Cybersecurity Doesn't Fail Because We Don't Know Enough. It Fails Because We Become Too Certain About What We Think We Know.

By: Jaiz Anuar

7 June 2026 · Cybersecurity · Leadership · Digital Trust · 8 min read

The biggest cybersecurity failures rarely begin with ignorance. They begin with confidence.

Every major cyber incident is followed by a familiar question.

"How did nobody see this coming?"

The uncomfortable answer is that, quite often, somebody did.

The indicators existed. The risks had been documented. Audit findings had been raised. Engineers had voiced concerns. Threat intelligence had warned about similar attack patterns elsewhere.

Knowledge was not the problem.

The problem was certainty.

Knowledge Is Growing Faster Than Ever

Today's cybersecurity professionals have access to more information than at any other point in history. Every day brings new threat reports, vulnerability disclosures, security frameworks, maturity models, industry guidance, and technology innovations.

The challenge is no longer finding information. The challenge is deciding which information still deserves to be questioned.

Ironically, the more experience organisations accumulate, the easier it becomes to confuse familiarity with certainty.

The Most Dangerous Sentence In Cybersecurity

Every organisation has its version of this sentence.

"We've always done it this way."

It sounds harmless. It sounds practical. It sounds efficient.

But hidden inside those six words is an assumption that tomorrow will behave like yesterday.

Cybersecurity rarely rewards that assumption.

Attackers evolve. Technology evolves. Business models evolve. Artificial intelligence evolves. Cloud platforms evolve. Supply chains evolve.

Yet many organisations continue defending assumptions that were designed for a completely different environment.

Certainty Creates Blind Spots

Confidence is valuable. Overconfidence is dangerous.

The organisation becomes convinced that its firewall is sufficient. Its privileged accounts are properly managed. Its cloud environment is secure. Its third-party suppliers are trustworthy. Its monitoring covers everything important.

Eventually, questioning stops.

And once questioning stops, learning usually stops as well.

Cybersecurity does not fail overnight. It gradually becomes less curious.

Experience Can Become A Liability

Experience is one of the greatest strengths a cybersecurity professional can possess.

It is also one of the easiest ways to develop invisible assumptions.

Experienced professionals naturally recognise patterns. That helps them make faster decisions.

But attackers study those same patterns.

The most sophisticated adversaries rarely defeat organisations by exploiting what security teams do not know. They exploit what security teams believe cannot happen.

Good Security Leaders Doubt Their Own Assumptions

The best security leaders are rarely the most confident people in the room.

They are usually the ones asking uncomfortable questions.

What assumptions have we never tested?

Which controls have we trusted for years without verification?

What would happen if our most trusted administrator's account were compromised today?

If our monitoring failed, how long would it take us to notice?

Could our own architecture be creating the very risk we believe it prevents?

These questions are not signs of weakness. They are signs of professional humility.

Humility Is A Security Control

Perhaps humility should be recognised as one of cybersecurity's most overlooked controls.

Humility encourages continuous validation. It encourages peer review. It encourages architecture reviews. It encourages red teaming. It encourages threat modelling. It encourages asking, "What if we are wrong?"

Most importantly, humility prevents confidence from becoming complacency.

Questions Worth Asking

Which security assumptions have we not challenged in the past two years?

What do we believe is impossible simply because it has never happened?

Are our security decisions based on evidence, or familiarity?

Have we confused compliance with confidence?

If our biggest assumption proved false tomorrow, would we recognise it before an attacker did?

Final Thought

Cybersecurity is often described as a battle against attackers.

Perhaps it is also a battle against our own certainty.

Technology will continue to evolve. Threats will continue to evolve. Artificial intelligence will continue to evolve.

The organisations most likely to adapt will not necessarily be those that know the most.

They will be those that remain willing to question what they think they already know.

Because cybersecurity rarely fails through ignorance.

It fails when confidence quietly replaces curiosity.

Question assumptions. Share knowledge. Build trust.