LANDY Insurance

Herbert H. Landy Insurance Agency, Inc.
75 Second Ave., Suite 410 | Needham, MA 02494-2876
800-336-5422 | Fax: 800-344-5422

www.landy.com

August 28, 2018

Cybercrime – Who's Next?
An Insurance Primer

Despite the abundance of news, how-to tips and cautionary tales, cybercrime has infiltrated the local, regional and national business space, impacting real estate professionals with a special severity. The sophistication and global reach of the cybercriminal can easily overwhelm most precautions and risk-management practices (assuming they exist at all) of small to medium sized firms. While data theft and ransom attacks are most common, the most damaging crimes include the misappropriation of escrow, IOLTA and other custodial funds held by attorneys, title agents and real estate brokerages. Recent events illustrate the severity of the problem, with stolen funds in the tens to hundreds of thousands of dollars.

These losses, if needing to be reimbursed by the affected real estate practice, can easily force a firm to go out of business. Many law, title and real estate firms have started taking preventative steps to reduce cybercrime risk, including strengthening office protocol and putting informational and instructional language on websites and emails related to monetary transfer procedures. Hopefully this is done in conjunction with regular staff training and includes a forensic and system-wide analysis by an IT-security expert. Nevertheless, breaches and crime are almost exclusively a consequence of human error. Putting aside the buzzwords like phishing, hacking and spoofing, ultimately the bad guys will infiltrate a computer system when someone clicks a bad link, opens an infected document, forwards the latest "joke of the day" or other seemingly innocent moves done in the middle of a busy work day. Once that happens, the flood gates are open, with 90% of all cyberattacks coming through an infected email. It may be weeks or months before the innocent party even becomes aware (if at all) of the breach. Even if one does not adopt the "when, not if" attitude about the likelihood of becoming a cyber-victim, a risk-management program must consider insurance coverage to help mitigate the damage and cost of a data or monetary breach.

There are numerous insurance plans available to protect one's cybercrime exposure. Sound coverage and reasonable premiums are becoming readily available though plans and terminology can be confusing. An understanding of policy language and available coverage can be instructive when choosing protection.

A first step for a firm (or a non-profit) would include an assessment of the risk – i.e. what does my practice have that a criminal might want? Here, there are two main categories – data and money. Most businesses have confidential and privileged information (awareness and compliance with various state regulations and laws which outline consumer protections, required practices and data security regulations are critical but should be seen as a starting point). Thus a good place to begin is understanding what the consequences of a data breach are, and therefore what should be covered in an insurance policy. Besides the civil penalties imposed by the government – fines can be imposed on a "per record" basis rather than per breach - a compromised firm might face lawsuits, be required to provide notifications of breach and credit monitoring to each affected party, conduct forensics to determine and eliminate the infection, perform data and system restoration to be able to continue business, payment card industry fines and reputational harm and loss of income. A cyber insurance policy should provide coverage for these as a basic level of protection. The Better Business Bureau reported in

LANDY Insurance

Herbert H. Landy Insurance Agency, Inc.
75 Second Ave., Suite 410 | Needham, MA 02494-2876
800-336-5422 | Fax: 800-344-5422

www.landy.com

2017 that the average cost of a cyberattack (not including theft/loss of funds) is almost $80,000. Within six months of an attack, 60% of small companies will go out of business. Another type of cyberattack is ransomware. Here, the criminal installs malignant software into a computer network, effectively disabling the network until a ransom is paid. Ransom demands are usually small, typically under $10,000 with a demand for bitcoin or alternate currency. Businesses can be shut down for days trying to remedy this and there is also the cost of forensics and system restoration in addition to the ransom and loss of production. Again, ransomware coverage should be included in an insurance policy.

Firms that control funds have additional threats, including wire and computer fraud, social engineering and employee dishonesty/theft. The distinction in these terms is important, as insurance plans define them differently, effecting coverage. Briefly, wire and computer fraud is when the criminal uses a firm's computers to steal money directly or act as a representative of the firm to trick a third party into sending money. Social Engineering is when a representative of the firm is duped into sending funds themselves. Again, policy language and coverage may be different for wire, computer fraud or social engineering, so diligence is needed in setting up a policy. Also in the "money" category of computer threat is employee dishonesty, including embezzlement, fraud, theft of property or alteration of records, and ERISA Compliance malfeasance. These risks are properly addressed in a Crime or Fidelity insurance policy, not typically in a cybercrime policy.

There is no denying that the threat of computer and cyber crime is real. Though the process of developing an appropriate insurance plan might be daunting – and yes require another insurance premium – the cost of a breach can be enormous or even put one out of business. Assessing the threat and vulnerabilities and putting a risk management and insurance plan in place can effectively provide predictability of cost and long-term security to a law or real estate practice.

John Torvi is the Vice President of Marketing & Sales at the Landy Insurance Agency of Needham, MA. He is a regular speaker and contributor to the legal, real estate, accounting and insurance professions. He can be reached at 781-292-5417 or at johnt@landy.com.