PASC Yearly Brief YB-2023-01

PASC Yearly Brief YB-2023-01
State of Predictive Cyber Risk & Governance
Based on global data and trends observed in 2022

This brief is written for boards, regulators and senior practitioners who must make calm, high-stakes decisions in an environment saturated with dashboards, alerts and vendor claims. It focuses on a small set 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 incident, but to provide a reliable mental model for the year ahead, grounded in evidence rather than marketing.

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 staffed and supported, and how senior decision-makers interpret technical signals such as CVSS scores, KEV lists, EPSS predictions and patch statistics.

0. Context: from 2018 to 2022 – the world and Africa

Between 2018 and 2022, four converging trends shaped the current landscape:

- **Breach cost and complexity kept climbing.**
  Global average breach costs moved from ≈USD 3.86M in 2020 to ≈USD 4.35M by 2022, with detection/containment times still around 270 days for many organisations. Finance, healthcare and critical infrastructure remained the most expensive sectors to breach.

- **Ransomware industrialised.**
  Ransomware evolved into a full ecosystem: initial access brokers, data-leak marketplaces, negotiation specialists and "as-a-service" operators. Many "data breaches" were now also ransomware, and many ransomware incidents involved prior data theft.

- **Identity and cloud became the real terrain.**
  Public reports consistently showed that the main initial vectors were **compromised credentials, phishing and misconfigurations**, with classic perimeter exploits playing a supporting role rather than the main story.

- **Africa's exposure increased faster than its instrumentation.**
  Accelerated digitisation (mobile money, digital IDs, e-government, health, education) created concentrated risk in African countries. Yet observability, specialised workforce capacity and adapted governance frameworks lagged, leaving many institutions dependent on imported standards and vendors, with limited local capacity to challenge architecture or prioritisation.

By 2022, the world—and Africa within it—was operating in a **permanently hybrid, identity-centred, data-driven risk environment**, while many control frameworks and dashboards still reflected older, perimeter-centric assumptions.

---

1. Executive snapshot – what 2022 really showed

The 2022 data confirms three core points.

1. **Cost, dwell time and impact remained high.**
    - Global average breach costs were in the ≈**USD 4.3–4.4M** range, with finance, healthcare and critical services above that baseline.
    - The combined time to identify and contain a breach still hovered around **250–280 days** for many organisations, giving attackers months of undetected activity.
2. **Initial vectors were dominated by identity and configuration, not just CVEs.**
    - Stolen credentials, phishing and human error (including misconfiguration) were among the top initial attack vectors in 2022 incident datasets, ahead of pure vulnerability exploitation in several sectors.
    - Misconfigured cloud storage, lax access policies and poorly governed third-party access repeatedly appeared in large-scale breaches.
3. **KEV and EPSS appeared – and were immediately misunderstood.**
    - CISA's Known Exploited Vulnerabilities (KEV) catalogue and exploitation prediction models (EPSS and similar) gained traction as tools to refine prioritisation.
    - However, in many organisations, "KEV + high CVSS + patch SLA" was quickly treated as a **proxy for holistic risk**, even though KEV/EPSS focus on exploitation of specific CVEs and say nothing about identity abuse, design flaws, governance or workforce health.

For PASC, 2022 is the year when **"patch what KEV/EPSS tells you" became a ritual**—useful, but dangerously incomplete when treated as the main measure of safety.

---

2. 2022 metrics that actually correlate with harm

Security and risk functions in 2022 were surrounded by numbers. The PASC lens focuses on those that showed consistent correlation with real harm across multiple data sources.

2.1 Incident-linked performance

- **Breach cost and lifecycle.**
  - Average global breach costs ≈USD 4.35M; sectors such as finance and healthcare substantially higher.
  - Detection and containment times still close to **9 months combined** for many organisations, even when "average detection time" in dashboards appeared lower for less severe events.
- **Detection source.**
  - Breaches first detected by internal security operations, threat hunting or structured testing were consistently cheaper and shorter than those disclosed by customers, regulators, law enforcement or the media.

Within the OSPCRM framework, these map directly to **False Negative Rate (FNR) for P0/P1 events** and **P0/P1 precision**: how many severe incidents originate from issues previously treated as low-risk, and how often "critical" labels are correct.

2.2 Identity, cloud and third parties

- **Stolen or abused credentials.**
  - A large share of malicious breaches in 2022 began with credential theft (phishing, brute forcing, reuse, token abuse), often chained with MFA fatigue or social engineering.
- **Misconfiguration and cloud-native risk.**
  - Cloud storage misconfigurations, over-permissive access policies and insufficient logging were implicated in numerous high-profile exposures.
- **Third-party and managed service providers.**
  - Several major incidents in 2022 illustrated that weaknesses in suppliers, integrators or MSPs could act as force multipliers, propagating risk into multiple client institutions simultaneously.

