Integrity360

your security in mind

Q&A follow-up

Under fire: The anatomy of Incident Response

May 28th, 2026

1. Question: What makes an incident major?

   Answer: Critical systems affected, admin account compromised, ransomware, multiple devices compromised, sensitive data exposed and lack of coverage from security software.

2. Question: Common mistakes organisations make when responding to a breach?

Answer: Business pushback – "you can't shut down systems; we need operations running". First mistake many organisations make is to try and stay operational while containing ransomware. A good IR director will communicate the risks of containment vs business continuity, using experience as persuasion. Putting a plaster on doesn't actually fix the problem.

3. Question: How do you decide when to contain vs continue monitoring an attacker?

Answer: Risk based judgement based on multiple triggers. Often you want to contain if there is active exfiltration or destructive activity detected like ransomware or access to critical systems. You might monitor instead of containing if you're tracking lateral movement paths early on in the attack chain and have strong detection coverage and containment confidence.

4. Question: How is misinformation or speculation handled during an incident?

Answer: Control the narrative early and communicate frequently even if there is no change. Separate facts from hypothesis (for example "confirmed"). Actively monitor internal and external noise.

5. Question: How is that Priv Escalation and lateral movement was not picked up? What rules would need to be in place to detect disabling of AV via GPO.

Answer: The indicators were there but it had a low energy rating due to the attacker using LOTL techniques. To detect against AV being disabled via GPO, watch for registry key modifications, GPO event logs for changes, behavioural activity of gpsvc and EDR specific detections.