Courtesy of
ABEX

CYBERRISKS&LIABILITIES_

Basic Loss Control Techniques

Protecting your business from cyber risks can be an overwhelming venture. With each passing month, new and more sophisticated viruses are being discovered, more spam is reaching your inbox and yet another well-known company becomes the victim of a data breach.

The world will never be free of cyber risks, but there are many loss control techniques you can implement to help protect your business from exposures.

1. **Install a firewall for your network.**
   Operating systems often come with pre-installed firewalls, but they are generally designed to protect just one computer. Examine the firewall's options and select the best configuration to keep the computer safe.

   If your business has a network of five or more computers, consider buying a network firewall. They can be pricey but network firewalls provide a fine level of coverage for an entire network.

2. **Install anti-virus, anti-malware and anti-spyware software.**
   This loss control technique is the easiest and most effective way to increase security at your business. Make sure to install the software on each computer in your network—computers that don't include these types of software are much more likely to be exposed and can possibly spread malware to other computers in the network. There are a host of viable options for each type of software, ranging in price from free to an annual subscription. Be sure to keep the software as up-to-date as possible.

3. **Encrypt data.**
   No firewall is perfect. If a hacker manages to get through your firewall and into your network, your data could be a sitting duck. Encryption will make the data unreadable to a hacker. Consider using an encryption program to keep computer drives, files and even email messages safe from hackers.

4. **Use a Virtual Private Network (VPN).**
   A VPN allows employees to connect to your company's network remotely. VPNs eliminate the need for a remote-access server, saving companies lots of money in remote server costs. In addition to these savings, VPNs also provide a high level of security by using advanced encryption and authentication protocols that protect sensitive data from unauthorized access. If your company has salespeople in the field or employs workers who work from home or away from the office, a VPN is an effective way to minimize cyber risks.

5. **Implement an employee password policy.**
   One of the most overlooked ways to keep your business safe is instituting a password policy. Essentially, a password policy should force employees to change work-related passwords every 90 days. The policy should encourage the creation of easy-to-remember, hard-to-guess passwords that include letters, numbers and special characters. For example, an easy-to-remember, hard-to-guess password could be "M1dwbo1025." (My first daughter was born on Oct. 25th.)

   Passwords that contain words from the dictionary or contain sensible combinations (abc123, qwerty, etc.) should never be allowed. Let employees know that they should not write passwords down and leave them in a desk or out in the open. If they are having trouble remembering passwords, there are

password-keeping programs available for download.

6. **Back up data regularly.**
   Important data should be backed up daily and in multiple locations, one being off-site. In addition to being safe from cyber risks, off-site data would not be exposed from physical attacks, like a fire or tornado.

   Restrict access to backed up data. The public should never have access to it. If the data is tangible, keep it in locked filing cabinets in a locked room, and only issue keys to those who absolutely need them.

7. **Develop a business continuity plan.**
   If the worst should happen and your company suffers a data breach or similar attack, you should have a business continuity plan in place. A business continuity plan helps:
   - Facilitate timely recovery of core business functions
   - Protect the well-being of employees, their families and your customers
   - Minimize loss of revenue/customers
   - Maintain public image and reputation
   - Minimize loss of data
   - Minimize the critical decisions to be made in a time of crisis

   The plan should identify potential cyber risks, along with the recovery team at your company assigned to protect personnel and property in the event of an attack. The recovery team should conduct a damage assessment of the attack and guide the company toward resuming operations.