The Quiet Beginning of a Cyber Incident: What Leaders Should Be Asking Now

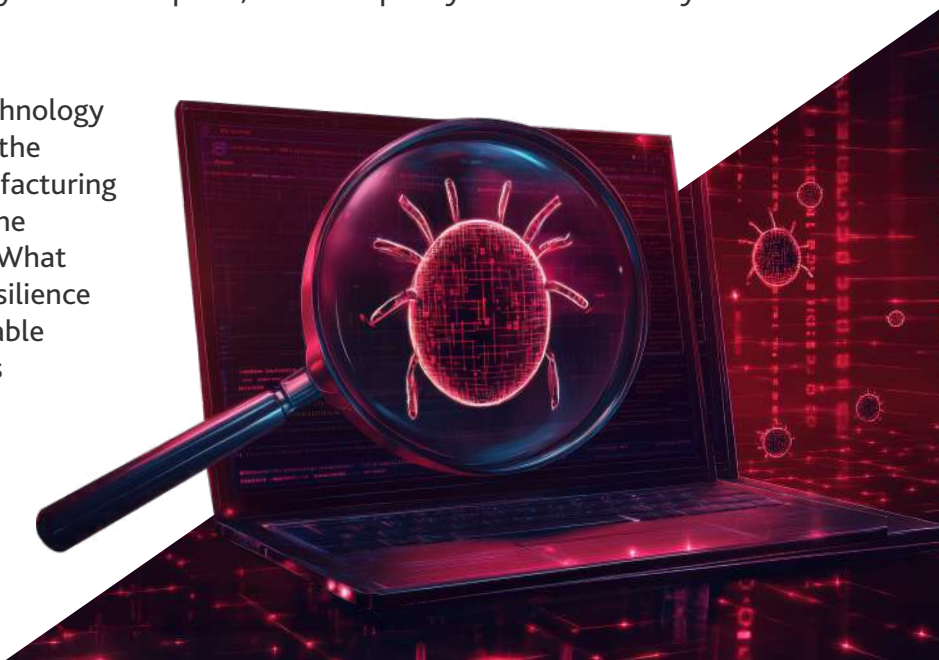
Periods of geopolitical tension, economic disruption and wider global uncertainty tend to sharpen cyber risk. When leadership attention is stretched and operations are under pressure, cyber adversaries often see opportunity. Quiet probing increases. Phishing becomes more convincing. Exposed systems are tested. Third-party pathways are explored. Most attempts fail. The ones that succeed may remain unseen for longer than expected.

Most cyber incidents do not begin with alarms. They begin quietly: compromised credential works, a familiar looking connection is accepted, and business carries on as usual. Nothing appears broken. For a while, no one notices.

That is what makes the early stage of a cyber incident so dangerous. The attacker is not yet disrupting operation, they are learning. They observe how systems connect, which accounts carry privilege, and where the organisation is most dependent on technology. By the time systems lock, data disappears, or services fail, the intruder may already understand the environment better than the organisation understands the threat.

Many organisations take comfort in the fact that they have invested in cybersecurity tools. That is necessary, but it is not the same as readiness. Real incidents do not test whether controls exist on paper; they test whether the organisation can recognise that something is wrong early enough to act. The more revealing question is not whether security tools are in place, but how quickly abnormal activity would be identified, responded to and contained.

This is where cyber stops being only a technology issue. Once critical systems are affected, the consequences become operational. Manufacturing slows. Transactions fail. Customers feel the disruption. Reputational pressure builds. What looked like a security event becomes a resilience event. The difference between a manageable incident and a business crisis often comes down to one factor: **Speed of detection.**



The challenge is no longer confined within organisational walls. Modern businesses operate through cloud platforms, managed service providers, software vendors and digitally integrated supply chains. Every connection improves efficiency, but every connection also extends exposure. Increasingly, attackers look for the weakest point in that wider ecosystem rather than the strongest point inside the organisation itself. In many cyber incidents, the entry point was not the organisation itself, but someone connected to it.

This is where the conversation begins to change. Less about what exists, and more about what is truly understood, validated, and under control today. From that point, the most useful questions are often the simplest and the hardest to answer with certainty

At this point, leadership teams should now be asking direct questions, less about what exists, and more about what is clearly understood and validated today:

- How often are we testing our ability to detect and respond to real-world attack scenarios, not just reviewing policies or controls
- Which systems, if disrupted without warning, would immediately affect our ability to operate and are we absolutely clear on that today?
- What gives you confidence that we would detect a real attack early, not based on reports, but based on something we've seen work?
- Where are we most exposed right now, and not last quarter, not in an audit report, but today?
- Which external party could create the biggest problem for us if they were compromised, are we aware and how comfortable are we with that exposure?
- Are we relying on the belief that our controls are working or do we have evidence that they have worked when it mattered?

These are not purely technical questions. They go to the heart of operational continuity, governance and leadership judgement. In an environment where cyber threats remain persistent and may intensify when the external world becomes more unstable, resilience depends less on confidence and more on clarity.

> ***If a cyber intrusion began quietly inside the organisation today, how confident are you that you would notice before the attacker decides it is time to act?***

Keshvinderjit Singh
Executive Director,
Cybersecurity and Privacy

T: +603 2616 2998
E: keshvin.s@bdo.my

www.bdo.my