RAM MUTUAL INSURANCE

BREACH PROTECTION TIPS

FOUR WAYS YOUR BUSINESS CUSTOMERS ARE VULNERABLE TO CYBER ATTACKS

Hollywood and news media will have you think of cyber criminals as an innovative lot, coming up with new, sophisticated ways to steal data that are just beyond the reach of security best practices.

But the reality is much more mundane. More often than not they are exploiting vulnerabilities that are well-known, according to the 2016 Verizon Data Breach Investigations Report. And the compromise of business, employee and customer information can lead to identity theft.

Here are four useful takeaways from the report for business customers:

1. **Known weaknesses.** Most attacks, 85 percent, target known vulnerabilities.
2. **Money talks.** Most attacks, 80 percent, are financially motivated.
3. **Weak passwords.** 63 percent of data breaches involve weak, stolen or default passwords.
4. **Rise in ransomware.** Ransomware attacks are up 16 percent.

Fortunately, there are basic steps businesses can take to enhance their security posture that won't break the bank.

- **Perform a security assessment.** Bring on a knowledgeable expert to help identify critical weak points and practices.
- **Stay updated.** Off-the-shelf antivirus software can be highly effective if kept up to date and used judiciously.
- **Train employees.** Basic education for employees on how to follow security best practices and spot potential data exposures can mitigate pre-breach risks and post-breach damages.
- **Control access.** Manage physical access to computers, and access to networks and protected data. Enforce strong user names and passwords
- **Manage risk with coverage solutions.** SMBs can manage their risks with cyber liability and data breach policies.

POWERED BY CYBERSCOUT™