These factors align with OSPCRM's **context fields**: asset/service criticality, data sensitivity, exposure, threat activity and resilience controls.

2.3 Governance and structural health

2022 also made it clearer that **governance and workforce conditions** are risk factors in their own right:

- **Juniorisation and overload.**

    - Many security teams were heavily staffed with junior analysts managing high alert volumes, while senior expertise was fragmented across too many responsibilities or outsourced without strategic integration.
- **Ambiguous accountability.**
    - In many institutions, it remained unclear who had the authority to halt risky deployments, challenge architecture, or escalate chronic under-resourcing.
- **Treatment of staff and externals.**
    - High churn, limited training and inadequate collaboration with external experts produced shallow, repetitive responses to complex threats.

ORG-GOV treats these as measurable indicators: tenure and seniority distribution, independence of security/risk, escalation power, workload and burnout signals, and how staff and external partners are treated.

---

3. 2022 and the illusion of "KEV + CVSS = risk model"

CISA's KEV catalogue and exploitation prediction models were significant advances, and PASC recognises them as **valuable inputs**. However, 2022 showed how easily they can be misused.

Three recurring failure modes:

1. **Narrow scope treated as complete map.**
    - KEV lists only vulnerabilities known to be exploited in the wild; EPSS estimates exploitation likelihood for CVEs. Both are, by design, centred on **documented software flaws**, not misconfigurations, identity abuse, insider activity or poor design.
    - Many severe 2022 incidents arose from issues that were not naturally representable as CVEs at all.
2. **Checklist thinking.**
    - In numerous organisations, patching KEV-listed vulnerabilities with high CVSS became a "proof of diligence" for boards and auditors. This created a **false sense of closure** and diverted attention from more complex, structural issues.

3. **Neglect of negative space.**

    - KEV and EPSS can indicate where attackers are active; they cannot show where attackers will be active next, nor where the **absence of logging** or visibility hides entire classes of problems.
    - Treating "no KEV/EPSS hit here" as "no risk here" is precisely the kind of negative-space error OSPCRM is designed to prevent.

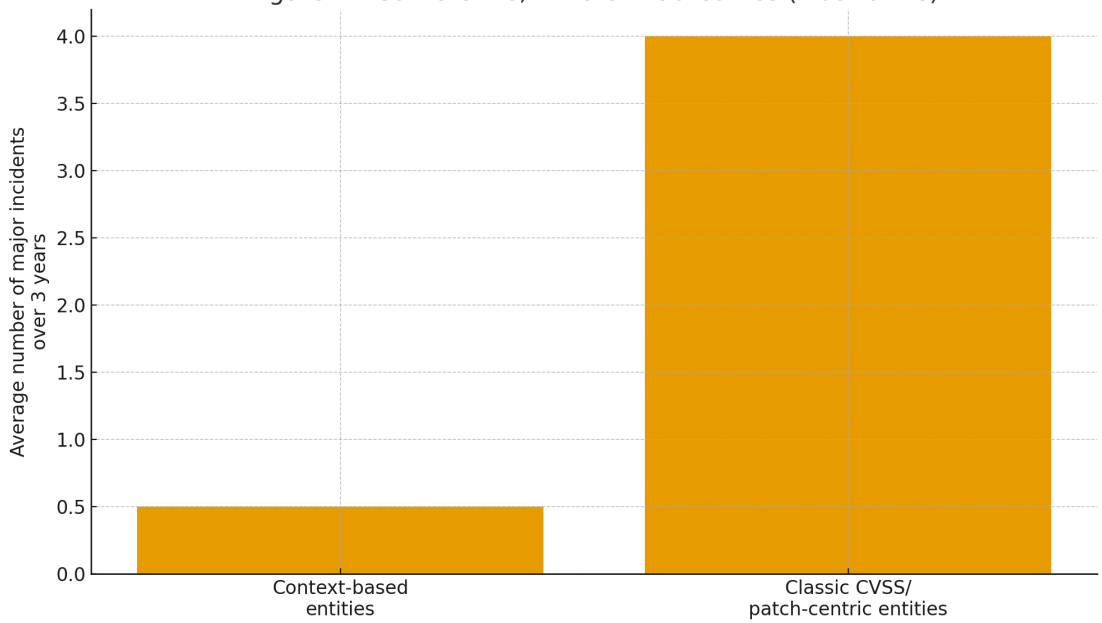
Same CVEs, same tools, radically different outcomes

Over the last years, PASC has observed a recurring pattern inside large international groups, including Fortune-listed institutions. Within the same group, entities share almost identical technical stacks: same CVE profile, same infrastructure family, same vendors and often overlapping IP ranges. Yet their incident histories diverge sharply.

