ResilientTech Advisors

September 2025

THE 2025 VZ DBIR PARADOXES CISOS NEED TO DECODE

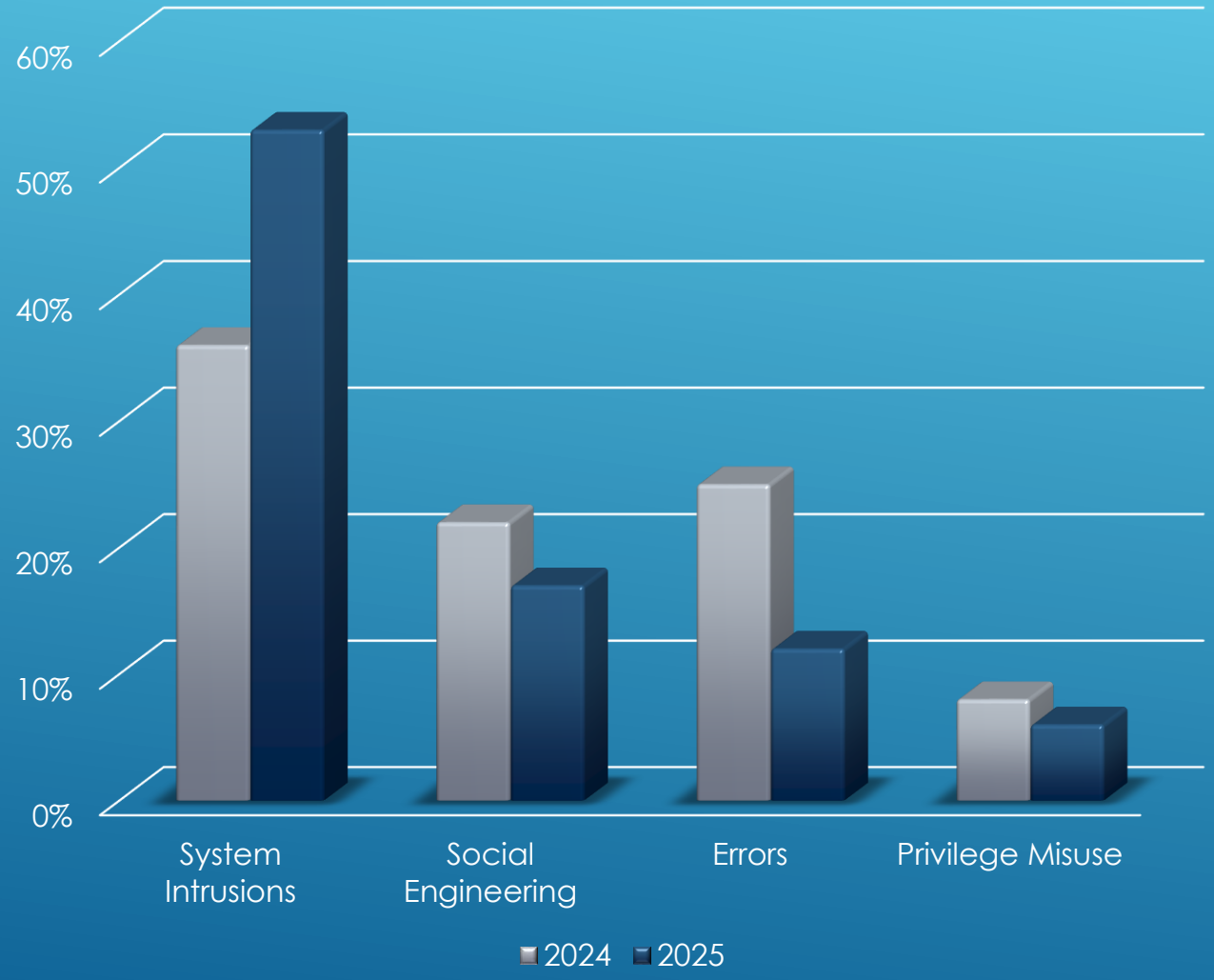
When the Data Disproves Conventional Wisdom

WHY THIS MATTERS

- **Verizon's Data Breach Investigation Report (DBIR)** is one of the most cited breach datasets in cybersecurity
- This year's report **contains surprises** that contradict conventional wisdom.
- To lead effectively, **CISOs need to read past the charts.**

Verizon 2025 Data Breach Investigation Report

Shifting Breach Patterns: 2024 → 2025



THE CHART TELLS ONE STORY. THE DEEPER READ TELLS ANOTHER.

