Cybercrime Represents a Very Real, and Very Serious Threat to Small Business

The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses

Cyberspace is the new burglar arena, stretching through wires and air and can destroy or wreak havoc on your business and life. Out of nowhere, these criminals will steal your time, money, and business.

If you are attacked, do you know what to do? Who do you call? What can it cost?

According to Commissioner Luis A. Aguilar, U.S. Securities and Exchange Commission*, cyber threats are a daunting risk facing small and midsized businesses (SMBs) today. Your clients may think their businesses are too small to be impacted, but the scary truth is that a staggering 1 in 5 SMBs will fall victim to a cyber attack and of these, 60% will shut down within 6 months.

The past several years have witnessed an array of successful cyberattacks against some of the most prominent firms in the country. In the past two years alone, eBay, JP Morgan, Home Depot, and Target all suffered major breaches at the hands of cybercriminals. These breaches, which affected approximately 353 million customers collectively, were spectacular not only because of their size, but also because of the relentless pace at which they seemed to occur. Since the popular press tends to focus on attacks, like these, that target the largest firms, it can be easy to overlook the fact that SMBs are at even greater risk, and are far more vulnerable once they are victimized. In fact, for every high-profile breach, there are many more threats to confidential data held by local businesses. According to a list of data breaches maintained by the California Attorney General, wine shops, dentist offices, community centers, and small manufacturers have all been victims of cybercrime in the past few years.

A recent survey conducted by the National Small Business Association underscores just how serious a threat cybercrime poses to SMBs. According to the survey, half of all SMBs surveyed reported being the targets of a cyberattack, a 14% increase over the prior year. The survey revealed other disturbing trends, as well. For example, the survey found that the cost of the average attack rose from $8,699 in 2013 to $20,752 last year (2015)—an increase of almost 140% in only one year.

The rate of the increase was even more pronounced for firms whose bank accounts were hacked, as the average cost of those attacks rose by almost 187%. The survey also found that it is becoming increasingly difficult for SMBs to recover from an attack. The number of firms reporting that it took them at least three days to recover from an attack rose to 33% last year, up from only 20% the year before. And, in an especially dispiriting development, the survey found that SMBs that were the victims of a cyberattack were more likely to be targeted again.

From tablets, to servers, cellphones, laptops, credit cards, even manufacturing equipment, heating & cooling equipment, telephone systems can all be hacked with devastating consequences.

Despite over $90 billion of annual consumer and business spending on cybersecurity defense, the problem is only growing. Unfortunately, the state of the cyber world is that nothing is or will ever be 100% secure and no one can defend themselves 100% of the time. The time has arrived that cyber risk management is a must for all organizations, no matter their size.

Best protection is a sound cyber risk management program and a well-drafted cyber insurance policy. Often these days insurance carriers are adding Cyber Coverage to some policies, however the coverage limits are small, coverage is vague. Some or many of the major risks are not covered. Like the old saying, “You get what you pay for.”

This is why I created a 20-point/endorsement checklist I use to review coverage. (And why I purchased a standalone Cyber/Privacy policy for my business through the Coalition and why I offer and recommend the same to my customers.) With Coalition, you're putting all the cybersecurity power in your clients' hands.

Look for more articles in future newsletters to learn more about what makes Coalition so powerful, including:

1. Underwriting Engine: Coalition scans publicly available information, collecting tens of thousands of signals and correlating this to insuring agreements selected. This all happens in seconds to ensure an efficient process where you can rate, quote, bind, and obtain a policy in under 4 minutes!

2. Comprehensive Coverages: Coalition offers the broadest coverages available offering full limits across all coverages including funds transfer fraud/social engineering, bodily injury, property damage, and contingent business interruption. There are a variety of unique coverages including Coalition's new **Breach Response Separate Limits Endorsement**, which provides additional coverage for breach response costs by moving these costs outside of the aggregate limit.

3. Risk Management Tools: Coalition's cyber risk management platform provides automated security alerts, threat intelligence, ongoing monitoring and expert guidance, among other tools all available at no additional cost.

4. Claims Approach: From pre-breach support to incident containment and recovery, Coalition's insurance and security experts are there to help. In the event of a breach, Coalition's cyber team is in place for rapid response to mitigate risk. This Coalition-assisted claims mitigation all occurs at no additional cost.

Call Dennis McCurdy today about cyber insurance for your business: 508-347-9343.

*(Source: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html)