KRESTON IL GROUP

COMSEC

New work-from-home reality creates opportunities for hackers and cyber risks for organizations

The attack surface is expanding and the climate for cyber-attacks is rapidly evolving as organizations scramble to move their activities online to protect their employees and maintain business continuity in the face of COVID-19.

With hackers looking to capitalize on opportunities in this new reality, organizations are exposed to a broader range of potential threats than ever before. As the organizations are forced to implement remote work solutions, it is vital for them to prioritize security and ensure that the front lines are impenetrable.

Within the framework of this changing environment, Comsec and Kreston have partnered to offer a range of innovative services to ensure that your organization is protected. These include:

Cyber Security COVID-19 Health Check

- Employee Computer Security Assessment
- Network Vulnerability Check
- Network Risk Assessment

Education and Awareness of management and employees

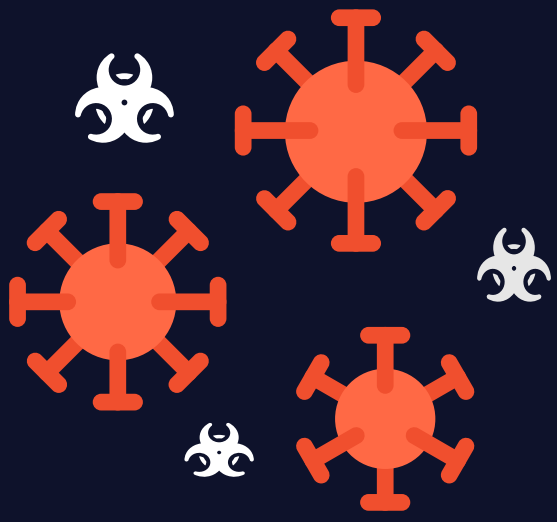
- Security Awareness Training videos
- Social Engineering – ransomeware, shutdown / business continuity
  - Phishing Awareness campaign
  - Phishing Simulation (offensive)
  - PCI DSS
- Business Continuity – DDoS simulation (offensive); mitigate risks and verify measures and policies to minimize costly downtime due to Distributed Denial of Service attacks
- Incident Response team to deal with breaches in real time, as the attack surface expanded due to high volume of remote connections
- Governance – Chief Information Security Officer (CISO-as-a-Service)

Privacy / GDPR COVID-19 Assessment

- GDPR Compliance – Prevent exposure of sensitive corporate and private data

CyberHat SOC – a 45-day free trial of 24/7 security operation monitoring

Collaboration System Implementation



Click here for more information