The Most Dangerous Incidents Start as Normal Days

By: Jaiz Anuar

29 June 2026 · Cybersecurity · Operational Resilience · 7 min read

Most major incidents do not begin with alarms. They begin quietly: as a normal shift, a routine operation, or a familiar task that has been performed hundreds of times before.

They do not begin with panic, flashing red dashboards, emergency meetings, or declarations of crisis.

That is precisely what makes them dangerous.

When everything feels normal, people naturally lower their guard.

The Illusion of Familiarity

Experience is valuable. Familiarity is comforting. Routine creates efficiency.

But routine can also create assumptions: “We have done this before.” “This has never caused problems.” “We know how this works.” “The risk is low.”

Over time, these assumptions become embedded into operations. Verification becomes less frequent. Challenges become less common. Controls become expectations rather than actions.

Eventually, the organisation stops actively managing risk and starts relying on familiarity instead. That is often where the conditions for major incidents begin to form.

Incidents Rarely Start With the Final Mistake

When investigations are conducted, there is often a temptation to focus on the final action: the final command executed, the final approval granted, the final procedure missed, or the final decision made.

But major incidents rarely originate from the last mistake. The last mistake is usually just the final link in a chain that started much earlier.

A missed verification. An undocumented workaround. An overloaded operator. An outdated procedure. A delayed maintenance activity. A known issue accepted as normal.

Each decision may appear reasonable in isolation. Together, they create the conditions for failure.

Normalisation of Deviation

One of the most dangerous behaviours in any organisation is the gradual acceptance of conditions that were once considered unacceptable.

The first exception feels uncomfortable. The second exception feels manageable. The tenth exception becomes the new standard.

Over time, temporary workarounds become permanent solutions. Manual processes replace intended controls. Teams become accustomed to operating outside design assumptions.

The organisation adapts to risk instead of removing it.

This phenomenon has been observed repeatedly across aviation, healthcare, manufacturing, military operations, cloud engineering, and cybersecurity. The industry changes; human behaviour rarely does.

The Problem With Successful Failure

One of the most deceptive operational risks is what some organisations unknowingly reward: failure that succeeds.

The patch applied directly in production because there was no time. The firewall change that bypassed review because the business needed urgency. The access request approved because the executive was travelling. The undocumented workaround that kept the service running.

Nothing bad happened. The operation continued. The organisation moved forward. The shortcut appears justified.

Unfortunately, successful shortcuts teach organisations the wrong lesson. They teach that controls are optional when pressure increases.

The danger is not the first exception. The danger is when exceptions become the operating model.

Near Misses Are Gifts

High-reliability organisations understand something many others do not: near misses are free lessons.

An outage that almost happened. A change that almost failed. An email sent to the wrong recipient but recalled in time. An administrator account accidentally granted excessive privileges. A production deployment caught minutes before execution.

These are opportunities, because every major incident was once a near miss that nobody recognised.

The organisations that learn fastest are often the ones willing to investigate events that never became incidents.

Cybersecurity Has the Same Problem

Cybersecurity teams often believe incidents begin when the alert arrives: the ransomware encryption starts, the account becomes compromised, the malware executes, or the data is exfiltrated.

In reality, the incident usually started much earlier. An exception was granted. A patch was delayed. A privileged account remained active. An unsupported server remained online. A monitoring gap was accepted temporarily. An operational risk became normal business practice.

By the time the SOC sees the alert, the conditions for compromise may have existed for months or years.

Building Organisations That Fail Safely

No organisation can eliminate mistakes. Humans will make errors. Technology will fail. Processes will break.

The objective is not perfection. The objective is resilience.

Resilient organisations create environments where:

assumptions can be challenged,

junior staff can stop an operation,

unusual conditions are escalated early,

near misses are investigated seriously,

exceptions remain exceptions,

controls are tested under pressure, and

learning happens without blame.

The goal is not to create organisations that never fail. The goal is to create organisations that fail safely and recover quickly.

Final Thought

Major incidents rarely announce their arrival. They usually arrive disguised as ordinary work: a routine change, a familiar procedure, a temporary exception, or a normal day.

That is why operational resilience is not tested during extraordinary moments. It is tested during ordinary ones.

Because the most dangerous incidents do not start with chaos. They start when everyone believes nothing unusual is happening.