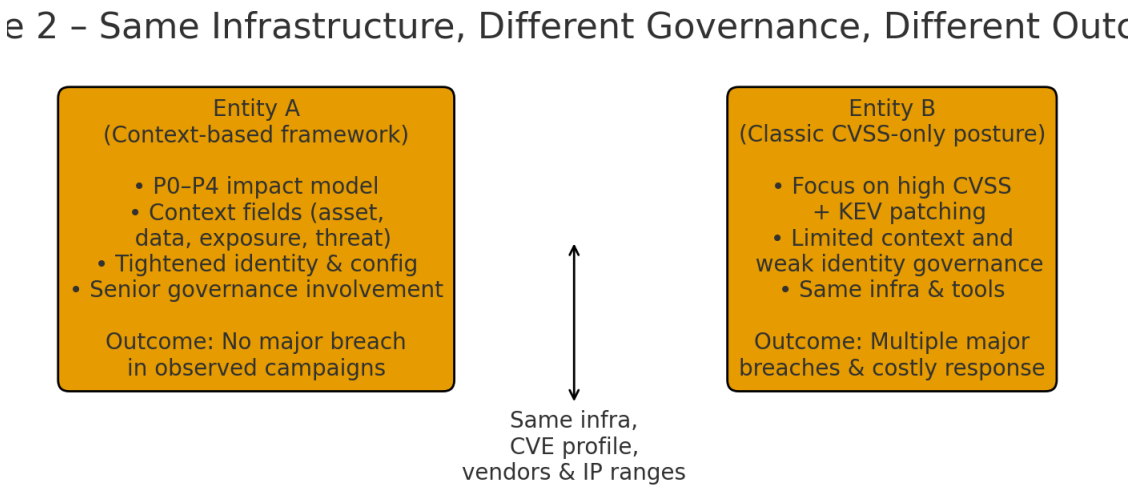
In one global financial group, the business unit that adopted a **context-based, impact-driven risk model** (P0–P4 impact, enriched context fields, and structural governance indicators) used the standard patch tooling but changed how it **interpreted** and **prioritised** signals. It tightened identity and configuration, re-scoped critical permissions and simulated realistic attack paths ahead of time. As a result, when sector-wide campaigns hit the group, this unit largely **shrugged off the top threats**: no major breach, no prolonged business interruption.

Sister entities in the same group, operating on the same CVE profile and infrastructure but still relying on **classic "patch the highest CVSS" playbooks**, were repeatedly exposed. They experienced significant breaches, prolonged investigations and expensive remediation programmes, despite showing "good numbers" on patch SLAs and KEV coverage.

Figure 1 – Same CVEs, Different Outcomes (Illustrative)



A similar pattern appeared in a global industrial group with both manufacturing and financial services affiliates. The core group was breached via exposed components on shared infrastructure. Yet one national finance subsidiary, which had proactively **hardened configuration and access paths** using a context-based framework, was not breached—even though it was running the same software versions, with the same nominal vulnerabilities and overlapping IP ranges. The difference lay not in the scanners but in **how governance interpreted and acted on the findings**.



These case patterns repeat year after year:

- Entities that treat CVSS/KEV as **inputs into a contextual, impact-driven model**, and adjust identity, configuration and governance accordingly, consistently absorb or avoid the worst incidents.
- Entities that treat CVSS/KEV and patch counts as **the model itself** continue to be surprised by large-scale breaches on the same infrastructure.

From a PASC perspective, this is the clearest available evidence that **risk is decided by context, governance and workforce structure—not by CVE lists alone**.

---

4. Workforce, juniorisation and the "dashboard without depth" problem

By 2022, security operations centres and risk dashboards looked impressive: millions of events, AI-assisted correlation, colourful charts. The reality on the ground was often more fragile.

4.1 Juniorisation as a structural risk

- Critical detection and triage functions were frequently staffed by relatively junior analysts on rotating shifts, expected to make rapid judgements on complex events with limited time and limited access to senior architects or threat experts.
- Senior staff were stretched thin across architecture reviews, crisis response, audits and projects, leaving little space for deep mentoring, systematic threat modelling or long-term design work.

ORG-GOV treats this not as a moral failing but as a **measurable structural condition**:

- Ratio of senior to junior staff in key roles;
- Average tenure;
- Number of severe incidents per 12–24 months vs seniority balance;
- Existence (or absence) of structured mentoring and knowledge transfer.

