, are **Early Adopters and Evaluators**. The widest gap between the two: how fast they close an incident.

Organisations reporting a greater than **25% reduction** in average incident response time.



Organisations increasing AI security investment by more than **25%** over the next 12 months



Beyond the Breach measures what Indian security teams have put into production, and where the rest are still deciding.

Data leakage is the most frequently cited AI risk (67%), ahead of shadow AI (50%) and third-party AI risk (46%). Model poisoning ranks last at 21%.

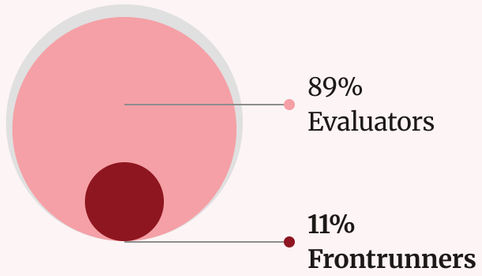
Governance coverage is thin: only 21% keep most AI applications under formal control.

Post-quantum cryptography shows the clearest gap between expectation and action: 50% expect board attention within 12 months, while 20% haven't started an assessment.

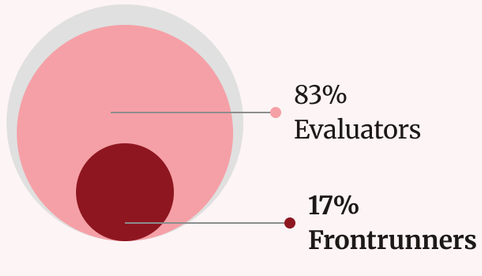
Frontrunners and Evaluators by city

We split the over 200 respondents into two groups by AI use: **Frontrunners** (more than half their operations, 16% of the sample) and **Evaluators** (everyone else). The charts below show that split by city and industry.

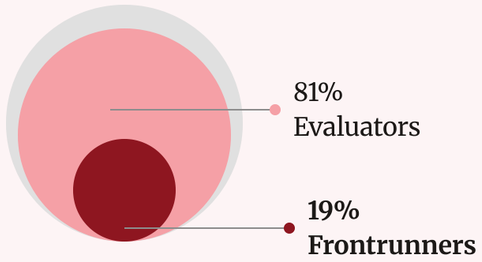
Mumbai



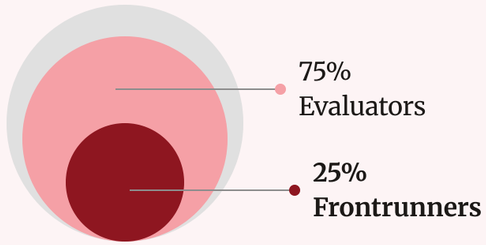
Bengaluru



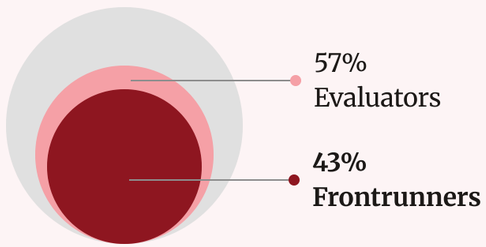
Delhi NCR



Pune



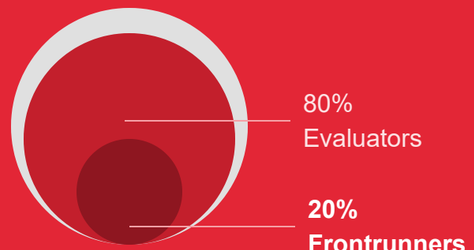
Hyderabad



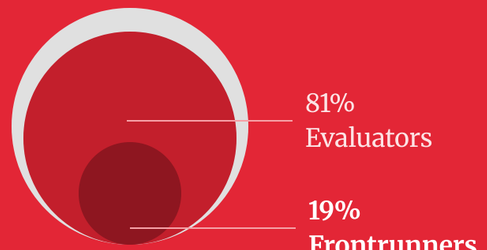
Frontrunners and Evaluators by industry

Outer ring: Evaluators. Inner disc: Frontrunners, by industry.

