Cyber Crime

10 ways your small business can fight it

1. Protect the Perimeter

Protect your company's physical perimiter to prevent hackers from accessing sensitive data and your company's computer network.

2. Train Employees

Educate your team because employees are your company's first line of defense against cyber criminals.

3. Build a Firewall

Activate your firewall to block connections that are used to hack into your system and deliver viruses.

4. Update Software Regularly

Install and regularly update spyware, antivirus and malware software to help prevent and detect any of those from affecting your computers.

5. Change Passwords Often

Use stronger password of 8-10 characters that include letters, numbers and special characters; change those passwords regularly on your network, and require all employees to change their passwords regularly as well.

6. Secure Your Networks

Secure your Wi-Fi networks to prevent hackers from accessing your servers or using your internet connection without your knowledge.

7. Monitor Social Networks

Set social networks profiles to private and check security settings, also, be mindful of what information you post online.

8. Encrypt Data

Encypt your most sensitive data, make a backup and store it in a fireproof safe or off-site; use a dedicated computer for all sensitive information.

9. Confirm Your Vendor's Security

Carefully select online computing services, because any information you share with them can be compromised by their system.

10. Buy the Right Insurance

Acquire cyber insurance to cover losses in case of a breach or fraud. Agents should review the client's business insurance package and ensure that the appropriate coverage is in place.

Hebard Insurance & Tax Solutions
3837 Taylor Road – Loomis, CA 95650
(916) 652-0404
www.hebardsolutions.com

Examples of Cyber Claims

Ransomware / Cyber Extortion

An employee clicks on the attachment in an email which launches “Ransonware” and it rapidly spreads to the organization’s network effectively locking all the businesses electronic files. Business receives a phone call a short while later demanding $10,000 in order to gain access to their data.

Malware Data Breach

A regional retail computer system was compromised when a third party sent a malware program via email to a number of employees. The invasive software allowed the third party to access the system and capture the names, addresses and credit card numbers for more than 5,000 customers.

Personal Records Disclosure

Computer was purchased that used to belong to a financial services business. The company did not wipe the hard drive and it contained client’s old information, such as names, addresses, social security numbers, and lists of financial accounts.

The cost of notifying parties that were affected per state law totaled almost $110,000. Two different parties filed separate lawsuits, one who claims they lost their job from the result of the negligence for damages more than $200,000 and another from claiming that their identity was compromised and the damages resulted in over $100,000.

Stolen Laptop

An employee’s company laptop containing private customer information is stolen from his home. As a result, customers sue the company for damages resulting from alleged failure to protect their private financial information. The business spend nearly $700,000 in defence of lawsuits.

Rogue Employee

An employee stole a donor’s credit card information from a non-profit that resulted in a forensics investigation, a lawsuit and a PCI fine. The total costs were in excess of $500,000.

Hebard Insurance & Tax Solutions
3837 Taylor Road – Loomis, CA 95650
(916) 652-0404
www.hebardsolutions.com