COVID-19: Mitigating cyber risks during crisis

In light of the COVID-19 crisis, most organisations have invoked their business continuity plans (BCPs) across the globe. Working from Home requires remote access to your business network and it comes with its own set of challenges. Cyber criminals have begun taking advantage of unsuspecting users and tackling cyber-attacks in these challenging times could result in significant drain of resources. Key stakeholders / CXOs in the organisation will need to come together to navigate this comprehensively.

Activate Business Continuity strategy

- Devise and invoke a holistic BCP covering the pandemic scenario
- Take need-based necessary approvals from the top management.
- Define standard operating procedures (SOP) for employees to work from home using either company-specific communication channels or other channels such as MS Teams/Skype etc.

Prepare a cyber-attack defense model

- Take periodic backups and ensure proactive IT/ system patch updates to minimize cyber attacks.
- Identify, validate and authorize legitimate emails to avoid possible data breach or phishing attacks.
- Make employees aware of various phishing attacks prevalent today. Refer to Cert-In advisory for more details on COVID-19 related attacks.
- Stay up to date on various cyber attacks and with inputs from various security feeds, include them in a Cyber Threat Intelligence Model to identify trends and emerging risk/threat areas and provide timely warnings.

Stay updated on all legal, regulatory and technical developments

- Regulators are tightening controls and formulating new guidelines to tackle the growing number and complexity of cyber attacks.
- Stay updated on changes to data privacy, protection and cyber laws and regulations, as well as evolving risks and technical developments.

Secure your IT assets

- Update Policies and Procedures to support working remotely.
- Enable two-factor authentication for any connectivity to office network.
- Patch remote access supporting infrastructure with latest updates.
- Update antivirus, malware protection programmes, data leakage prevention (DLP), mobile device management (MDM) and other solutions on time to ensure endpoint security.
- Issue advisories to employees on relevant anti-virus or malware updates required to secure home networks

Ensure contract compliance

- Review vendor and third-party contracts.
- Understand key provisions and laws such as force majeure, data protection etc., to ascertain what likely event might trigger any of these provisions.

Considering the above pointers, all organisations will need to ponder about their Business Continuity Plans whether documented or undocumented, in a bid to enable remote working or work from home for their employees. As much as there is risk of operational continuity, loss of the organisation's or customer's data cannot be ignored. Further, due to sudden invocation of the BCPs, organisations might fail to meet their cyber / privacy obligations with their vendors, third-parties and business partners.

Contact a specialist

To find out how Grant Thornton can help you effectively plan and mitigate potential cyber risks to navigate these challenging times, contact **Aswin Vaidyanathan** on (+267) 76 237 135 / aswin.vaidyanathan@bw.gt.com, or **Sampath Kumar** on (+267) 74 194 825 / sampath.kumar@bw.gt.com.