MICHAEL MILLER INSURANCE
SINCE 1977

Cyber Security Checklist

The topic of cyber security covers many actions that, together, help to deter hackers and protect against viruses and other potential risks to the networked enterprise. This handout provides security tips, developed by the Department of Homeland Security, to assist business managers in assessing and improving their cyber security plans and procedures.

	Yes	No	N/A
Management. The key to effectively managing cyber security is to demonstrate top-level executive support. Some key management activities that should be addressed include:			
Have you created security policies to match the size and culture of your business?	☐	☐	☐
Are security policies written, enforced, and kept updated?	☐	☐	☐
Have you established a computer software and hardware asset inventory list?	☐	☐	☐
Have you classified data by its usage and sensitivity?	☐	☐	☐
Have you established ownership of all data?	☐	☐	☐
Information Technical Staff. They are on the front line when it comes to cyber security and are responsible for some key activities. Examples of activities to be addressed include:			
Are you maintaining configuration management through security policy implementation and systems hardening?	☐	☐	☐
Are you maintaining software patch management on all systems by following a regular schedule for applying patches for operating systems, specific software, and anti-virus updates?	☐	☐	☐
Do you subscribe to security mailing lists?	☐	☐	☐
Are you maintaining operational management through the reviewing of all log files, ensuring system backups with periodic data restores (data restores shouldn't be done unless a problem corrupted the live data), and reporting any known issues or risks?	☐	☐	☐
Are you performing security testing through security audits and penetration scanning?	☐	☐	☐
Are you ensuring physical security of systems and facilities?	☐	☐	☐
Do you ensure users have anti-virus software loaded and active on systems?	☐	☐	☐
End Users. Some of the key activities that end users should address include:			
Do you have anti-virus software loaded and active on your computer?	☐	☐	☐
Do you delete, without opening, e-mails from unknown sources?	☐	☐	☐
Do you back up data on a regular basis?	☐	☐	☐
Do you utilize strong, hard-to-guess passwords?	☐	☐	☐
Do you use personal firewalls?	☐	☐	☐

	Yes	No	N/A
Do you download and apply security patches?	☐	☐	☐
Do you disconnect your computer from the Internet when not in use?	☐	☐	☐
Do you restrict access to systems to authorized users only?	☐	☐	☐

Business Continuity. In order to ensure continuity of business, proactive security measures must be taken and be part of daily operations. Routine security testing, and regularly-scheduled risk assessments and third-party security audits, should be performed. These are continuity measures that should be addressed:

Do you have an emergency response plan?	☐	☐	☐
Have you systematically evaluated all of the potential sources of disruption to your business?	☐	☐	☐
Do you have an active program to reduce the likelihood of a disruption?	☐	☐	☐
If you could not re-enter the workplace because of an emergency, do you have a pre-determined location to meet to coordinate recovery operations?	☐	☐	☐
Do you maintain a current list of employees, customers, and suppliers at an off-site location?	☐	☐	☐
Have you met with local emergency response groups to discuss their role in maintaining the business?	☐	☐	☐
If you lost a critical system, do you have a pre-determined plan to restore the system?	☐	☐	☐
Do you have an established business resumption team?	☐	☐	☐
Is your business resumption plan securely stored in a remote location?	☐	☐	☐
Do you periodically test your business resumption plan along with your site emergency response plan?	☐	☐	☐