cdt360
by Curran Data Technologies

Assess Your Cyber Resilience in 5 Critical Steps

In today's ever-evolving threat landscape, fortifying your business against cyber-risks is paramount.
Our infographic is your trusted security roadmap, empowering you to strengthen your defenses against the lurking dangers in this digital world.

Achieve cyber resilience success with cdt360 by Curran Data Technologies

"Cyber resilience is the concept to help organizations as it looks at a wider scope where it comprises cybersecurity and business resilience. Cyber resilience can be defined as the organizations ability to withstand and/or quickly recover from cyber events that disrupt usual business operations."

Cyber Resilience

1: Prepare/Identify: Identify actions for when cyber event will occur:

Resilience address preparedness as a specific emergency management business function; but more importantly, as being impacted by numerous functions across organization. These may include asset management, human resources, strategic planning, financial management, information technology, and risk management.

2: Protect: Actions to mitigate damage or make assets an unattractive target:

The focus is to maintain assets' core function and ward off harm. Organizations plan for protection against specific threats or categories of threats. Resilience approaches the issue from a standpoint of taking reasonable protective actions, but having alternative capabilities as needed or ability to withstand disruption.

3: Detect: Focus on activities to rapidly identify an attack and ensure a timely response:

This stage is concerned with continuing to monitor network for other attack indicators related to that attack and making sure safeguards in place were effective. A critical downside of an organization spending so much time and effort trying to protect itself from attacks is that entity often fails to prepare for what to do when an attack succeeds.

4: Respond: A response plan clarifies action in case of an incident:

Organizations need a response plan that clearly tells people what to do when an incident occurs. An Incident Response Team should be established, with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned responsibility of declaring an incident, coordinating activities of response team, and communicating status reports to upper management.

5: Recover/Review: Review systems and plans to restore any data affected:

Critical to any resilient security strategy is recovery. This stage involves developing and implementing appropriate systems and plans to restore any data and services that may have been impacted during a cyber-attack. No matter the preparation and protection measures an organization implements, it may not be able to avoid certain types of attacks. Even if the response is quickly to a cyber breach, an attack may have consequences. No matter the outcome, organizations must be able to restore their people, processes, and systems as quickly as possible. An effective recovery depends on a clear and thorough recovery plan.