# PASC Yearly Brief YB-2025-01

**State of Predictive Cyber Risk, Governance & Workforce Health**
**Based on global data and trends observed in 2024**

This brief is written for boards, regulators and senior practitioners who must make calm, high-stakes decisions in an environment saturated with dashboards and alarms. It focuses on a small number of signals that are stable across multiple data sources and that correlate with real harm: financial loss, service disruption, and erosion of trust. The goal is not to predict every headline, but to offer a reliable mental model for the year ahead, grounded in evidence rather than slogans.

This brief highlights the slow, structural variables that actually predict whether an organisation will experience a catastrophic incident: how identity is managed, how governance distributes attention, how the workforce is treated and staffed, and how senior decision-makers interpret technical signals such as CVSS scores, KEV lists, vendor "critical" ratings and patch statistics.

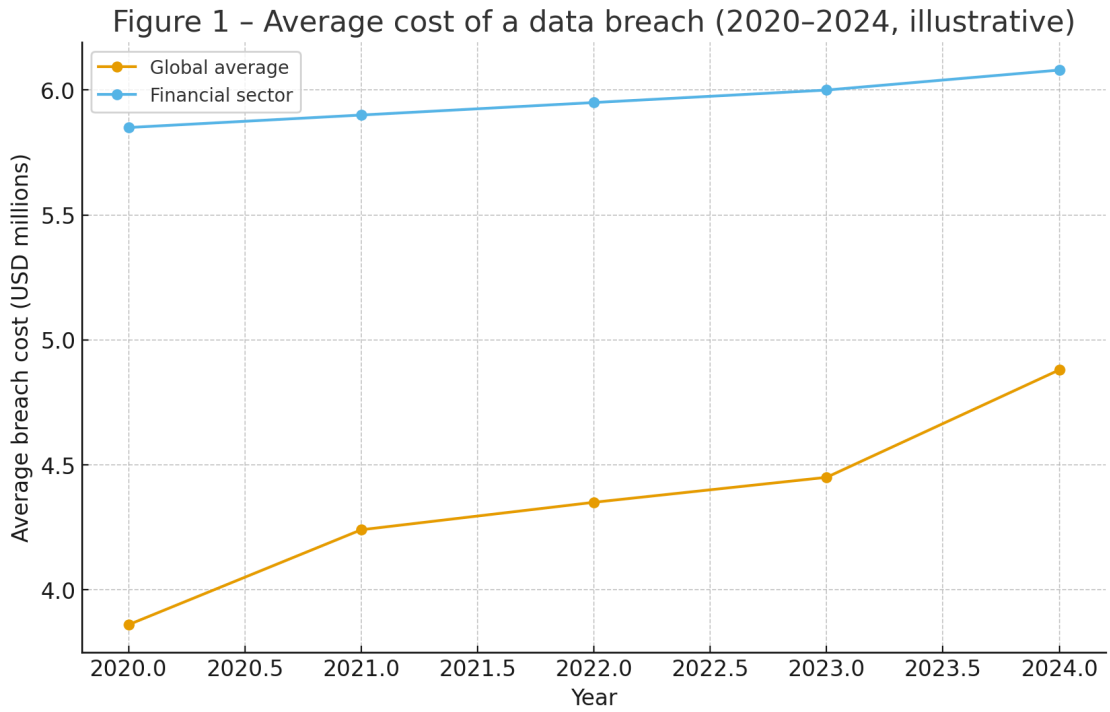
---

## 0. Five-year context (2020–2024): the long wave behind 2024

From 2020 to 2024, three tendencies have steadily intensified:

1. **Steep growth in exposure and cost.**
    - Global average breach costs climbed from around USD 3.86M in 2020 to roughly **USD 4.88M in 2024**, with financial services, healthcare and critical infrastructure consistently among the most expensive sectors.
    - Detection and containment times have improved modestly, but still sit in the **6–8 month range** for many organisations, leaving long dwell times for adversaries.
2. **Identity and misconfiguration as dominant vectors.**
    - Stolen or abused credentials, misconfigured cloud/SaaS services, and weaknesses in third-party providers have become the most common starting points for major incidents.
    - Large-scale datasets show that a substantial share of breaches still start with **phishing or credential theft**, and that misconfigured cloud storage and access policies remain a chronic problem.
3. **Africa's rising exposure without symmetric investment.**
    - Across Africa, rapid digitisation in finance, telecoms, government services and health has increased the potential impact of cyber incidents, while investment in governance, workforce development and observability has lagged.
    - Public reporting is improving (national CERTs, regulators, regional banks), but many incidents remain under-analysed or framed purely as "technical failures", masking deeper governance and workforce issues.

