Business Cyber Security Checklist for Unprecedented Times

As the global political landscape becomes increasingly unstable, top information technology firms recommend accelerating digital innovation and cyber security transformations. In the wake of landmark events of tragic proportions, organizations may face unparalleled cyber security threats. In preparing for this cyber reality, explore strategies for ensuring the stability and continuity of your business.

The following cyber security check list can help leaders avoid risk-based disruptions and plan for success in digital journeys.

Endpoint Security

- ☐ Does your organization retain adequate endpoint security?
  Endpoint security enables systems to preemptively block both known and unknown threats. Sophisticated features allow endpoint solutions to turn threat intelligence into prevention, automatically. Optimal endpoint security facilitates unified security management and protects all applications without interrupting productivity.

Network security controls

- ☐ How well is your network protected?
  Has your organization audited its firewall ruleset and aligned its firewall ruleset with Next-Generation Firewall (NGFW) architecture?
  Does your next generation firewall retain features such as application control, integrated intrusion prevention and advanced threat capabilities, including sandboxing?
  Ensure that your organization implements high-caliber network security solutions.

Open source code

- ☐ Do your developers know the origins of the components that they rely on?
  Does your organization retain a software “bill of materials” in the event that security researchers discover a vulnerability within a source code library?
  Follow best practices when it comes to how your software is built, deployed and tracked throughout its lifecycle.

Patching

Despite the seeming improbability of zero day attacks, these threats can have an outsized impact on organizations. Ensure that your organization leverages zero day threat protection with cutting-edge evasion-resistant malware detection technologies built-in. Forget the reactive approach and take a proactive approach to zero day threats. This saves organizations time and limits sudden shifts into crisis-mode.

Employee awareness

Educating employees around cyber security seems like an easy win.
But are you 'bolting on' this cyber security methodology rather than 'baking it in'?
Are your engaging and dynamic trainings occurring more often than once or twice a year?
How are you measuring the training's effectiveness?
Establish reasonable benchmarks for evaluating employee awareness education efficacy.
Advanced levels of employee education are critical in curbing sophisticated cyber threats.

Executive boot-camp

In creating an environment of awareness, develop special cyber security trainings for executives and non-technical management personnel. Test how this group would handle specific cyber attack scenarios, and identify gaps in understanding, communication, and tactical procedures. These types of exercises help organizations ensure a streamlined and efficient approach in coping with and addressing a cyber security crisis.

Backup systems

Review and test your organization's backup procedures. In some cases, cyber criminals deliberately attempt to destroy organizational data backups as to force-the-hand of executives in paying ransomware demands.
Are your data backups segregated from network connections?
Is your organization adhering to the expert-recommended 3-2-1 data backup principle?

Maintain an IR plan

An incident response (IR) plan can cross-leverage organizational resources, roles and capacities to mitigate a cyber threat. Effective incident response plans assist with triage and containment of incidents, enabling organizations to rapidly regain control of systems, processes and productivity. Follow industry standards when developing an incident response plan and ensure that it aligns with your overall security strategy while complying with regulatory measures.

Is your organization catastrophe-averse and equipped with leading resilience strategies, technologies, tactics and techniques?

To develop an even more secure and resilient organization, visit CyberTalk.org.