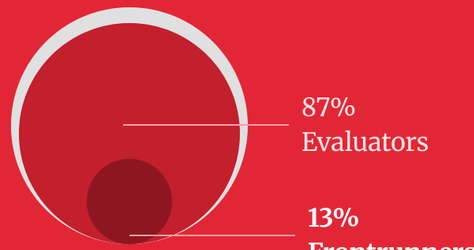
BFSI



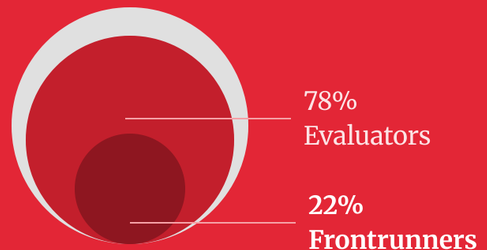
Manufacturing & Industrial



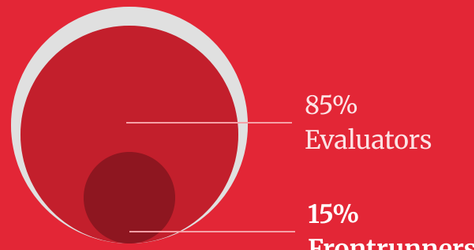
IT / ITES



Healthcare & Pharma (small base)

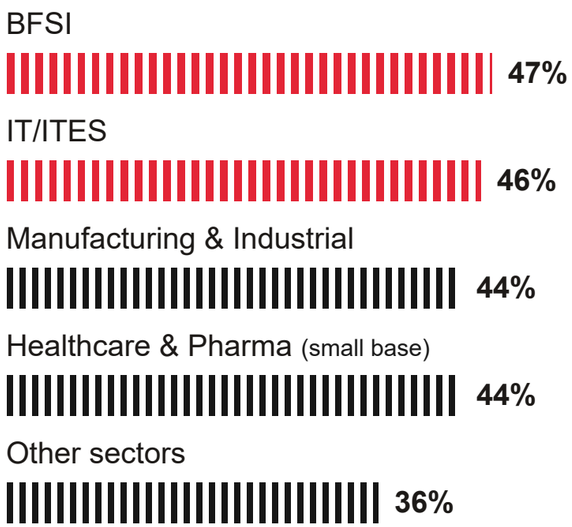


Other sectors



Industry snapshot

Planned AI security spend increase above 25%, by industry



25% plan to increase budget by more than 50%, evenly spread across BFSI, IT/ITES and Manufacturing, versus 13% in Other sectors.

What CISOs should do, by sector

BFSI

Highest DPDP confidence (33%) and Frontrunner rate, and the largest planned spend increase (47%). Validate coverage against evidence, not confidence.

IT/ITES

Lowest Frontrunner rate despite the broadest generative AI use and the second-largest spend increase (46%). Close the governance gap before expanding GenAI access.

Manufacturing & Industrial

Weakest governance and data mapping, despite market-rate spend plans. Fund governance to match committed investment.

Healthcare & Pharma

Sample too small for a reliable Frontrunner comparison, but the lowest DPDP confidence (11%) needs attention.

Other sectors (telecom, travel, FMCG, government)

Smallest planned spend increase, but fastest reskilling and strongest governance. Budget, not intent, is the constraint.

AI value varies by industry, with **threat detection** among the highest-ranked functions across most sectors.

Top 3 AI functions by industry

Industry	Top 3 functions
BFSI	Threat detection (60%), Vulnerability Mgmt (53%), SOC automation (49%)
Manufacturing & Industrial	Threat detection (59%), SOC automation (59%), Email Security (50%)
IT/ITES	Threat detection (56%), Vulnerability Mgmt (54%), Incident response (40%)
Healthcare & Pharma	SOC automation (78%), Identity & Access Mgmt (56%), Threat detection (56%)
Other sectors	Threat detection (62%), SOC automation (53%), Email Security (49%)

† See methodology, Appendix 2: industry bases are small.



47% of BFSI respondents plan to raise AI security spend by more than a quarter next year, the highest of any sector. For BFSI, threat detection is the most frequently cited high-value AI function.



01

CHAPTER 01

Where AI already delivers value

58%

name threat detection as their highest-value AI use case

Most security teams run AI across 10–50% of their operations. Three functions account for most of the reported value: threat detection, vulnerability management and SOC automation.

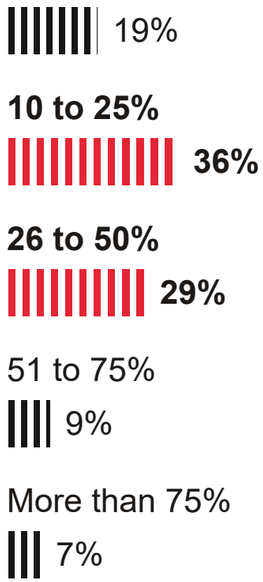
Adoption clusters in the middle. 36% of organisations run AI in 10–25% of security operations and 29% in 26–50%. Only 7% are past three-quarters.

