Cybersecurity

WELLS FARGO

The Accountability Trap

How blaming users hides the real cyber risk

Sarah Gosler, Managing Directior - Head of Cyber Human Defense

How an overempahasis on individual actions can limit what organizations learn from cyber incidents

April 2026

Summary

In the aftermath of a cyber incident, the first question almost always sounds the same:

Why did they click?

On its face, the question is reasonable. In cybersecurity, as in any risk discipline, understanding the immediate point of failure matters. Individual actions do play a role, and accountability is part of any serious post-incident review.

The problem arises when that question becomes the conclusion rather than the starting point.

When complex incidents are framed primarily around a single human action, organizations unintentionally narrow their field of view. Attention gravitates toward what one person missed, rather than toward the conditions that shaped the decision. Investigations close quickly. Corrective actions feel decisive. And yet the same types of incidents recur; often in different teams, under slightly different circumstances.

Over time, this pattern limits learning. And in a threat environment increasingly shaped by human behavior, that limitation carries real risk.

When explanation feels like resolution

Post-incident reviews tend to follow a familiar structure. A timeline is reconstructed. The moment of compromise is identified. The human action closest to that moment becomes the focal point. Controls, tools, and processes are reviewed, often through the lens of why they failed to stop one individual from making one decision.

From there, remediation follows predictable paths: refreshed training, new reminders, updated banners, tighter policies. None of these are inherently wrong. But when they are deployed as primary fixes, they can create a false sense of closure.

The organization believes it has addressed the root cause, when in reality it has treated a symptom.

Most successful cyber intrusions today are not the result of ignorance or recklessness. They are the predictable outcome of how work actually happens inside organizations operating under constant pressure...balancing speed, service, authority, and risk.

Understanding that distinction matters.

The role of context, not carelessness

Many employees who fall victim to social engineering attacks are well trained. They know what phishing looks like. They understand the rules. In regulated environments, they are often reminded of those rules frequently.

What they are navigating in the moment is not from a complete lack of awareness, but competing priorities.

They are responding to requests that align with business rhythms, come from familiar sources, and arrive at moments when hesitation carries perceived cost. Attackers understand these dynamics exceptionally well. They design interactions that fit seamlessly into existing workflows, exploiting normal patterns rather than breaking them.

In that context, human judgment behaves exactly as it is designed to behave...favoring continuity, cooperation, and resolution.

Treating that response as individual failure obscures the broader signal.

How narrow framing limits learning

Cybersecurity is now confronting the same challenge.

When incident analysis centers too tightly on individual action, several things tend to happen. Patterns across incidents are missed. Cultural pressures, such as reluctance to slow the business or challenge perceived authority, go unexamined. And teams receive the implicit message that being deceived is worse than speaking up.

That last effect is particularly costly.

Blame-oriented framing suppresses early reporting. Delayed escalation increases dwell time and blast radius. Small incidents become larger ones, not because defenses are absent, but because signals arrive too late.

The framing intended to reinforce accountability can, unintentionally, increase exposure.

What attackers are really exploiting

Adversaries are not guessing at human behavior. They study it.

They observe how approvals work, how vendors communicate, how executives delegate, how urgency is signaled, and how decisions are made under pressure. They exploit assumptions about what “normal” looks like inside an organization.

From that perspective, the human is not a weak link. It is a consistent one.

Recognizing this does not absolve responsibility. It reframes where insight lives.

Reframing the first question

Human-centric cyber defense does not mean expecting people to be perfect. It means recognizing that behavior is shaped by environment, incentives, and constraints...and designing defenses with those realities in mind.

That shift begins with inquiry.

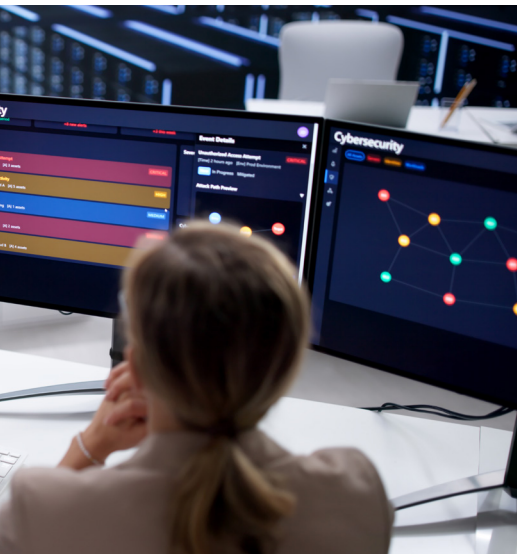
Instead of stopping at "Why did they click?", organizations that learn the most ask additional questions:

- Where does urgency routinely override verification?
- Which roles are asked to make high-risk decisions with limited context?
- How is trust signaled, implicitly or explicitly?
- What behaviors are discouraged in practice, even if policies say otherwise?

These questions are harder. They do not yield simple answers or quick fixes. But they surface risks that training alone cannot address.

Most security leaders recognize this intellectually. The challenge is operationalizing it consistently, especially under budgetary and business constraints. The opportunity lies in using incidents not just as moments of correction, but as sources of organizational intelligence.

Incidents as signals, not just failures



Every cyber incident reveals something, not only about an attacker's technique, but about how the organization functions under stress.

Organizations that broaden their inquiry tend to see tangible benefits. Reporting improves. Containment accelerates. Repeat incidents decline, not because attacks stop, but because learning compounds.

People stop being treated solely as liabilities and start being recognized as sensors within the system.

That shift does not weaken accountability. It strengthens resilience.

Asking a better first question

The most important moment in an incident response process may be the very first question leadership asks.

Not “Who made the mistake?”

But “What conditions made this outcome likely, and what does that tell us about how our organization operates under pressure?”

In a threat landscape increasingly shaped by psychology, that question can make the difference between repeating familiar failures and building defenses that evolve as fast as the attacks themselves.