evolution SYSTEMS

FIVE QUESTIONS

YOUR LEADERSHIP WILL ASK ABOUT RECOVERY

AND WHAT EACH ANSWER REVEALS ABOUT YOUR POSTURE

When recovery becomes a leadership conversation, it usually happens at the worst possible moment. An incident occurs, an insurer asks at renewal, a compliance audit surfaces the topic, or an executive reads about a ransomware attack and asks the question in the next meeting. The technology leader in the room is expected to answer with confidence, not with approximations.

This brief covers the five questions most likely to come from a CEO, COO, executive team, or ownership group when recovery is on the agenda. For each: what the question is really asking, what the response needs to cover, and the follow-up you need to be ready for.

QUESTION 1: HOW QUICKLY CAN WE RECOVER IF SYSTEMS GO WN?

What they are actually asking: **Do you have a number, and have you tested it?**

What your response needs to cover: A specific recovery time objective for critical systems, how that figure was established, and when it was last validated under realistic conditions. The distinction between restoring a single file and recovering the systems the business depends on - because that distinction will come up.

The follow-up you need to be ready for: The conversation moves from *"how long"* to *"how do you know"*. An untested number does not survive that follow-up. In a regulated environment or during an actual incident, the gap between an assumed figure and a validated one becomes the story.

QUESTION 2: WHEN DID WE LAST TEST RECOVERY?

What they are actually asking: **Is recovery proven, or assumed?**

What your response needs to cover: A specific date, a description of what was tested - which systems, what scale, what conditions - and confirmation that outcomes were documented. Frequency matters. Annual testing of a single system does not constitute a validated recovery capability for a complex environment.

The follow-up you need to be ready for: *"We test regularly"* invites the follow-up nobody wants - what exactly was tested, and what did it cover. An answer that cannot be specific about scope and outcomes will not hold up, and leadership will notice.

QUESTION 3: ARE OUR BACKUPS PROTECTED FROM A RANSOMWARE ATTACK?

What they are actually asking: **Could an attacker compromise our ability to recover while they're attacking our systems?**

What your response needs to cover: Whether the backup environment is logically isolated from the production network, whether immutable copies exist that cannot be deleted or encrypted, and whether access to backup management is protected separately from production credentials.

The follow-up you need to be ready for: This question has a technical answer and a strategic one. Leadership may not understand the architecture, but they will understand the implication - if the backups can be taken out alongside production systems, the organisation has no fallback. Being unable to answer specifically signals that the question has not been asked internally either.

QUESTION 4: WHO IS ACCOUNTABLE DURING A RECOVERY EVENT?

What they are actually asking: **Does our recovery posture exist on paper, or can we prove it?**

What your response needs to cover: That recovery tests are documented with scope, timing, and outcomes recorded, that the backup architecture can be described in terms an insurer or auditor will accept, and that evidence is available on request rather than assembled under pressure.

The follow-up you need to be ready for: Insurers now ask specific questions about immutability, isolation, and tested recovery at renewal. Assembling evidence after the question has been asked is a different position to having it ready. The distinction between the two is increasingly reflected in premiums, coverage terms, and renewal outcomes.

QUESTION 5: CAN WE DEMONSTRATE THIS TO OUR INSURER OR AUDITOR?

What they are actually asking: **Is there a defined owner, or will this be resolved through improvisation?**

What your response needs to cover: The accountable role, the escalation path, and confirmation that a recovery process has been exercised, not just documented. Accountability is not the same as technical capability, and the distinction will surface quickly under pressure.

The follow-up you need to be ready for: If the answer involves more than one name or includes any version of *"it depends"*, the follow-up is immediate - so who makes the call? An organisation that cannot answer that question in advance will be answering it for the first time during an incident.

If any of these questions gave you pause, now is the right time to address them - before an incident makes that urgent.

Suite 6.04 247 Coward St, Mascot NSW 2020 www.evolutionsystems.com.au sales@evolutionsystems.com.au