

LOSS CONTROL DATA GUIDE

Cyber Security Tips

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 businesses in assessing and improving their cyber security plans and procedures.

Management. The key to effectively managing cyber security is to demonstrate top-level executive support. Some key management activities that should be addressed include:

	Yes	No	N/A
Have you created security policies to match the size and culture of your business?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are security policies written, enforced, and kept updated?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you established a computer software and hardware asset inventory list?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you classified data by its usage and sensitivity?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you established ownership of all data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Information Technical Staff. They are on the front line when it comes to cyber security and are responsible for some key activities. Examples of questions to be addressed include:

	Yes	No	N/A
Are you maintaining configuration management through security policy implementation and systems hardening?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you subscribe to security mailing lists?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are you performing security testing through security audits and penetration scanning?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are you ensuring physical security of systems and facilities?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you ensure users have anti-virus software loaded and active on systems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are you limiting access to computer facilities to key personnel only?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

End Users. Some of the key activities that end users should address include:

	Yes	No	N/A
Do you have anti-virus software loaded and active on your computer?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you delete, without opening, email from unknown sources?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you back up data on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you utilize strong, hard-to-guess passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you use personal firewalls?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you download and apply security patches?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you disconnect your computer from the Internet when not in use?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you restrict access to systems to authorized users only?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you been instructed on what to do when a system indicates a virus is present?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 example questions to be addressed:

	Yes	No	N/A
Do you have an emergency response plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you systematically evaluated all of the potential sources of disruption to your business?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have an active program to reduce the likelihood of a disruption?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If you could not re-enter the workplace, do you have a pre-determined location to meet to coordinate recovery operations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you maintain a current list of employees, customers, and suppliers at an off-site location?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you met with local emergency response groups to discuss their role in maintaining the business?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If you lost a critical system, do you have a pre-determined plan to restore the system?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have an established business resumption team?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is your business resumption plan securely stored in a remote location?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you periodically test your business resumption plan along with your site emergency response plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>