Measured return is still the exception. 26% report cutting incident response time by more than a quarter; 13% report no measurable improvement at all.

Partial by design: where security teams have put AI into production

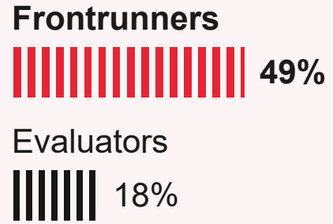
Most organisations sit in the middle bands: meaningful adoption, not yet full coverage.

% of organisations, grouped by how much of their security operations run on AI

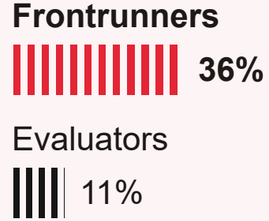


Frontrunners also govern better. They are nearly 3x as likely to have strong governance coverage, and more than 3x as likely to have a fully implemented AI governance framework.

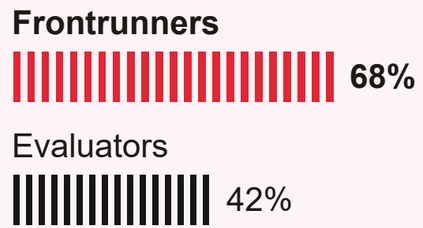
Organisations with strong governance coverage across their AI estate (above 60%)



Organisations with a fully implemented AI governance framework

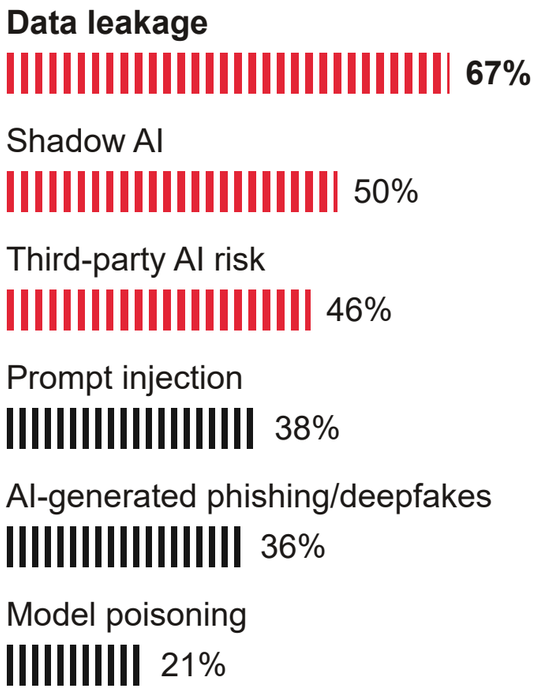


Organisations where AI now covers more than 25% of security automation



Shadow AI now ranks as the second-highest AI security risk, ahead of third-party AI risk.

AI security risks, share of all respondents



Threat detection is the highest-value AI function (58%), then SOC automation (51%) and vulnerability management (47%). Frontrunners' one difference: threat intelligence makes their top three.

> "Managing modern AI risk requires balancing rapid innovation with strict vigilance guarding against data leaks, curbing unsanctioned Shadow AI, and defending against emerging model attacks."

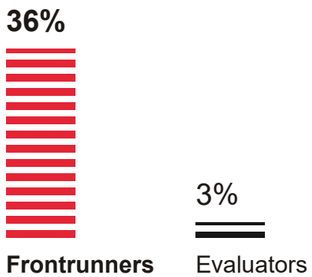


Nageshwaran C
CISO
TVS Holdings

Highest measurable value from AI, by function

Function	All respondents
Threat detection	58%
SOC automation	51%
Vulnerability management	47%
Email security	41%
Threat intelligence	37%
Security analytics	33%

Organisations reporting a greater than 50% reduction in response time



Organisations reporting no measurable improvement from AI



Where the budget is moving

44%

of organisations plan to raise AI security spend by more than a quarter over the next year, led by BFSI (47%) and IT/ITES (46%)

1

AI coverage remains partial across most organisations. Most teams run AI across 10–50% of operations, planning for it to carry part of the load, not all of it.

2

Value concentrates in three functions: threat detection, vulnerability management and SOC automation. Everything else trails by ten points or more.

3

The top risks, data leakage, shadow AI and third-party AI, come from using AI, not attacking it.

