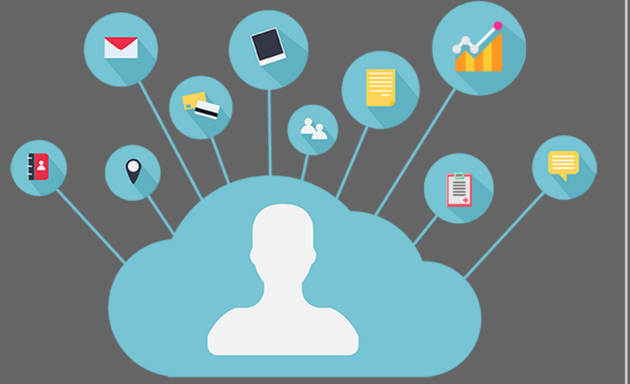
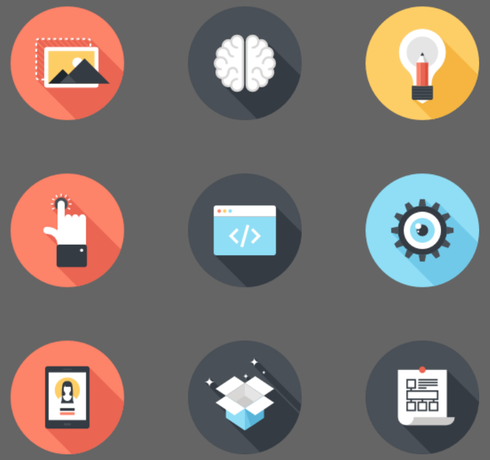
Cybersecurity Incident Response Plan

NESTOR™ Consulting

Struggling with?

- *Extending existing Business Continuity Plans to address Cybersecurity Incidents*
- *Identifying cyber threat scenarios using risk-based approach*
- *Identifying and using industry best practices*
- *Training employees to use the plans effectively*
- *Conducting refresher and regular exercises*





The solution?

CREST's 3 phase Cyber Security Incident Response Process provides support in the preparation, response, investigation and follow up of a Cyber Security incident

- *Prepare - Carry Out Threat Analysis and Criticality Assessment*
- *Plan - Identify cyber security incident, define objectives and investigate, act, recover systems, data & connectivity*
- *Follow Up - Carry out post incident review, Communicate and build on lessons learned, Update key information, controls and processes.*

How ?

The response plan presents key actions and tools to use after an incidence

- ✓ *Introduction & Purpose*
- ✓ *Event Handling*
- ✓ *Topology*
- ✓ *Team and War Room*
- ✓ *Response Plans*
- ✓ *Post-Incident Procedures*