PASC Yearly Brief YB-2024-01

PASC Yearly Brief YB-2024-01
State of Predictive Cyber Risk, Ransomware Economics & Governance Health
Based on global data and trends observed in 2023

This brief is addressed to boards, regulators and senior practitioners who must take strategic decisions under pressure, with incomplete information. It deliberately ignores most "noisy" statistics and focuses instead on a small set of indicators that reliably correlate with real harm: sustained operational disruption, direct financial loss, and measurable loss of trust.

Our central message for 2024 is simple: **classical hygiene metrics (CVSS, KEV, patch counts) are diverging from the patterns of actual damage.** Ransomware economics, identity-driven intrusion and governance fragility are now better predictors of catastrophic outcomes than the sheer number of vulnerabilities discovered or patched.

0. 2019–2023: the curve that brought us here

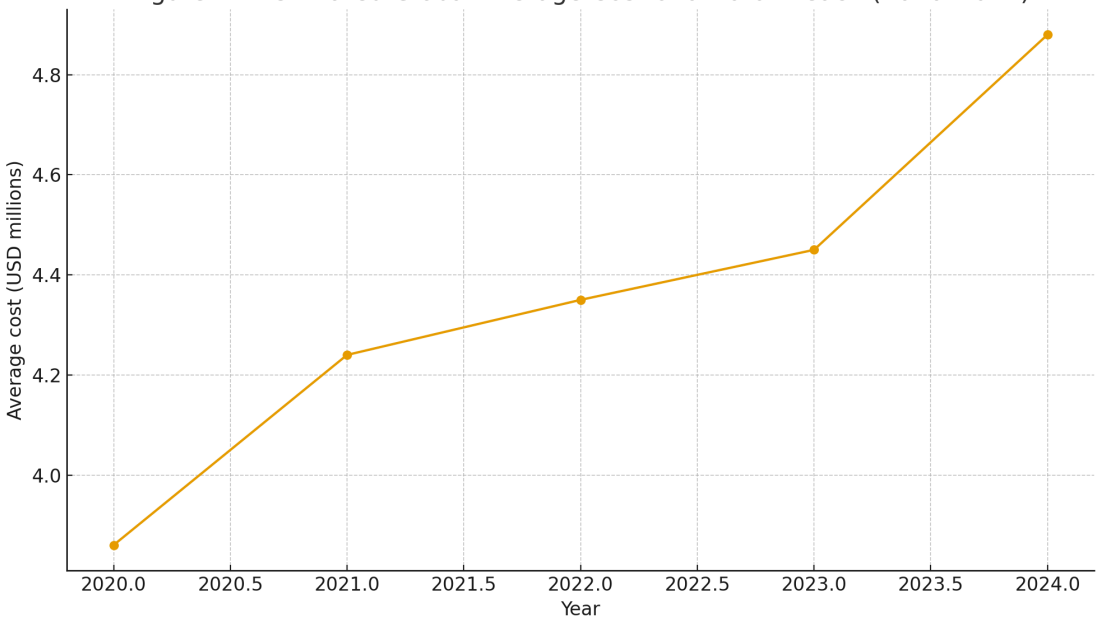
Across the five-year window from 2019 to 2023, three long trends matter for decision-makers:

1. **The cost of a breach keeps climbing.**
   IBM's 2023 Cost of a Data Breach report places the **global average cost at USD 4.45 million**, up from USD 4.35 million in 2022 and USD 3.86 million in 2020—a cumulative increase of over 15% since 2020.

2. **Ransomware matures into an economic system.**
   Chainalysis and other blockchain-analytics sources estimate that **ransomware payments exceeded USD 1.1 billion in 2023**, nearly double 2022 levels and the highest volume ever recorded.
   This does not include indirect losses from downtime, recovery and reputational damage.

3. **Africa moves from peripheral to primary target.**
   In Q2 2023, Africa recorded the **highest average number of cyberattacks per organisation per week**, with a 23% increase versus the same period in 2022.
   Earlier analyses suggest that **over 90% of African companies still operate without adequate cybersecurity protocols**, leaving a large exposed surface in rapidly digitising sectors.

Figure 1 – Estimated Global Average Cost of a Data Breach (2020–2024)



For 2024 decision-making, 2023 should therefore be read as a **consolidation year**: the structural weaknesses that emerged after 2020—identity, supply chain, governance and workforce—have now fully translated into hard economic signals.

---

1. Executive snapshot – what 2023 actually showed

Three patterns from 2023 stand out for boards and regulators.

1.1 Record breach costs, with persistent dwell times

- The **average cost of a data breach** reached **USD 4.45 million**, a new high and part of a steady upward trend since 2020.

- Detection and containment still take **hundreds of days** on average; while exact figures vary by sector, most large studies place total breach lifecycle in the ~250–280-day range, leaving adversaries ample time for exploration and lateral

movement.