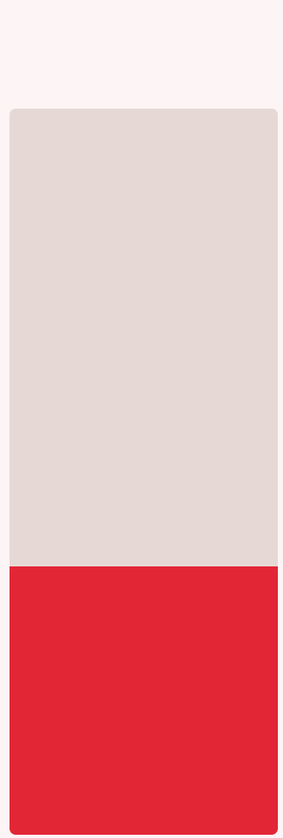
What CISOs should do: set a baseline before approving AI pilots. Fund threat detection, SOC automation and vulnerability management first, and measure response time before and after rollout. Frontrunners were 5.5x as likely as Evaluators to report a >25% reduction in incident response time.

Threat detection and vulnerability management draws the largest single share of planned AI security spend in every sector except Healthcare & Pharma, where it splits evenly with SOC automation.

Top AI-security investment priorities by industry

Industry	Top budget lines
BFSI	Threat detection & vuln. mgmt. (37%), Identity security (18%), SOC automation (12%)
IT/ITES	Threat detection & vuln. mgmt. (32%), Cloud security/CNAPP (18%), SOC automation (15%)
Manufacturing & Industrial	Threat detection & vuln. mgmt. (30%), SOC automation (18%), OT/ICS security (12%)
Healthcare & Pharma (small base)	SOC automation (20%), Threat detection (20%), Identity security (16%)
Other sectors	Threat detection & vuln. mgmt. (30%), SOC automation & incident response (19%), Identity & access security (12%)

Remaining share in each sector spreads across data security, privacy and identity line items not itemized above.



37%

Threat detection & vuln. mgmt. takes 37% of BFSI's AI security budget, the largest single allocation of any sector.

CHAPTER 02

Governance and the CISO's mandate

78%

of security leaders own or co-own AI governance

78% of security leaders own or co-own AI governance. Far fewer can say what share of their AI estate that mandate actually covers.

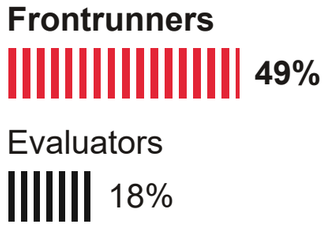


Governance coverage is the weakest number in the benchmark: only 21% of organisations keep more than 60% of AI under formal control, and 32% keep less than a fifth.

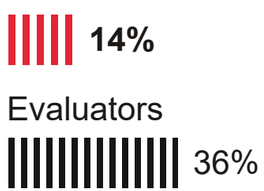
A formal AI governance framework is live in 42% of organisations, but only 15% call it fully implemented, rising to 32% among Frontrunners.

Manufacturing has the weakest governance maturity of any sector: 3% report fully implemented governance, against 17-20% elsewhere. Much of its AI runs on legacy OT systems that predate formal security governance.

Organisations keeping more than 60% of AI applications under formal governance



Organisations keeping less than 20% of AI applications under formal governance



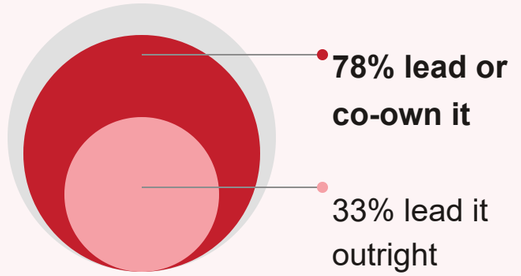
Generative AI is associated with much of the ownership-coverage gap: it's the fastest-moving, least-governed part of the AI estate. 34% say more than half their AI now involves generative models.

"AI is rapidly reshaping cybersecurity, from accelerating incident response to transforming workforce capabilities. Sustainable adoption requires stronger governance, privacy readiness and risk management. Success will come from responsible adoption, not adoption alone."

