Incident Severity Assessment Matrix

Grade an incident by impact and risk, not by how technically interesting it is. Any factor can promote an incident to a higher level.

The four levels

Level	Meaning	Response
CRITICAL	Business-wide impact, or the attacker holds the keys.	Full response now. Executive-led. External help. Report as required.
HIGH	Confirmed compromise of an account or important system.	Urgent, coordinated response the same day.
NORMAL	Contained and understood.	Work through in normal hours. Document it.
LOW	Blocked, benign or a false positive.	Record it and move on.

Assessment factors

Factor	Ask yourself
Availability	How much of the business is disrupted?
Confidentiality	Could data have been seen or taken?
Integrity	Could data or systems have been altered?
Scale	How many users, devices and sites are affected?
Privileged access	Are admin or identity accounts involved?
Critical systems	Are business-critical systems in scope?
Personal data	Is personal data known or suspected to be involved?
Financial impact	Is money or payment fraud in play?
Regulatory	Are there reporting duties (ICO, sector)?
Customer / safety	Are customers or anyone's safety affected?
Active attacker	Is the attacker still demonstrably present?
Scope	How far has it spread across the organisation?

Worked examples

Level	Examples
CRITICAL	Active ransomware across multiple systems; confirmed privileged-account takeover; confirmed large-scale data theft; major payment fraud in progress; compromise of the identity platform; attacker still active.
HIGH	Confirmed single Microsoft 365 account compromise; malware on an important server or endpoint; suspected exfiltration needing urgent investigation; supplier breach giving meaningful

	access; targeted phishing with credentials used.
NORMAL	A single, already-isolated endpoint infection; a suspicious login to check; a lost device protected by encryption and remote wipe.
LOW	A blocked or reported phishing email that was not clicked; a false-positive alert; a benign event logged for completeness.

> Context can promote any incident. A single laptop sounds Normal, until you learn it was unencrypted, signed in, and held the customer database. Set severity early, write it down, and change it as you learn more.