APPLE
GROW+H
PARTNERS
Healthy Growth.

TOP CYBERSECURITY RECOMMENDATIONS AMID COVID-19

Globally industry has seen a sharp rise in cyber-attacks since the Chinese government disclosed the spread of the coronavirus or COVID-19 within China and internationally. Especially, cyber-attacks focused on health-care systems using spear-phishing and ransomware, impersonation attacks combined with business email compromise (BEC) targeting financial systems, supply-chain cyber-attacks focused on re-directed manufacturing operations outside of China, and distributed denial of service (DDoS) cyber-attacks on the energy, hospitality, and travel industries.

With the spread of COVID-19, increased demands for information technology (IT) support services are occurring across nearly all industries, as worldwide employees, students, university faculty, and others are being asked or required to work or study remotely from their homes to reduce the spread of the virus. As a result, nation-state cyber-attack groups and criminal cyber-attack groups are taking maximum advantage to target cyber vulnerabilities in select industries, especially those most impacted by the current crisis.

Realizing that 40% or more of cyber vulnerabilities are directly linked to employee behavior, per Gartner's latest studies, it is vital that organizations focus more on their employees via cybersecurity awareness, education, training, and use of simulations to create a stronger human firewall to protect their vital digital assets. After all, according to IBM Security's latest findings, the average cost of a cyber data breach is now $8.2M.

Cybersecurity Top Five Recommendations

To reduce both the probability of a cyber-attack or significant data breach and mitigate the negative financial and reputational impacts, we offer the following cybersecurity recommendations which are clearly applicable to all industries:

1) Create an organizational culture of cybersecurity – Ensure the C-Suite consistently promotes and supports all employees practicing effective cybersecurity policies, processes, and procedures via a comprehensive cybersecurity awareness, education, and training program including spear-phishing campaigns and cyber data breach table-top exercises.

2) Implement advanced cyber diagnostic assessments, on a regular basis, including:

- Email Cyber-Attack Assessments
- Network & Endpoint Cyber-Attack Assessments
- Vulnerability Scanning Assessments

- Penetration Testing
- Spear-Phishing Campaigns

3) Establish a Rapid Cyber-Attack Incident Response Plan - Develop and periodically test an enterprise-wide well-coordinated information system incident response plan to quickly identify, contain, eradicate, and recover from cyber-attacks.

4) Conduct 24 x 7 x 365 Monitoring, Detection, & Response (MDR) – It is essential to continually monitor, detect, and respond to all cyber incidents including: email system, network, software applications, and all information system endpoints using advanced security information event management (SIEM) software, data visualization tools, automation, and artificial intelligence (AI) capabilities.

5) Ensure information system resilience - Implement and periodically test an enterprise-wide business continuity plan (BCP) and disaster recovery plan (DRP).