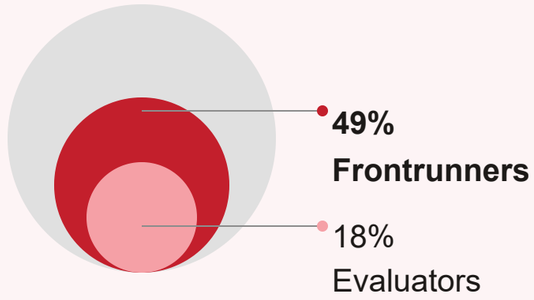


Vivek Shankar
CISO & Vice President
Axis Max Life Insurance Limited

Unlike Chapter 1, Frontrunners and Evaluators are close on governance. Running more AI hasn't produced more control. The advantage compounds: Frontrunners' AI governance ownership



More than 60% of AI applications under formal governance



Organisations where more than half of AI applications involve generative models



Organisations with a formal AI governance framework live in some form

Organisations describing that framework as fully implemented

Where the budget is moving

36%

of Frontrunners have a fully funded, fully implemented governance framework, more than 3x the rate of Evaluators (11%)

1

Governance ownership is established across most organisations; coverage is not. 78% of cybersecurity leaders lead or co-own AI governance, but only a fifth govern most of the AI estate.

2

A documented governance framework is common; a fully implemented one is rare. Fifteen per cent call theirs fully implemented.

3

Generative AI is scaling faster than the controls around it, the source of shadow AI and data-leakage risk.

What CISOs should do: stop reporting framework status to the board. Report coverage percentage instead, the number that separates a document from a control.

Cybersecurity leaders hold the AI governance mandate in most organisations. The gap is the fifth of organisations where **no one** holds it at all.

Who owns AI governance

Ownership	Share
CISO leads outright	33%
CISO co-owns with risk, legal or CIO	45%
Neither leads nor co-owns	22%

22% of organisations have no clear AI governance owner.



organisations have **no one** leading or co-owning AI governance, not the CISO, not risk, not legal, not the CIO.



03

CHAPTER 03

DPDP: confident, not evidenced

45%

have mapped more than half their personal data, versus 71% who call themselves DPDP-confident

71% are confident of meeting India's DPDP Act obligations. Fewer than half have mapped more than half their personal data.

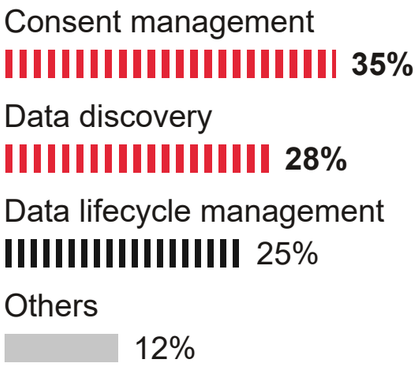
Confidence and evidence diverge by 26 points: 71% say they're confident of meeting DPDP obligations; 45% have mapped more than half their personal data.

Planned DPDP investment concentrates upfront: consent management draws the largest share (35%), then data discovery (28%); data lifecycle management, which sustains compliance after initial mapping, gets 25%, with the remaining 12% spread across other measures.

Confident or fully confident of DPDP compliance, but have mapped less than half their personal-data processing

71% report confidence in DPDP readiness, while only 45% have mapped more than half of their personal data — a 26-point gap between confidence and evidence.

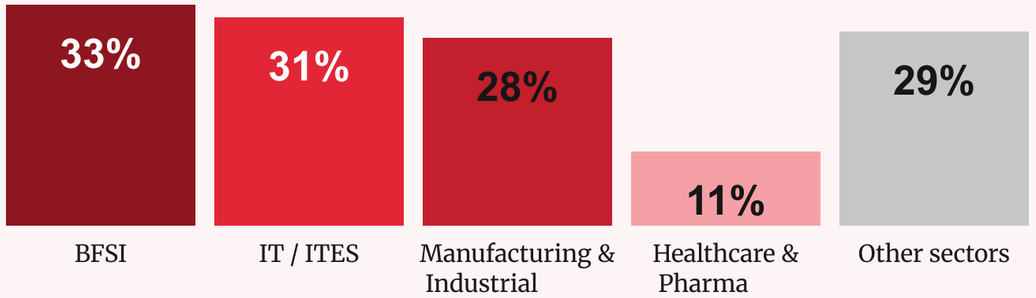
The compliance investment mismatch: consent and discovery outspend lifecycle management, 35% and 28% to 25%



Data lifecycle management, which sustains compliance after initial mapping, gets a smaller share than upfront consent and discovery work.