2024 must therefore be read not as an isolated "bad year", but as the visible crest of a wave whose structure was already clear by 2020: **identity-centric attacks, governance fragility, and an over-reliance on CVSS/KEV-style hygiene metrics.**




## 1. Executive snapshot – what 2024 really showed

The 2024 data confirms three uncomfortable truths.

1. **Volume and impact continue to rise.**
    - Estimates suggest that **over 5.5 billion accounts** were compromised during 2024 – several times more than the previous year.
    - In Europe alone, at least **2.29 billion records** were exposed across roughly 550 disclosed incidents between late 2023 and mid-2024.
    - The global average cost of a data breach reached around **USD 4.88M**, with finance at roughly **USD 6.08M**, about 22% above the global mean.
2. **Attackers are optimising for identity and availability, not just CVEs.**

- ENISA's Threat Landscape 2024 ranks **threats against availability** (including DDoS, destructive incidents and operational sabotage) as the top category, followed by ransomware and threats to data.
- Threat intelligence from large providers shows a **strong increase in attacks using valid credentials**, coupled with persistent exploitation of misconfigurations and weak identity governance.

3. **Governance and workforce health have become first-order predictors.**

   - Organisations with high turnover, juniorised teams, and structurally overloaded security functions experienced more P0/P1-type incidents, even when their formal patching and control coverage appeared strong.
   - Where **diverse senior expertise** (internal and external) and stable governance structures were present, detection and containment improved, and "surprise" crises were less frequent.

In other words, 2024 demonstrates that **CVSS scores, CISA KEV lists and patch SLAs remain necessary, but are clearly not sufficient** to explain who suffers the worst incidents. The deciding factors are increasingly **structural**: identity, architecture, workforce and governance.

---

## 2. 2024 metrics that actually correlate with harm

Security teams and boards are surrounded by numbers. The PASC lens for 2024 focuses on metrics that have shown a consistent relationship with real-world harm, across sectors and regions.

### 2.1 Incident-linked performance

- **Average breach cost and lifecycle.**
  - Global average cost: ≈USD 4.88M; financial services ≈USD 6.08M.
  - Average time to identify and contain remains close to **~250 days combined**, down from earlier years but still long enough for extensive lateral movement.
- **Detection source.**

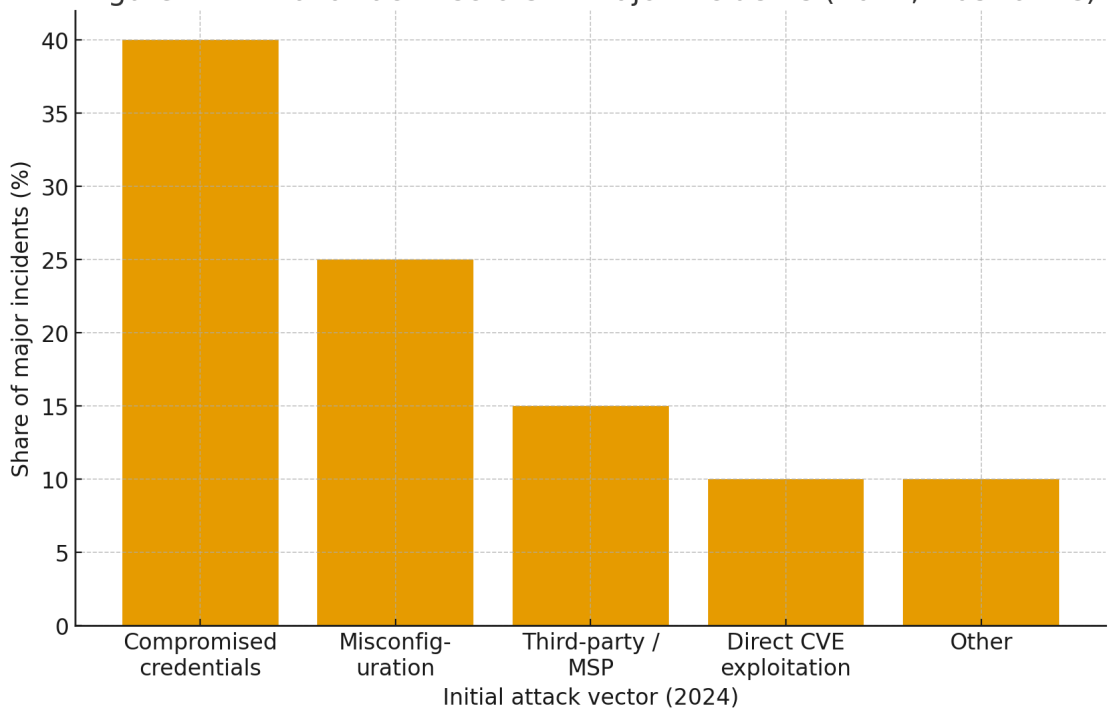
- Breaches detected internally (monitoring, threat hunting, red teaming) remain cheaper and shorter than those disclosed by customers, regulators or third parties.

