REOPENING YOUR BUSINESS:

A 51-POINT IT & CYBERSECURITY PREPAREDNESS CHECKLIST

01

OFFICES & WAREHOUSES

- [ ] Prepare visitor security procedures such as sign-in books and badges.
- [ ] Notify third-party vendors that you are reopening.
- [ ] Check your security camera systems to make sure they are monitoring and recording.
- [ ] Secure your server access room; restrict access to key personnel and log all visitors.
- [ ] Check your climate control settings in the server room.
- [ ] Check for physical damages to the office space.

02

EMPLOYEES

- [ ] Create strong password requirements to be used throughout the network.
- [ ] Conduct a debriefing to evaluate the tools you were using while working remotely.
- [ ] Update your user account security policies.
- [ ] Clean up your active directory to account for any personnel changes.
- [ ] Hold an employee cybersecurity awareness training class
- [ ] Develop/update BYOD, acceptable use, remote and wireless access removable media, work from home policies.
- [ ] Follow CDC Guidelines.

03

HARDWARE & DEVICES

- [ ] Check all power strips for signs of wear and damage
- [ ] Check for frayed or loose cables
- [ ] Use compressed air to clean your hardware.
- [ ] Do an audit to make sure all borrowed equipment has been returned.
- [ ] Plan for extended start-up times for devices.
- [ ] Clean all devices returned by employees.
- [ ] Check the current and extended warranty coverage on your servers.
- [ ] Make sure all laptops are encrypted.
- [ ] Replace consumer grade laptops with business class equipment.
- [ ] Look for red/flashing lights on hardware/server room.

04

HONE YOUR STRATEGIES

- [ ] Prepare to continue to offer remote services.
- [ ] Change email signatures to reflect your open status.
- [ ] Consider a permanent transition to cloud computing services.
- [ ] Consider outsourcing some IT services.
- [ ] Review/purchase cyber liability insurance.
- [ ] Engage a third party to regularly perform external vulnerability and penetration tests.
- [ ] Move to a cloud-hosted VoIP phone system.
- [ ] Consider a Cloud-Based Managed firewall.

05

VALIDATE & TEST BACKUPS

- [ ] Check your backup disaster and recovery platforms.
- [ ] Test backups before allowing employees to log in for the first time
- [ ] Verify whether you can spin up your servers locally or remotely via the cloud.
- [ ] Ensure your backup destination is blocked off from the rest of the network.
- [ ] Conduct daily server imaging.
- [ ] Talk with IT about RPO (Recovery Point Objective) /RTO (Recovery Time Objective).

06

CYBERSECURITY

- [ ] Install software patches on all devices.
- [ ] Reboot all internet devices and networks.
- [ ] Utilize SSL-VPN connection security.
- [ ] Check that your mission critical hardware is under warranty, and supported by the manufacturer.
- [ ] Make sure your firewall, antivirus and WiFi are designed to work collaboratively.
- [ ] Make sure desktop operating system are current and updated.
- [ ] Check for updated anti-malware.
- [ ] Review event logs for anything unusual.
- [ ] Identify any systems that were disabled.
- [ ] Ensure that mission critical applications are proactively monitored by IT experts.
- [ ] Make sure software Is updated.
- [ ] Require two-factor authentication for sensitive applications.
- [ ] Run a dark web scan.

FOR A FREE CONSULTATION, CONTACT US AT www.i-evolve.com/contact-us **or email us at** *info@i-evolve.com.*