These numbers make it look like some risks are shrinking. They create the **paradoxes** we'll explore next.

UNDERSTANDING THE DBIR SHIFTS

DBIR data can shift year to year due to

- Contributor bias & sampling changes
- Reclassification of patterns (e.g., ransomware-only extortion)
- Evolving attacker tactics that change category weightings

Examples

Error pattern decline may reflect relative mathematical effects & changes in contributor datasets.

Social engineering appears smaller because intrusions surged while attackers shifted toward AI-enabled techniques.

Takeaway: These aren't contradictions. They're shifts that require context.

We call them paradoxes because they challenge conventional wisdom, not because the data is wrong

PARADOX #1 – SOCIAL ENGINEERING SHRINKS

2024: 22% → 2025: 17%

Conventional wisdom: **With AI deepfakes, phishing should be increasing.**

Reality: Social engineering is still rampant; **however, it was dwarfed by the surge in intrusions.**

PARADOX #2 – ERRORS SHRINK

2024: 25% → 2025: 12%

Conventional wisdom: With SaaS sprawl, **errors should be rising**

Reality: Errors were **buried under intrusion growth**

In the DBIR context, "errors" refers to unintentional human mistakes that lead to data breaches or security incidents.

Common error types:

- Misconfigured databases or cloud storage (leaving S3 buckets open)
- Sending sensitive data to wrong recipients
- Publishing confidential information accidentally
- Misconfigured access controls or permissions
- Lost or stolen devices/laptops
- Improper disposal of sensitive data
- Publishing internal data to public repositories (like GitHub)
- Email misdelivery or CC/BCC mistakes

PARADOX #3 – PRIVILEGE MISUSE SHRINKS

2024: 8% → 2025: 6%

Hype: Insider risk is often portrayed as the next big, growing threat.

Reality: DBIR shows insider-driven breaches were a smaller share, while **external exploitation accelerated.**

THE DRIVER BEHIND THE PARADOXES

System Intrusions exploded

- 2024: 36%
- **2025: 53%**

Attackers are:

- Exploiting **edge devices**
- Chaining **vulnerabilities**
- Using **stolen credentials** at scale

Result: Apparent declines are relative. **Intrusions are growing faster than everything else combined.**

THE HUMAN ELEMENT GOES BEYOND SOCIAL ENGINEERING

DBIR: **~60% of breaches involve a human factor**

- Phishing clicks
- Password reuse
- System misconfigurations
- Privilege misuse

Even inside "system intrusions," humans play a role:

- Credential theft & misuse
- Help desk resets
- Weak passwords & patch hygiene

Humans remain the majority factor, but **exploit-driven automation is accelerating.**

LEADERSHIP LESSON

Don’t misread shrinking slices

- Smaller percentages ≠ smaller problems.

Prepare for the fronts that matter most

- Human-driven compromise is steady.
- Exploit-driven compromise is rising fast.

Educate with nuance

- Boardrooms need to hear that both realities are true.
- Picking one narrative leaves blind spots

WHAT CISOS SHOULD DO NOW

Rebalance roadmaps

Example: Dual investment - 60% human controls, 40% technical acceleration

Elevate help desk defenses

Risk-tiered verification, training, escalation playbooks,

Push for exploit readiness

Faster patch cadence, zero-day monitoring, stronger vulnerability intelligence

Tell the full story

Human element + technical surge = two fronts, one battle[1]

1: In 2025, the story is two fronts — human & technical. In other years or environments, the mix may differ.

THE RESILIENCE FRAME

Resilience

…is **balance**

…requires **a clear picture** of the threats & risks that matter most in your environment

…**integrates defenses** across human, technical, & organizational threats

ResilientTech Advisors

September 2025

We partner with CISOs to:

- ✓ **Decode** threat intelligence into practical strategy.
- ✓ **Translate** complexity into board-level language that drives alignment.
- ✓ **Design** roadmaps that balance awareness, identity, & intrusion defense.
- ✓ **Build** dual-front resilience: human-centric + exploit-centric defenses.

ResilientTech Advisors
inquiries@resilienttechadvisors.com