eBay, Target and the Maricopa County Community District. These three seemingly unrelated entities were recently in the news earning unwanted publicity for the same humiliating experience. “We were hacked,” the executives admitted.

These are not unsophisticated victims. Two Fortune 500 companies and a community district consisting of ten colleges - entities you’d think would have the financial and intellectual resources necessary to protect their data from hackers. And yet, names of customers and students, passwords and, in some cases, private data, including dates of birth, were all obtained surreptitiously. Theft of personal and/or financial data results in a great financial burden (according to the Ponemon Institute, data breaches cost, on average, $188 per stolen record) to those companies and institutions attacked, but also significant is the damage to their reputation.

Cybercrime losses are on the rise. The internet has made attacks possible from anywhere in the world. They offer low risk and high returns for criminals who are rarely caught let alone punished. A growing number of well-publicized data breaches coupled with the public’s growing concerns regarding protection of their private information has resulted in a snow ball effect -- the number of claims against large businesses and organizations increase daily. Meanwhile, the effectiveness of hackers to overcome physical and software security barriers has also dramatically increased. Most cyber attackers follow the path of least resistance.

In many cases, this means targeting the very businesses that can least afford to be hit. Struggling with far less financial and technological resources than any Fortune 500 company are community associations. Associations also face potential claims of negligence for failing to place greater safeguards on private data which can mean a huge exposure for the Board and the residents in the community.

For community associations, data breaches can stem from any number of causes such as accidental publishing of information, having their system hacked, an inside job by a disgruntled worker or vendor, a lost or stolen computer, lost or stolen media, or just poorly maintained security. The effects of a data breach generally take on one of two forms: **Monetary theft** (gaining illegal access to an Association’s funds and initiating an unauthorized fund transfer)and **Data theft** (gaining access to a treasure trove of personal information about residents in the community).

These two types of exposures are nearly always excluded on the Association's underlying package (fire & liability) policy, and therefore require specialized insurance coverage to address them.

Unauthorized funds transferred by an association employee *can* be addressed on a traditional crime policy; however, for the policy to respond, it must be tailored specifically for common interest development exposures by adding two important endorsements. The first endorsement redefines the definition of "employee" to include board members as non-compensated "employees" of the Association. The second endorsement would extend the definition of "employee" to include a "designated agent" (such as a manager) as an insured.

Unauthorized access by an individual other than an "employee" as defined above requires special "Computer Fraud" and "Funds Transfer" extensions which are only available when an insurance agent or broker has requested the broadened insuring agreements (#6 and #7) be added to the policy. These insuring agreements may have separate (typically lower) stated limits so be sure to talk with your agent/broker to understand what limits may apply to a given loss.

A hacker who successfully gains access to data on the Association's or management company's database triggers the need for coverages that a traditional crime policy wouldn't necessarily provide. Instead, a separate **Cyber Liability** policy would need to be procured. This could be a standalone policy or, in some cases, there may be a modest extension of coverage on the Association's D&O policy. In any event, there are three fundamental exposures which present themselves if such a breach of data occurs: (1) **Liability** for loss or breach of the data itself should the Association be sued for negligence (failing to properly care for data); (2) **Remediation** costs to respond to the breach, which could include expenses related to investigation, public relations, customer notification, and credit monitoring for impacted individuals; and (3) **Coverages for fines and/or penalties** imposed by law or regulation (carriers may provide a defense, but most carriers will NOT pick up the costs of any fines or penalties imposed by an administrative body). Cyber Liability policies are written on a Claims Made form so, embarrassment aside, Boards need to be very careful about putting the carrier on notice the minute a data breach becomes apparent.

Only by obtaining both a broad Crime policy (with all "insuring agreements") and a broad Cyber Liability policy could a community association be prepared for an attack by someone with criminal intent and even then, some costs will not be covered (such as the cost of establishing the amount of the loss).

Cyber threat actors often lay the groundwork with early reconnaissance. They know what to look for, where to look and all too often, the weak links in the potential victim's cyber defenses. Your data is more valuable than you think. Identifying potentially valuable data and how it could be vulnerable to well-funded, highly organized attackers is a great first step to determining the weakest links in your security system and highlighting what needs to be done to protect any assets. Steps an Association can take to prepare against cyber theft include: (1) regularly performing required operating system and web browser security updates; (2) use of complex passwords (combination of letters, numbers) and changing them

regularly; (3) downloading anti-malware and anti-spyware software and keeping it up-to-date; and (4) being careful not to open any attachment received from an unknown sender which might expose a computer to a Trojan horse.

Q: We hire a management company to help with the day-to-day management. The management company has the option of collecting the monthly dues for us using a web-based portal. As a part of the processing of the transaction, they collect and store unit owner's name, address and credit card info. I'm worried that we might still have liability. Could the Association's Board of Directors be sued if our management company's website is hacked?

A: Yes, we believe that it's likely both entities (community association and management company) could be named by any potentially impacted unit owner and, depending on the indemnification language in the management agreement, the community association may have an obligation to pick up 100% of the cost to defend and indemnify the manager.

Q: We have workers driving an Association-provided vehicle and we require personal information from each driver so we can run their driving record. Could the passing of driver's names, home addresses, birthdates and license numbers to our insurance agent/broker provide an exposure should an email account be hacked?

A: The kind of data you might unintentionally share is a virtual "cyber buffet" for any hacker. Obtaining this type of information could help a third party use your worker's personal information to assume the worker's identity, obtain credit and destroy the worker's credit history in the process. The Association might be held liable for failing to forward this information securely.

Q: In order to know the identity of people who wish to access our property, we require our security guards to request guests to relinquished drivers licenses for photocopying before accessing the premises. Does this create an exposure if those documents aren't properly disposed of (shredded)?

A: Yes, the community could be held liable for the neglectful handling of this personal information.

Q: Could a missing laptop or media storage device result in a loss of data (owner's names, addresses, phone numbers, email addresses)?

A: Laptops, thumb drives and portable hard disks are all extremely portable and subject to theft, but, quite frankly, so are iPhones, iPads and other tablet devices. Any of these devices that contain personal information (or can access a database containing such information) should never be left unsecured and must always be protected by a complex password which is changed regularly.

By Timothy Cline, CIRMS

Timothy Cline Insurance Agency, Inc.

For more information please visit us at: www.timothycline.com

or call us today at: (800) 966.9566