Kindus

What Is cyber incident response management?

Cyber incident response management is a process of planning, coordinating, and executing actions to detect, analyse, mitigate, and recover from cybersecurity incidents, ensuring effective response and minimising potential damage.

The three R's stratergy

Readiness

To ensure readiness, have 24/7 monitoring, a skilled team, and crisis simulations to assess your organisation's preparedness.

Response

Coordinate to avoid crisis and minimise losses.Communicate effectively, including through social media, to reassure stakeholders and protect reputation, and finances.

Recovery

The process to assess the incident's causes, evaluate the response's effectiveness, and extract valuable lessons for future improvement.

Why Is CIR needed?

To prepare for cyber-attacks and data breaches as they are inevitable. GDPR and NIS regulations require reporting within 72 hours to report breaches with substantial fines for non-compliance. Emphasising the need for a swift response.

What is a cyber security incident?

- Attempts to gain unauthorised access to a system/data.
- Malicious disruption and/or denial of service.
- The unauthorised use of systems and/or data.
- Modification of a system's firmware, software or hardware without the system owner's consent.