Grocery Risk Management Bulletin

✔ *Helping Grocers reduce their cost of insurance by preventing accidents and claims*

CYBER SECURITY FOR GROCERS

High-profile cyber attacks on companies such as Target and Sears have raised awareness of the growing threat of cyber crime. Recent surveys conducted by the Small Business Authority, Symantec, Kaspersky Lab and the National Cybersecurity Alliance suggest that many small business owners are still operating under a false sense of cyber security.

The statistics of these studies are grim; the vast majority of U.S. small businesses lack a formal Internet security policy for employees, and only about half have even rudimentary cybersecurity measures in place. Furthermore, only about a quarter of small business owners have had an outside party test their computer systems to ensure they are hacker proof, and nearly 40 percent do not have their data backed up in more than one location.

Don't Equate Small with Safe
Despite significant cybersecurity exposures, 85 percent of small business owners believe their company is safe from hackers, viruses, malware or a data breach. This disconnect is largely due to the widespread, albeit mistaken, belief that small businesses are unlikely targets for cyber attacks. In reality, data thieves are simply looking for the path of least resistance. Symantec's study found that 40 percent of attacks are against organizations with fewer than 500 employees.

Outside sources like hackers aren't the only way your company can be attacked—often, smaller companies have a family-like atmosphere and put too much trust in their employees. This can lead to complacency, which is exactly what a disgruntled or recently fired employee needs to execute an attack on the business.

Attacks Could Destroy Your Business
As large companies continue to get serious about data security, small businesses are becoming increasingly attractive targets—and the results are often devastating for small business owners.

According to the Kaspersky Lab, the average annual cost of cyber attacks to small and medium-sized businesses was over $200,000 in 2014. Most small businesses don't have that kind of money lying around, and as a result, nearly 60 percent of the small businesses victimized by a cyber attack close permanently within six months of the attack. Many of these businesses put off making necessary improvements to their cyber security protocols until it was too late because they feared the costs would be prohibitive.

10 Ways to Prevent Cyber Attacks
Even if you don't currently have the resources to bring in an outside expert to test your computer systems and make security recommendations, there are simple, economical steps you can take to reduce your risk of falling victim to a costly cyber attack:

1. Train employees in cyber security principles.

2. Install, use and regularly update antivirus and antispyware software on every computer used in your business.

3. Use a firewall for your Internet connection.

4. Download and install software updates for your operating systems and applications as they become available.

5. Make backup copies of important business data and information.

6. Control physical access to your computers and network components.

Secure your Wi-Fi networks. If you have a Wi-Fi