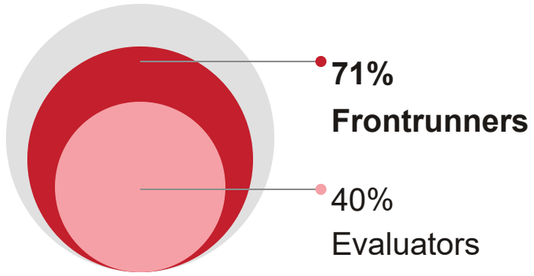
Full confidence in DPDP readiness ranges from 33% in BFSI to 11% in Healthcare & Pharma.

Organisations reporting full confidence in meeting DPDP obligations, by industry



† See methodology, Appendix 2: Healthcare & Pharma is directional given its small base.

Personal-data processing mapped above 50%



Where the budget is moving

35%

of DPDP compliance investment goes to consent management, the single largest line item, ahead of data discovery (28%)

1

71% of organisations say they're confident of meeting DPDP obligations, but only 45% have mapped more than half their personal data. Confidence in DPDP readiness exceeds the evidence behind it.

2

Frontrunners map more of their data. AI adoption seems to drive the inventory work compliance also needs.

3

Full confidence in DPDP readiness varies by sector without a clean regulated/unregulated split. BFSI leads at 33%; Healthcare & Pharma, despite faster AI adoption elsewhere, trails at 11%.

What CISOs should do: report confidence and mapping side by side, never alone. Fund mapping first where confidence is lowest: Healthcare, at 11%.

CHAPTER 04

Board attention is arriving faster than migration plans

50%

expect post-quantum security to become a board priority within 12 months

50% expect post-quantum security to become a board priority within 12 months, but only 8% report a migration strategy underway.

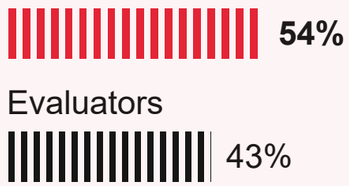


45% of organisations have taken post-quantum cryptography past awareness. 20% have not started; only 8% have a migration strategy under way.

Expectations exceed preparation: 50% anticipate board attention inside 12 months. Manufacturing is furthest behind, with 32% yet to start an assessment.

What CISOs should do: fund customer-facing systems and identity infrastructure first, the two most-named priorities.

Organisations that have moved beyond awareness on post-quantum cryptography



Organisations expecting board-level priority within 12 months



Where the budget is moving

92%

have no dedicated post-quantum budget line; the work competes against immediate threat remediation.

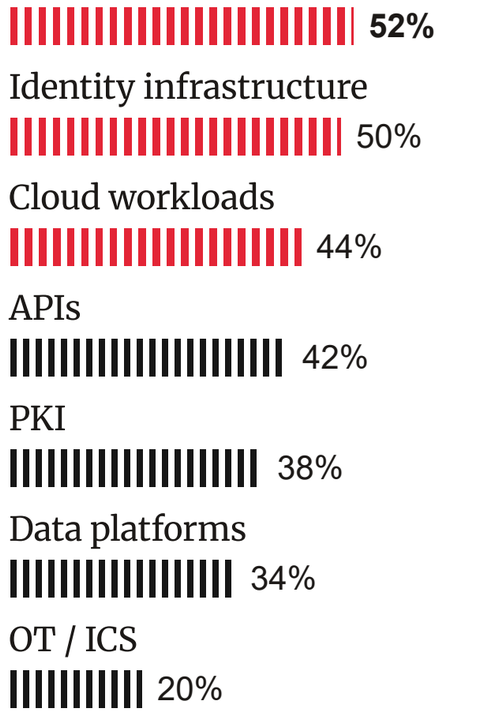
Respondents most often prioritise customer-facing applications and identity infrastructure for post-quantum migration, with OT/ICS named least often.