4.2 Internalisation vs diverse expert ecosystems

- Some organisations sought to internalise nearly all security functions, in part to "reduce external dependency" and costs. In practice, this often led to **closed, self-referential ecosystems** with limited challenge to prevailing assumptions.
- Others deliberately cultivated ecosystems that combined internal teams with **independent senior experts, specialised boutiques, academic partners and community signals**.

Incident reviews from 2022 repeatedly show that the latter group:

- detected and understood complex scenarios earlier;
- avoided repeated mistakes;
- and provided more credible narratives to boards and regulators.

For PASC, the conclusion is clear: **diverse, senior ecosystems are not a luxury; they are a control**.

---

5. Remote and hybrid work in 2022: stabilised, but not neutral

By 2022, remote and hybrid work had stabilised as normal operating modes. Their impact on risk depended chiefly on governance quality:

- Where identity, device trust, network segmentation and logging were aligned with remote realities, there was no inherent increase in breach frequency; in some cases, distributed workforces even led to faster detection of certain anomalies.
- Where remote access had been bolted onto pre-existing designs as a "temporary measure" and never revisited, 2022 incidents showed **elevated credential abuse, uncontrolled lateral movement and longer detection times**.

PASC's reading is that **remote/hybrid is not a risk category, it is a multiplier**: it magnifies strengths and weaknesses in identity, architecture and observability.

---

6. PASC lens: what 2022 proves about predictive standards

The patterns from 2022 strongly validate the core assumptions behind PASC standards:

- Hygiene metrics (CVSS, KEV, EPSS, patch rates, control inventories) are essential, but **cannot explain** why similar-looking organisations have radically different incident histories.
- The difference emerges when we look at **impact modelling, context richness, incident-linked performance and governance/ workforce health**.

PASC's standards provide a minimal predictive spine:

- **OSPCRM** for cyber risk:
    - P0–P4 impact scale (business consequences, not just technical severity);
    - mandatory context fields (criticality, data sensitivity, exposure, threat activity, resilience controls);
    - incident-linked metrics (FNR, P0/P1 precision).
- **ORG-GOV** for structural health:
    - indicators of seniority balance, turnover, independence and escalation power;
    - measures of workload, burnout risk and treatment of staff and externals.

For 2022 and the upcoming 2023 period, PASC recommends that organisations implement at least the following:

1. **Decouple impact from CVSS.**
   Use a P0–P4 impact scale and report serious risks in those terms, with CVSS as one input, not the headline.

2. **Attach a minimal context spine to serious items.**
   For every P1/P2-level finding or incident, record: the asset/service, criticality, data sensitivity, exposure, threat activity (including KEV/EPSS), and resilience controls.

3. **Track FNR and P0/P1 precision over time.**
   Treat these as core KPIs for the security function, alongside classical operational metrics.

4. **Add at least two ORG-GOV indicators.**
   For example: seniority ratio in security/architecture, and annual turnover in key roles. Discuss them with the board as **risk factors**, not HR trivia.

---

7. PASC priorities and advice for 2023

Looking forward from early 2023, PASC would highlight the following priorities:

1. **Make KEV/EPSS your "threat activity layer", not your whole model.**
   - Use KEV/EPSS to enrich context and refine prioritisation, but never as proof of safety.
   - Explicitly track which incidents in 2022 originated from issues *not* visible in KEV/EPSS/CVSS.
2. **Bring identity and architecture to the board table.**
   - Present a concise map of identity providers, critical trust relationships and cloud control planes, with their associated P0–P4 risks.
   - Explain concrete 2022 incidents (internal or sector-wide) in those terms.
3. **Measure and discuss workforce structure.**
   - Put at least basic ORG-GOV indicators in front of the board: seniority ratio, turnover, burnout risk signals, independence of the security function.

- Make it explicit that persistent juniorisation and churn is itself a risk.

4. **Pilot OSPCRM and ORG-GOV in one or two critical domains.**
    - For example: payments, core banking, clinical systems, or national digital identity.
    - Apply the P0–P4 scale, context fields, and FNR/P0–P1 metrics for 6–12 months and compare with classical dashboards.
5. **In Africa: move from imported checklists to co-authored standards.**
    - Use PASC standards as a bridge between international requirements (ISO, NIST, regional regulations) and local realities.
    - Document early African implementations as case studies, to build evidence that the continent can be a **co-author** of standards, not just a consumer.

---

8. Working with PASC

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 the 2023 cycle, 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 data-sharing initiatives**, especially those measuring FNR, P0/P1 precision and ORG-GOV indicators across sectors.
3. **Seek accreditation or certification** for tools, services and training programmes that demonstrably align with PASC profiles and improve predictive performance.
4. **Collaborate on Africa-rooted extensions**, including standards for public safety, medical safety and assessment of governance for high political or 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.