LANDY Insurance
Herbert H. Landy Insurance Agency, Inc.
100 River Ridge Drive, Suite 301 | Norwood, MA 02062
800-336-5422 | Fax: 800-344-5422
www.landy.com

The Cybercrime Trap – Information & Advice on Lowering Your Risk

Cybercrime, including data breach, ransomware, computer fraud and social engineering, poses an increasing risk to businesses. The consequences are substantial, with the Small Business Association reporting that 60% of small to medium-sized businesses that experience a cybercrime go out of business in less than one year. Real estate professionals hold a special attraction to cyber-criminals. Think about how an agent conducts business – highly personal and access to sensitive information, including financial data; out of office work requiring regular use of personal communication devices (PCD's); frequent use of social media and not least of all, a typical lack of "techy" skills and IT support. In short, cyber-criminals want YOU.

Making your business less vulnerable to attacks or the consequences of an attack (as the saying goes, "There are two kinds of businesses; those that have been attacked and those that don't know they've been attacked") is a three-pronged effort. That includes modifying behavior, taking steps to secure your place in cyber-space, and insuring against the costly consequences of an attack.

The Human Role in Preventing Cybercrime

The great majority of cyberattacks stem from what we do, or do not do, every day. Verizon reports that 90% of all computer crime begins with a phishing email. We open 30% of emails that contain a path to a link or attachment that allows access to our networks. Learning to recognize suspicious emails can significantly reduce the chance of a breach. Slowing down our pace to review an email, its' sender and contents is one thing we can all do:

- Do you know the sender?
- Are you expecting the email?
- Is the spelling and punctuation professional, or at least correct?
- Does the sender email look legit – zeros instead of O's, 1's instead of I's, etc?
- Are there links or attachments that look unusual, unexpected or out of place?

A significant method of changing our "Cyber Behavior" lies in developing protocols that are adopted by all members of a firm and consistently practiced. For example, a Brokerage might implement a secure email system or website, but all is for naught if agents use unsecured emails or websites that are independent of the Brokerage. Similarly, postings and communications through social media lack any real security and are amongst the easiest avenues for the bad guys to begin the process of a crime.

Successful behavioral change should also include regular changing of passwords (and not from Password1 to Password2). Even more effective is to use a password manager (see below). Emails should be encrypted, and all logins should require multi-factor authentication. If you are involved in the transfer of funds, there should be a consistent procedure that requires personal authentication of routing numbers, etc. Cyber-criminals are now setting up their own 800 numbers to thwart phone verifications, so you should have a name and direct line to someone you know. Be suspicious of any change or deviation from established plans or protocols.

LANDY Insurance
Herbert H. Landy Insurance Agency, Inc.
100 River Ridge Drive, Suite 301 | Norwood, MA 02062
800-336-5422 | Fax: 800-344-5422
www.landy.com

Security Measures to Consider

Unsecure passwords are a gateway to a breach. Recognizing that managing numerous passwords can be difficult, there are several good password managers that will constantly create and change passwords for all of the websites you need to access. They include *LastPass, Dashlane, Keeper, Sticky Password* and many others. All are more or less similar, very low cost and there are numerous on-line reviews and evaluations of the pros and cons of each option – the bottom line being that a password manager will go a long way towards enhancing your security.

Downloading free apps is risky business. Many "free" apps, including battery saving applications, games and banking/credit card applications are nothing more than Trojan apps developed to infiltrate your computer. Consider a policy that forbids the downloading of non-authorized applications onto company devices, and of course be extra diligent with personal devices as well. This is equally true for data storage devices like thumb drives, which are often made strategically "available" at conferences and other public events but are loaded with malware. If you are using Android devices, including phones, consider installing anti-virus software such as *Bitdefender, Webroot, Avast, Sophos* or similar. Finally, make sure your computer or network automatically updates third-party applications, including Adobe, Java and your internet browser.

As mentioned earlier, many companies do not have the skills, time or resources to do these and the many other things needed to maintain a vigorous security plan. Consider hiring a network security firm to do semi or annual inspections and updates of your network, as well as review best practices. With the cost of a breach typically in the 10's or 100's of thousands of dollars for even a small firm, it would be money well spent.

The Insurance Solution

Considering that 70% of all cybercrime targets small businesses and is conducted by sophisticated international crime rings, the possibility remains strong that even well-protected businesses will get hacked. Cybercrime insurance should be considered as an important part of any business' insurance program. Here are some of the consequences, and costs, associated with a breach or ransomware attack:

- Needing to minimize the damage once a crime has been discovered
- Notifications to affected parties (complying with individual State law)
- Credit Monitoring of affected parties
- Civil Penalties (per record, per State)
- Forensics & Data Restoration
- Lawsuits
- Reputational Harm
- Loss of business/productivity due to ransomware
- If money is misappropriated, then replacement of stolen funds and potential lawsuits from additional economic loss

As mentioned, the cost of any or all of these can bankrupt a business. Cybercrime insurance is available to cover all the negative consequences of data theft, ransomware attack, computer fraud and social engineering.

LANDY Insurance
Herbert H. Landy Insurance Agency, Inc.
100 River Ridge Drive, Suite 301 | Norwood, MA 02062
800-336-5422 | Fax: 800-344-5422
www.landy.com

These coverages are typically not available in an Errors & Omissions, Professional Liability or General Liability policy and affordable plans can be developed to address the unique concerns of a particular business or industry. Lastly, remember that computer crime can happen from within as well, in the forms of employee dishonesty, embezzlement and property theft.

To find out more about protecting your business from cybercrime and its' consequences, contact John Torvi at Landy Insurance at johnt@landy.com, 781-292-5417.
Special thanks to Erik Celani of Netlogic Computer Consulting, www.netlogiccomputer.com. Erik can be reached at erik@netlogiccomputer.com, 603-546-6422.