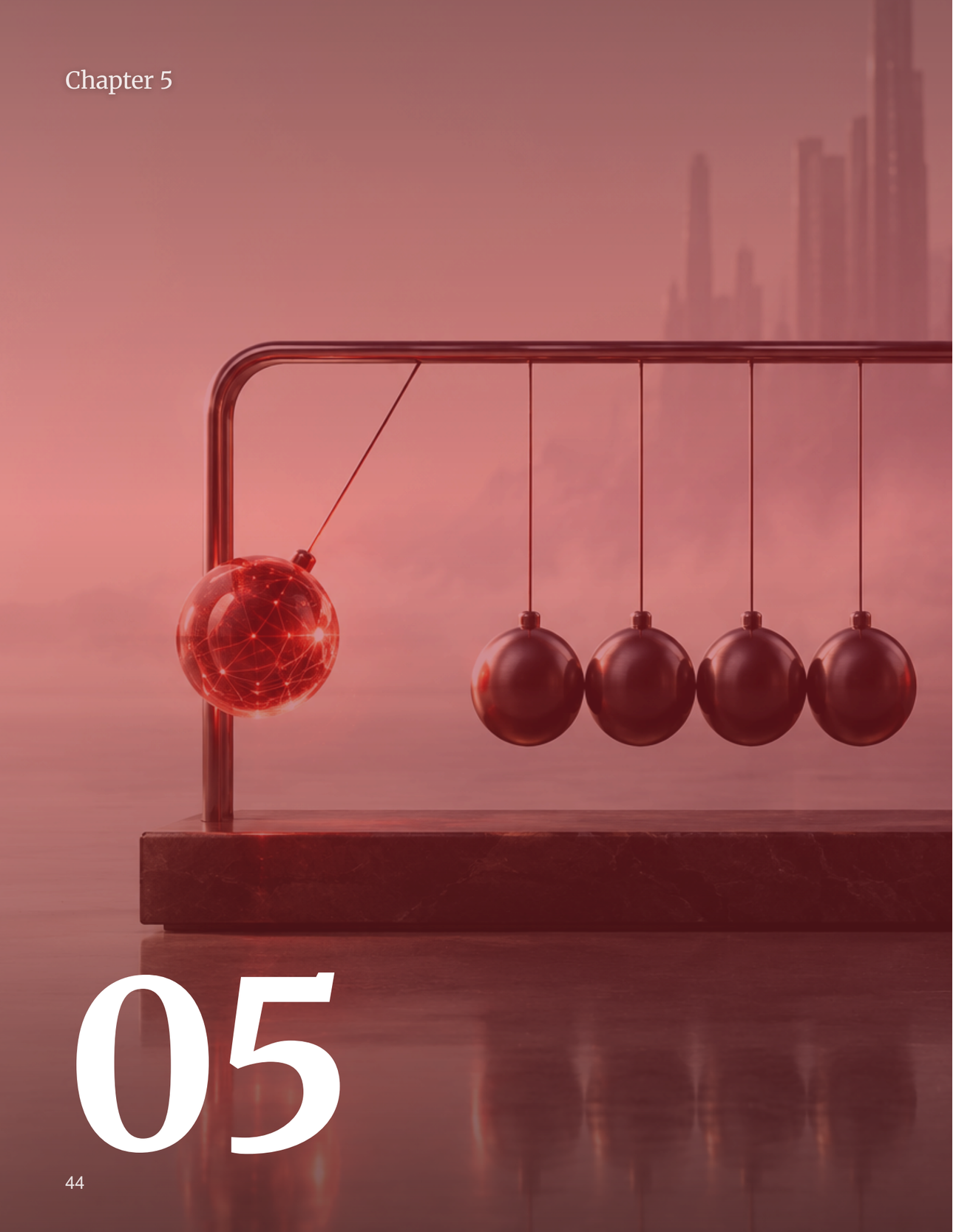
> "Harvest-now-decrypt-later has already happened. Tier your crown jewels by data shelf-life, not system criticality. That inverts most migration plans."



Aditya Khullar
CISO & DPO
Adani Digital Labs & NDTV

Systems named as first candidates for post-quantum migration





05

CHAPTER 05

The workforce dividend

71%

of Frontrunners report analyst workload down by more than a quarter

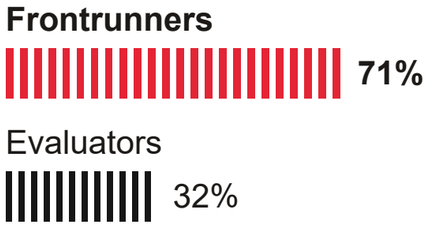
Workload reduction is most evident in Tier-1 work. 71% of Frontrunners report analyst workload down by more than a quarter.

AI is reducing workload faster than it is reducing headcount: 38% report analyst workload down more than a quarter, 71% among Frontrunners versus 32% of Evaluators. AI-driven automation is felt most strongly in Tier-1 SOC roles (22%), followed by the CISO office (17%) and threat-hunting functions (13%).

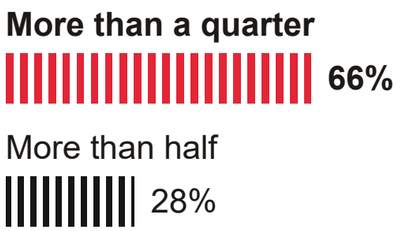
Reskilling is widespread but shallow: 66% have moved more than a quarter of staff through AI training; 28% moved more than half.