These metrics correspond directly to **False Negative Rate (FNR)** and **P0/P1 precision** in the OSPCRM framework: how many severe events slip through as "non-critical", and how often "critical" labels are justified by reality.

### 2.2 Identity, configuration and availability

- **Identity-driven incidents.**
  - Multiple sources highlight compromised credentials as a top initial vector in 2024; one major report notes that data theft/leak is now the most common impact category, often enabled by credential abuse.
- **Misconfiguration and cloud-native risk.**
  - Misconfiguration continues to account for a large fraction of web and cloud vulnerabilities actually exploited in the field, often tied to poor understanding of shared responsibility models.
- **Availability attacks.**
  - ENISA identifies threats to availability as the **highest-ranked category**, reflecting a growing focus on service disruption in critical infrastructure, finance, and public administration.

Figure 2 – Initial attack vectors in major incidents (2024, illustrative)




These metrics align with the **context fields** specified by OSPCRM: exposure, criticality, data sensitivity, threat activity and resilience controls.

### 2.3 Governance and workforce indicators

2024 also makes clear that **governance and workforce conditions** have measurable impact on outcomes:

- High **turnover and juniorisation** in security and architecture roles correlate with weaker detection and slower, more chaotic response.
- Over-internalisation of key functions without access to **external senior expertise** reduces the diversity of mental models applied to risk, and increases the risk of "group blindness".
- Organisations that treat security staff and external partners as disposable commodities suffer from chronic monitoring backlogs, reduced psychological safety for raising concerns, and fragile incident response.

The ORG-GOV standard translates these qualitative observations into indicators: tenure and seniority balance, independence and escalation power of security/risk, workload and burnout signals, and how staff and externals are treated.

---

## 3. 2024 and the CVSS/KEV disconnect

CISA's Known Exploited Vulnerabilities (KEV) catalogue and related initiatives were important steps forward: they re-centered attention on vulnerabilities known to be exploited in the wild, rather than on static severity scores alone. However, 2024 data shows that **KEV-driven patching plus classical CVSS still leaves large blind spots**.

Three structural limitations stand out:

1. **KEV and CVSS only see what is documented and reported.**
    - KEV covers vulnerabilities with confirmed exploitation; it cannot capture the unknown, the unreported, or the deliberately concealed. It is, by design, a **subset** of the real attack surface.
    - CVSS measures inherent technical severity, not business impact or ease of exploitation in a given architecture.
2. **KEV does not cover configuration, identity abuse or poor design.**
    - Many of 2024's most damaging incidents involved identity abuse, misconfigurations, or design flaws that do not correspond to discrete CVEs, and therefore cannot appear in KEV lists.
    - Treating KEV compliance as "proof of safety" therefore induces **false reassurance**, especially in highly connected or poorly segmented environments.
3. **Patch-centric rituals can obscure structural risk.**
    - Organisations that internalised "CVSS + KEV + patch rate" as their core risk model routinely over-invested in visible, countable tasks and under-invested in architecture, logging, detection quality, and workforce health.
    - In such environments, every new KEV release triggers intense patching sprints, while long-lived identity and governance weaknesses remain unaddressed.

