

LOSS CONTROL DATA GUIDE

Improving Business Cyber Security

Businesses must protect their data and information technology systems. Every computer can be vulnerable to attack, and the consequences of such an attack can range from simple inconvenience to financial catastrophe. Depending on the particular industry, and the size and scope of the business, cyber security can be very complicated and may require specialized expertise. However, even the smallest business can be better prepared.

Start with the following simple steps, which are recommended by US-CERT, a partnership between the U. S. Department of Homeland Security (DHS) and the public and private sectors:

Use anti-virus software and keep it up-to-date.

- Activate the software's auto-update feature to ensure your cyber security is always up-to-date.

Don't open email from unknown sources.

- Whether they are from a known source or not, be suspicious of unexpected emails that include attachments.
- When in doubt, delete the file and the attachment, and then empty the computer's deleted items file.

Use hard-to-guess passwords.

- Passwords should have at least 8 characters with a mixture of uppercase and lowercase letters, as well as numbers.
- Change passwords frequently.
- Do not give out the password to anyone.

Protect computers from Internet intruders by using firewalls.

- There are two forms of firewalls: software firewalls that run on a personal computer, and hardware firewalls that protect computer networks, or groups of computers.
- Firewalls keep out unwanted or dangerous traffic, while allowing acceptable data to reach a computer.

Don't share access to computers with strangers.

- Check the computer operating system to see if it allows others to access the hard-drive. Hard-drive access can open up a computer to infection.
- Unless you really need the ability to share files, the best bet is to do away with it.

Back up computer data.

- Many computer users have either already experienced the pain of losing valuable computer data or will at some point in the future. Back up data regularly and consider keeping one version off-site.

Regularly download security protection updates, known as patches.

- Patches are released by most major software companies to cover up security holes that may develop in their programs.
- Regularly download and install the patches, or check for automated patching features.

Check security on a regular basis.

- Evaluate computer security settings regularly. The programs and operating system on a computer have security settings that can be adjusted.
- Consider if tighter security at the office, such as multiple door locks or a high-tech access control system, is needed.

Make sure employees know what to do if the computer system becomes infected.

- Train employees on how to update virus protection software, how to download security patches from software vendors, and how to create a proper password.
- Designate a person to contact for more information if there is a problem.

Subscribe to the DHS' National Cyber Alert System.

- The National Cyber Alert System provides free, timely alerts on new threats and information on how to better protect computer systems.