1.2 Ransomware as a structural test of governance

- ENISA's Threat Landscape 2023 identifies **ransomware and DDoS** as top threats, with ransomware alone accounting for around **a third of EU-tracked threats** during the reporting period.
- Globally, ransomware payments pass the **USD 1.1 billion** threshold.
- High-profile campaigns (including supply-chain events such as the MOVEit exploitation) show that attackers are now using ransomware not only for short-term cash, but as a **lever to stress-test entire governance structures**: third-party oversight, disclosure discipline, and the ability to prioritise under pressure.

1.3 Identity, phishing and misconfiguration as main doorways

The IBM 2023 report confirms a shift in how attacks begin:

- **Phishing** accounts for about **16% of breaches**,
- **Stolen or compromised credentials** for **15%**,
- **Cloud misconfiguration** for **11%**, and
- **Business email compromise** for **9%**.

In other words, **at least half of recorded breaches start with identity and configuration issues**, not "exotic zero-days". This is essential context for reading CVSS and KEV data correctly.

---

2. 2023 indicators that matter for real risk

Most organisations already track large numbers of metrics. PASC's view is that leaders should focus on **a compact set** that aligns with predictive questions: "Where are we most likely to suffer a P0/P1-type incident in the next 12–24 months?"

2.1 Incident-linked performance

From a PASC / OSPCRM perspective, three families of metrics are more informative than raw vulnerability counts:

- **Cost and lifecycle per breach.**
  Average cost (USD 4.45M) and long dwell times remain direct proxies for **False Negative Rate (FNR)** and detection quality.

- **Initial vector distribution.**
  The dominance of phishing, stolen credentials and misconfiguration as initial vectors reveals how often security programmes **misallocate attention**: patch sprints are intense, while identity and architecture hygiene remain partial.

- **Effect of automation and AI.**
  Where security AI and automation were deployed coherently, IBM reports **up to 108 days faster detection/containment and roughly USD 1.76M lower breach costs** on average.
  This is less about technology fashion and more about **closing the FNR gap** by reducing missed signals.

2.2 Threat mix and concentration

ENISA records **2,580 significant cyber incidents between July 2022 and June 2023**, with public administration (19% of attacks) and health (8%) among the most targeted sectors.

Three points follow:

- Ransomware and DDoS remain primary tools to test the **availability and resilience** of services.

- Supply-chain compromises are no longer exceptional events but a recurring pattern.

- Sectors providing core public services (government, health) are structurally exposed, with direct implications for societal trust.

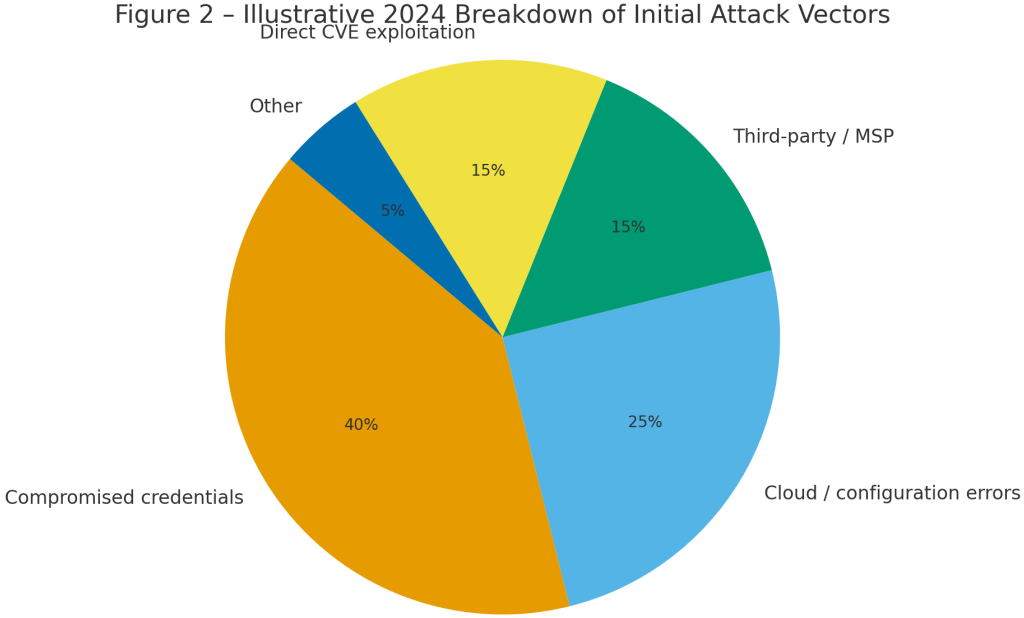
2.3 African exposure as a strategic variable

African-focused analyses add a critical dimension:

- Africa experienced the **highest average number of weekly attacks per organisation** in Q2 2023, with a 23% increase vs Q2 2022.