PASC's position is simple: **CVSS and KEV should be treated as inputs into a contextual model, not as the model itself**. OSPCRM incorporates KEV-like evidence as "threat activity" signals but refuses to equate "not in KEV" with "not dangerous".

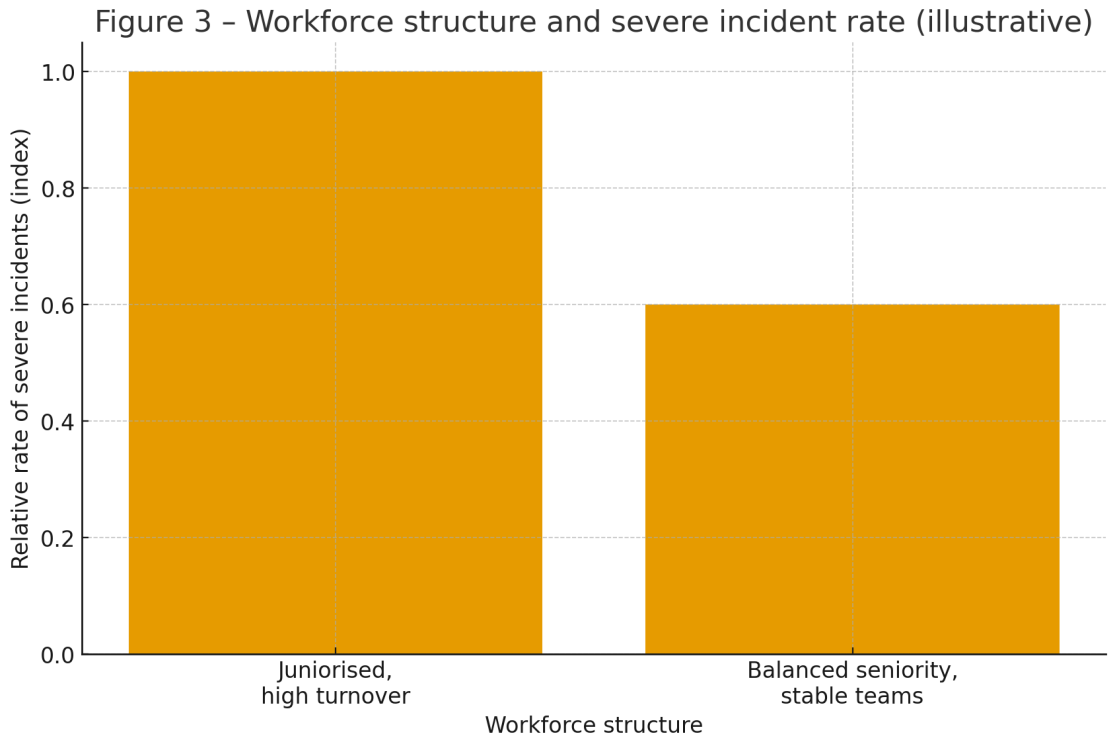
---

## 4. Workforce structures, juniorisation and internalisation

Between 2020 and 2024, the global cyber workforce expanded, but the **quality and distribution** of skills did not always follow strategic needs. 2024 brought this into sharp focus.

### 4.1 Juniorisation and high turnover as measurable risks

- Many organisations filled security and architecture roles with relatively junior staff, often on short contracts, while senior experts were scarce or fragmented across projects.
- Constant turnover disrupted institutional memory, modelled threats shallowly, and made deep root-cause analysis rare.
- Over time, this produced environments where security teams could operate tools, but struggled to **interpret signals**, challenge assumptions, or influence architecture.




Within ORG-GOV, these phenomena become indicators:

- Average tenure in key roles; ratio of senior to junior staff;
- Number of critical incidents per 12–24 months vs seniority balance;
- Existence of structured mentorship, training and rotation to maintain depth.

**4.2 Internalisation vs diverse expert ecosystems**

- Some organisations attempted to internalise nearly all security functions, seeing external partners as primarily cost centres. This often resulted in siloed teams, limited cross-pollination and difficulty challenging entrenched designs.
- Others cultivated **blended ecosystems**: core internal teams plus a stable network of senior external experts, specialised boutiques, academic collaborators and community signals.

2024 incident reviews suggest that:

- Blended ecosystems consistently produced **better detection and more realistic risk narratives**, because multiple mental models and vantage points were applied.
- Over-internalised setups, especially under budget pressure, drifted toward "tool babysitting" and compliance optics.