Reskilling is most extensive in Other sectors: 60% report having reskilled more than half of their security staff, against 10% in Manufacturing and 20% in BFSI.

Organisations reporting analyst workload reduced by more than 25%



Security staff moved through AI-related training



What CISOs should do: don't count reskilling by who's "started training": 66% have, but only 28% reskilled over half their team. Fund reskilling as a line item on every AI purchase, not a separate initiative.

Reskilled more than 50% of security staff on AI, by industry



> "AI is a rare paradox: it consolidates most technology functions but expands security's mandate. As adversaries orchestrate attacks at machine scale, defence talent must grow in both depth and judgement."



Praveen Kumar
CISO
Nykaa Fashion Pvt Ltd

22%

name SOC Analyst (Tier 1) as the role most affected by AI-driven automation

Roles most affected by AI-driven automation

Role	Share naming it first
SOC Analyst (Tier 1)	22%
CISO Office	17%
Threat Hunter	13%
SOC Analyst (Tier 2)	13%
Security Engineer	12%
GRC Analyst	7%

FIVE MOVES FOR LEADERS

What Cybersecurity Leaders Should Do Next

Build Trust Around the AI Estate

Only 21% govern more than 60% of their AI estate. CISOs & DPOs must move beyond traditional security frameworks to build enterprise-wide trust frameworks spanning cybersecurity, data, privacy, resilience, third parties and emerging technologies.

Take Leadership in AI Governance

78% of security leaders lead or co-own AI governance; only 21% govern most of the estate. Securing AI means building a resilient foundation with clear guardrails, accountability, human oversight and governance.

Translate AI Risk into Business Risk

Cyber risk is never binary. Future CISOs must frame decisions around risk appetite, tolerance and acceptance, translating technology risk into business impact for the Board.

Start the Quantum Migration Clock

50% expect board attention within 12 months; only 8% have a migration strategy underway. Shift to a phased quantum-readiness roadmap covering critical systems, identity infrastructure and cryptographic assets.

Turn Automation into Workforce Capacity

38% report >25% workload reduction; 71% among Frontrunners. Build AI literacy, governance expertise and automation skills across the workforce.



AI can improve security operations, this benchmark shows that clearly. Governing it consistently is another matter. The strongest outcomes are associated with broader AI adoption and stronger governance coverage.

Special Thanks

TO THE CISO COMMUNITY FOR THEIR CONTINUED SUPPORT

ETCISO TEAM

Krishna Mukherjee
Senior Lead, Content & Community, ETCISO

Shantheri Mallaya
Editor, ETCISO

Shreeja Dutta
Associate - Content & Research, ETCISO

Saima Khan
Senior Associate Community Relationship, ETCISO

Aakansh Gupta
Associate Community Relationship, ETCISO

Design
Shreeja Dutta
Ishan Arora

Appendix : About the research

ETCISO Intelligence surveyed over 200 senior security and technology leaders across India, spanning IT/ITES, BFSI, Manufacturing & Industrial, Healthcare & Pharma and other sectors, in Mumbai, Bengaluru, Delhi NCR, Pune and Hyderabad.

Respondents were grouped by how much of security operations use AI. Those above 50% are AI Security Frontrunners; the rest, Early Adopters and Evaluators.

"Where the budget is moving" figures come from respondents' self-reported spending intent over the next 12 months, not audited financial data.

Research note: Percentages represent respondent-level survey responses and may not sum to 100% where multiple responses were permitted. Sector-level findings for Healthcare & Pharma are directional because of the smaller base. Budget figures represent self-reported planned allocation/investment intent and are not audited financial data.

ET *CISO Intelligence*

About ETCISO Intelligence

ETCISO Intelligence is a comprehensive research and report product tailored for Cybersecurity leaders, specifically Chief Information Security Officers (CISOs), aiming to equip them with transformative insights essential for navigating the rapidly evolving digital cybersecurity landscape.

ETCISO Intelligence goes beyond data aggregation to actively gather insights from industry experts, thought leaders, and security practitioners. It employs a multi-faceted research approach, combining quantitative analysis, qualitative assessments, industry benchmarks, and expert opinions to provide a holistic understanding of key trends, opportunities, and risks in the cybersecurity domain. ETCISO Intelligence not only provides information but also distills it into valuable knowledge that cybersecurity leaders can leverage to drive meaningful change within their organisations.