YOU ARE UNDER ATTACK RIGHT NOW:

REDUCING YOUR RISK OF DAMAGE DUE TO CYBER WARFARE

by Kurt D. Kelley, JD

Weather damage to your property and bodily injury associated with your business operations are understood large risks to community owners and retailers. But the real and constant threat related to those transmission lines running in and out of your computers is less understood. Theft of your proprietary data, theft of your customers' data, destruction of your computing systems, wiping out of your bank accounts, and cyber extortion are some of these risks. If you don't know what your employees are doing on their computers right now, and who outside your company can access your systems, you are under constant threat.

In the past twelve months there have been multiple six figure thefts from the bank accounts of community owners. Proprietary data has been stolen from retailers, community owners and HUD code home manufacturers. Data theft and subsequent extortion attempts have hit businesses across the country. Hackers and cyber thieves now have "automated" regular attacks.

At Mobile Insurance, not only do we house private client information, but we also hold money in trust for our insurance company partners. We are a prime target. Here is what we are doing to reduce our risk:

1) Regular training of all employees. Our anti-virus software company offers free training modules via WebRoot. It's automated and thorough. Employees are sent regular simple online training videos and their progress is monitored. The most common way for

hackers to access your company system is by tricking employees into opening the door and welcoming them in.

2) This same system sends our employees regular simulated phishing attempts. Results are tracked. This educates management about when more training is needed. When an employee fails, they are directed to a corrective educational video (and publicly flogged, too, of course).

3) We use a password management software system. It sets complicated and regularly updated passwords for all our systems. Passwords are securely stored in one place with the need to only remember one.

4) Access of any of our systems via new or unidentified terminals requires further confirmation from approved terminals.

5) Electronic wire transfers require in person confirmation with our banking partners.

6) Advanced spam and virus filtering software is on all our systems. Encrypted email attachments are decrypted and subjected to an in-depth virus scan. Phishing emails are blocked and flagged

Because I've been forced to hire those pesky and fallible creatures commonly known as humans, I also purchased a quality cyber liability insurance policy. This protection is designed to save me when all else fails. For about $1,800 per year, I now have:

- ✓ a team of computer experts to respond and pay for all cyber extortion threats,
- ✓ $1,000,000 coverage for electronic wire fraud,
- ✓ replacement cost for all equipment ruined due to viruses,
- ✓ costs to restore and replace all my company's lost data,
- ✓ loss of income coverage if I can't operate because my systems are hacked,
- ✓ liability protection if credit card systems or data are misused, and
- ✓ and $1,000,000 of liability coverage if my system is co-opted to attack another's system or one of my employees uses copyrighted data or information.

My cyber liability company tests all my systems and sends me recommendations on how to better defend my company. I think this is the best value insurance policy I ever bought.

Kurt D. Kelley,President of Mobile Insurance, an agency specializing in insurance for manufactured home communities and retailers. Named top commercial insurance agency by American Modern Insurance Group. Member of numerous insurance companies' policy development and advisory teams. One of largest manufactured home specialty agencies in the country.

MOBILE INSURANCE

800.458.4320

www.MobileAgency.com