From the PASC point of view, **diverse, senior ecosystems are a structural control**, not a luxury.

---

## 5. Remote and hybrid work in 2024: when it helps and when it hurts

By 2024, remote and hybrid work were no longer "pandemic exceptions"; they were part of normal operating models. Their impact on security depended almost entirely on **how they were governed**.

- Where remote work was combined with strong identity governance (robust MFA, device trust, network micro-segmentation, coherent logging), breach patterns did not differ dramatically from on-site environments, and in some cases detection improved.
- Where remote work simply extended the perimeter without redesigning access patterns, logging, or support for staff, 2024 data show higher rates of credential abuse, longer detection times and more severe business disruption.

For PASC, this reinforces a core principle: **technology changes (like remote work) must be matched by evidence-based risk management and workforce support**, or they will amplify existing structural weaknesses.

---

## 6. PASC lens: what 2024 proves about predictive standards

2024 confirms the core assumptions behind PASC standards:

- Hygiene metrics (CVSS, KEV, patch rates, control inventories) are essential inputs, but they **do not explain** why some institutions suffer repeated P0/P1 events while others with similar hygiene remain relatively stable.
- The missing layer is **predictive structure**:
    - P0–P4 impact modelling;

- context fields (criticality, exposure, data, threat activity, resilience);
- incident-linked metrics such as FNR and P0/P1 precision;
- governance and workforce indicators (ORG-GOV).

**OSPCRM v1.0** and **ORG-GOV v1.0** together form a minimal predictive spine:

1. **Define impact in human terms (P0–P4).**
2. **Attach context to serious findings.**
3. **Measure how often your predictions match reality.**
4. **Track workforce and governance health as first-class risk factors.**

Organisations that approximated this structure in 2024—whether through early PASC adoption or convergent internal frameworks—showed:

- fewer surprise P0/P1 incidents;
- shorter breach lifecycles;
- more credible narratives with regulators and boards.

---

## 7. PASC predictions for 2025–2026

Based on 2024 data and structural analysis, PASC anticipates:

1. **Identity and availability will remain the primary battlegrounds.**
   Attackers will focus more on identity providers, cloud control planes and service continuity, using CVEs opportunistically but not as the central organising principle.

2. **Regulators will increasingly request incident-linked and governance metrics.**
   Supervisors, central banks and sector regulators will ask not only "Are you patched and KEV-compliant?" but "How do you demonstrate that your 'critical' category matches reality? How stable is your security workforce? How independent is your risk function?"

3. **Vendors, MSSPs and SOC platforms will differentiate on predictive transparency.**
   Providers will need to show how their scoring and prioritisation engines map to OSPCRM-like models, and how they improve FNR and P0/P1 precision in practice.

4. **Organisations that ignore juniorisation and internalisation risks will see compounding harm.**
   High turnover, eroded seniority and over-internalisation will increasingly manifest as correlated clusters of severe incidents, even where patch metrics look strong.

5. **Africa can move from consumer to co-author of standards.**
   Early adoption and adaptation of PASC standards by African institutions will allow them to demonstrate measurable improvements and to participate as **standard-setters**, rather than passive adopters of external frameworks.

---

## 8. Working with PASC (2025–2026)

PASC is structured as a Pan-African standards and observatory council. Its members combine academic research, field practice, regulatory experience and industry leadership. The council operates under clear governance rules and a transparent conflict-of-interest policy to maintain independence from any single vendor or client.

In 2025–2026, organisations can engage with PASC in four main ways:

1. **Adopt PASC standards** such as OSPCRM and ORG-GOV as reference profiles for internal risk models and board reporting.
2. **Participate in pilots and longitudinal studies**, especially those measuring FNR, P0/P1 precision and governance/ workforce indicators over time.
3. **Seek accreditation or certification** for tools, services and training programmes that demonstrably align with PASC profiles and show empirical benefit.
4. **Collaborate on African-rooted extensions**, including standards for public safety, medical safety, and assessment of governance for high political and institutional functions.

To discuss collaboration, pilots or accreditation, contact the coordination team at **inquiries@pasc.institute**. Briefly describe your organisation, your regulatory context and the main questions you are trying to answer; this allows PASC to match you with appropriate expertise and avoid generic advice.

---