EBOOK

My Security Console

Business Continuity Cyber Readiness Checklist

Business Continuity Cyber Readiness Checklist

Business disruptions from unanticipated events can cost money. Lost revenue plus extra expenses mean reduced profits and large loses that many small and medium business are unable to overcome.

Being prepared with a plan will help you minimize the risk that an emergency poses to your employees, clients and suppliers, the continuity of your business operations and your bottom line. Use the following checklist as a starting point for building your company's cyber readiness and ability to respond to a crisis.

Getting Started

1. Appoint an emergency coordinator and/or team with defined roles and responsibilities for preparedness and response planning. Be sure to include your IT support team.
2. Create a list identifying essential employees and other critical inputs and data required to maintain business operations by location.
3. Back-up all data and ensure easy and secure access to that data.

Employee Readiness

Training: Provide your staff with cyber-awareness training that addresses common threats like phishing email campaigns exploiting the latest threats like "COVID-19".	☐
Work Environment: Implement preventive hygiene for shared workstations such as providing antimicrobial wipes for shared keyboards and mice.	☐
Teleworking / VPN Access: Set up remote access such as VPN and ask employees to test and confirm that they are able to work remotely if needed.	☐
• Make sure that employees who can work from home, have anti-virus on their computers and can connect to critical business systems remotely and safely	☐
• Confirm that staff know how to securely share documents such as using password-protected ZIP files or using secure cloud storage.	☐
IT Staff Backup: Ensure there is more than one person with credentials for accessing critical IT systems and applications.	☐

Business Continuity Cyber Readiness Checklist

Communication

Business Phone Line Accessibility: Ensure that your primary business phone number can be forwarded to a different number and is remotely accessible should your primary business location become inaccessible due to an event like a quarantine.	☐
Email. Be sure that key email accounts will continue to be remotely accessible in the event that your primary location becomes inaccessible. Have provisions for remote accessibility to needed email accounts.	☐
Video Conferencing / Conference Bridge: Ensure that systems have been setup to enable your employees to collaborate remotely via video or phone conferencing.	☐
Data Privacy/Confidentiality: Provide routine status updates to keep staff, clients, suppliers and partners informed, however be sure not to violate privacy rights or disclose personal or private information like individual health status.	☐
Emergency Contacts: Provide an emergency contact list and ensure staff know who to contact for information in the event of a crisis or emergency.	☐

Equipment & Utilities

Cameras / Alarms: Test your security cameras and alarm systems to make sure they are in good operational order in case your place of business is not accessible. Test them to confirm remote access.	☐
Hardware Security: Ensure your critical hardware will remain safe (e.g. within a locked server room, secured with lock kits) if your place of business will remain closed due to events such as a quarantine.	☐
Backup Power: Ensure that critical systems are connected to backup power with enough capacity to sustain longer than usual power disruption and that critical systems can be remotely managed even with intermittent power disruptions.	☐
Internet : If internet connectivity to your office is critical for your business, make sure you have a redundant connection or can continue to function in the event of longer than usual internet outages.	☐

Email: info@mysecurityconsole.com | (647) 560-8687

Business Continuity Cyber Readiness Checklist

Data Security

Accessing Critical Systems & Data: Identify your critical systems and applications and make sure there is more than one person with the necessary credentials and access to those systems. For example payroll, invoicing, banking.	☐
Sharing Confidential Information Remotely: Ensure that employees are aware of the need to protect sensitive and confidential information if they need to collaborate remotely for a prolonged period of time, such as using password protected zip files or secure cloud storage to share files.	☐

Supply Chain

Service Providers: Coordinate discussion with suppliers and service partners to outline emergency contacts and how they plan to continue to provide you with the required goods and services in the event of a crisis.	☐
Supply Chain Backups: List third party services and suppliers that are critical to your business and identify and contact alternative providers.	☐

Email: info@mysecurityconsole.com | (647) 560-8687