- Earlier Interpol and policy reports point out that **a very high share of African businesses—often cited above 90%—lack mature cybersecurity protocols**, even as mobile finance, e-government and critical infrastructure digitise rapidly.

Figure 2 – Illustrative 2024 Breakdown of Initial Attack Vectors



From a PASC standpoint, this combination—**high exposure + incomplete governance + fast digitisation**—makes Africa a priority region not only for protection, but also for **innovative standards and measurement**.

3. 2023: ransomware, extortion and supply chain as governance exams

2023 is the year where ransomware and extortion stop being "just another threat type" and become a **diagnostic test of governance maturity**.

- Global estimates suggest ransomware actors harvested **around USD 1.1 billion** in 2023—double 2022—even though the proportion of victims paying appears to be decreasing.

- Large-scale exploitation of widely used solutions (such as MOVEit) showed that **even organisations with reasonable patch practices were caught unprepared**:

    - incomplete asset inventories;

    - unclear ownership of third-party risks;

    - limited ability to trace which data flows depended on which vendor systems.

From the PASC perspective, these events are **not anomalies**; they are symptoms of three structural weaknesses:

1. **Over-reliance on vendor severity labels and CVSS scores.**

2. **Under-investment in mapping critical data flows and dependencies.**

3. **Fragmented responsibility for risk, split between multiple teams and providers.**

OSPCRM treats such incidents as **high-value learning signals**: if a supposedly "well-governed" environment repeatedly suffers surprise P0/P1 events via supply-chain exploitation, this reveals a gap in its predictive model, not just "bad luck".

4. 2023 and the limits of CVSS/KEV-centric thinking

CISA's KEV lists and CVSS scoring were never designed to be full risk models. However, 2023 makes the gap particularly visible:

- Many of the most damaging incidents exploited **known vulnerabilities and misconfigurations** which organisations could have prioritised but did not; others used phishing and credential theft that **do not map cleanly** to CVSS at all.
- KEV coverage is, by design, limited to **documented exploited vulnerabilities**. It cannot see:
    - unpublished or undisclosed exploits,
    - identity-only attack paths,
    - design flaws and architectural weaknesses with no CVE.

The result, observed in 2023:

- Organisations show good **patch KPIs** and KEV compliance, yet still experience long dwell times and expensive incidents.
- Boards and regulators receive dashboards that look reassuring, while **the actual probability of a catastrophic event remains high**.

PASC's position is firm: **CVSS and KEV must be demoted from "risk model" to "input signal"**. OSPCRM and related standards treat them as one layer in a broader set of context fields and performance metrics.

---

5. Operating models and workforce: early structural warnings

By 2023, two human-structural tendencies become hard to ignore, even though they are less frequently quantified than technical metrics.

5.1 Tool sprawl and analyst overload

Across multiple sectors, 2023 incident reviews and surveys converge on a familiar picture:

- Security teams manage **too many tools**, each with its own dashboards and alert streams.
- Correlation and prioritisation depend heavily on a few over-stretched individuals.
- Alert fatigue and "background noise" lead to missed weak signals in the weeks before major incidents.

Where organisations invested in coherent automation and rationalised their toolsets, IBM observes **shorter breach lifecycles and lower costs**; where they did not, tooling became an additional cognitive burden.

5.2 Juniorisation and over-internalisation (first visible cracks)

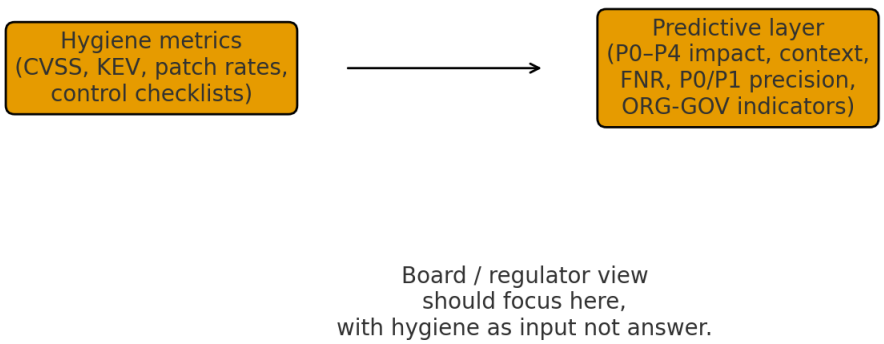
The full impact of **juniorisation** and **over-internalisation** becomes more visible in 2024, but 2023 already shows early cracks:

- Critical monitoring, architecture and identity functions are increasingly staffed by junior profiles, often without stable mentorship or proximity to senior decision-makers.
- Budget pressure encourages some organisations to **internalise everything**, limiting engagement with external senior experts, independent threat intelligence and specialised boutiques.

The pattern observed in post-incident analyses is consistent:

- Organisations that **kept a balance of senior internal staff and trusted external experts** showed better preparedness for novel attack patterns and a more realistic understanding of their own weaknesses.
- Environments that combined juniorisation, high turnover and isolation tended to **discover issues late**, often when damage was already substantial.

ɹre 3 – PASC View: From Hygiene Metrics to a Predictive Risk Mo



For PASC, these are not mere HR details; they are **governance indicators** that belong next to technical metrics in any predictive model.

Across the 2023 data, one of the most worrying patterns is the growing disconnect between where effort is spent and where incidents actually occur. Several organisations that reported excellent CVSS-based patch metrics and "green" KEV compliance curves nonetheless suffered multiple severe incidents shortly after or alongside security budget reductions, forced returns to office, aggressive internalisation of services or high turnover in key roles. In practice, headcount cuts and juniorisation in monitoring, architecture and governance functions quietly increased the False Negative Rate for serious scenarios, even as patch reports improved. Conversely, environments that maintained stable, respected security teams and a balanced mix of internal staff and senior external experts often experienced fewer and shorter incidents despite having similar vulnerability backlogs. For boards and regulators, this is a critical warning: **CVSS and patching effort cannot be used as a proxy for overall risk if workforce health, governance stability and operating-model changes are ignored.**

6. Africa in 2023: high pressure, limited measurement

The African context in 2023 is particularly important for a Pan-African standards council:

- Africa recorded the **highest average weekly number of cyberattacks per organisation** in Q2 2023, with a 23% increase over 2022.
- ICS-focused reports show **attack rates on industrial control systems in Africa exceeding global averages**, underlining the exposure of energy, manufacturing and critical infrastructure.
- Many countries still lack fully operational national CERTs, mature reporting regimes, or harmonised legal frameworks.

This creates both risk and opportunity:

- Risk, because the **gap between digital dependency and governance capacity** is widening.
- Opportunity, because Africa can **bypass some of the historical mistakes** of other regions by adopting standards that directly measure:
    - service continuity and availability;
    - governance quality and workforce health;
    - predictive power of risk models, not just compliance.

This is precisely the niche PASC aims to occupy.

---

7. PASC interpretation and recommendations for 2024

The 2023 data strongly validate the design choices behind PASC's emerging standards, including **OSPCRM** (Open Sovereign Predictive Cyber Risk Management) and **ORG-GOV** (Organisational Health & Governance Quality):

- Hygiene metrics (patches, CVSS, KEV, control inventories) remain necessary, but cannot be used as the **primary measure** of safety.
- Identity, configuration, workforce and governance must be elevated from background concerns to **first-class components of the risk model**.
- Incident-linked metrics (FNR, P0/P1 precision, breach lifecycle) should be tracked as carefully as financial indicators.

For 2024, PASC recommends that organisations aiming for **minimal, high-impact change** do the following:

1. **Introduce a P0–P4 impact scale** aligned with business language and governance realities.
2. **Enrich all serious findings** (regardless of origin—vulnerability, misconfiguration, identity) with a small, mandatory set of context fields: criticality, exposure, data sensitivity, known threat activity and resilience controls.
3. **Track two or three performance metrics** for the security function, such as FNR for P0/P1 incidents, P0/P1 precision and average time to escalate a realistic scenario to executive attention.
4. **Add one governance/ workforce indicator** to regular risk reporting (for example, turnover in key security roles, proportion of senior to junior staff, or independence of the security function).

These steps can be implemented without waiting for full tooling changes and will significantly improve conversations with boards, regulators and auditors.

8. Working with PASC (2024–2025)

PASC operates as a Pan-African standards and observatory council. Its membership combines:

- academic and clinical researchers;
- experienced practitioners from critical sectors;
- regulators and policy specialists;
- industry leaders and senior consultants.

The council is governed by clear rules on independence and conflict of interest. Vendors and individual clients cannot dictate the content of standards, although they are encouraged to contribute data and feedback.

In 2024–2025, organisations can engage with PASC through:

- **Adoption of standards** such as OSPCRM and ORG-GOV as reference profiles for internal models, board reporting and regulatory dialogue;
- **Participation in observatory pilots**, providing anonymised incident and governance data to refine the predictive metrics;
- **Accreditation and certification pathways** for tools, services and training that demonstrably improve FNR, P0/P1 precision or governance indicators;
- **Collaborative development** of sector- or country-specific profiles, particularly in African and emerging markets.

To explore collaboration, pilots or accreditation, contact the coordination team at **inquiries@pasc.institute** with a short description of your organisation, regulatory context and core questions. This allows PASC to respond with targeted guidance rather than generic recommendations.