Don't be a Target . . . or a JP Morgan Chase, or a Sony.

It's not only big companies that have data security breach obligations.

By: Jay L. Hack, Esq., partner, Gallet Dreyer & Berkey, LLP January, 2015

Hackers throughout the world are after companies large and small, trying to steal personal information that they have on their computer networks. When Target or Home Depot gets hacked, it's a boon only to the US Post Office - millions of warning notices are sent to customers whose information was stolen and millions of new credit cards are mailed.

If you think this is not your problem and it can't happen to you, you're wrong. If your real estate company has sensitive personal information on your computers, you are subject to the New York State Information Security Breach and Notification Act. The real estate industry is governed by that law just as much as banks and major retailers. If your system is infiltrated, then you have to notify everyone whose data was compromised and send notice to government officials. Even if your company does not have data that the law requires you to protect, exposure of even unprotected data could damage your reputation and generate private lawsuits.

You should do your best to eliminate the risks of exposing that data. Consider each of the issues below. Experts say that it is not a matter of whether a computer connected to the Internet will be infiltrated; it is only a matter of when. You can't hide from the hackers and no management company is too small. Google has software that searches the Internet to find public information. Hackers have similar software that automatically goes from one Internet-accessible location to another, looking for vulnerable systems that they can infiltrate. When they find a vulnerable site, they attempt a quick smash and grab. If they find name and social security number data, they sell it to criminal syndicates that use it for identity theft.

As I said in recent presentations to both the banking industry and the real estate industry, you lock your car when you park on the street. Even though a thief can smash your car window and get inside, it is easier for the thief to steal from an unlocked car than to break your window. Your job, as a real estate professional, is to lock your car as best you can and let the criminals go somewhere else.

Therefore, we recommend that you consider the following action items to reduce your risk of future liability.

a. Encryption – Is the data on your computer encrypted so that it can't be read even if someone "hacks" into your system? If not, implement encryption.

b. Vendor Management – Make sure that any vendor who has your data has procedures to protect confidentiality of data you give them and be sure to include appropriate clauses in all vendor contracts.

c. Limit "Toxic" Data – If you don't really need a social security number or a driver's license number, don't ask for it. Never collect passwords or PINs belonging to other people. Once you have the data, keep it only for as long as you need it and then dispose of it properly.

d. Viruses and Malware – Make sure that you have software to protect your computers from damage by viruses, spyware, and other malicious code. Update the "virus definitions" on your anti-virus software regularly to protect against newly discovered malicious programs. Consider restricting the receipt of high risk file types (such as .zip files).

e. Cyber Insurance – Does your liability insurance cover loss from cyber-attacks? If not, consider buying a policy or rider. Read exclusions carefully to make sure that the policy does not contain loopholes.

f. Employee Training – Train your employees to be careful with the computer system and computer data. One common method of infiltration is to send a sophisticated email to an employee that looks like it comes from someone else in the company. Clicking on a link in the email inserts a virus into the network. In a recent test, 50% of all bank employees who got an email that looked like it came from the head of the IT Department replied by sending their password when they were told it was needed for a system update.

g. Board Training – Managing agents need to take the lead in training board members and officers to be vigilant. This is especially true of coop building directors who often receive personal information about prospective purchasers and subtenants. Directors should not download or keep "toxic" information unless it is essential for them to do so.

h. Access Limits – Not everyone needs access to your most sensitive data. If it is password protected, don't leave passwords where every employee can get to it.

i. Secure Internet Connections – Consider firewall protection. Be especially careful with Wifi connections. Always use password protected Wifi. Change passwords regularly so that "guests" with passwords can't use them once they leave. If possible, separate the network where confidential data is kept from any public Wifi you make available to guests.

j. Update Software – Install all patches issued by your software vendors. Patches correct system vulnerabilities. Avoid software that is no longer being maintained by the manufacturer, such as Windows XP.

k. Physical Access Limits – If avoidable, do not leave computers and network components in public areas.

l. Personal Web Browsing – Employees who want to browse the web should do so at home, especially if you do not have vigorous anti-virus software. Don't try to prohibit access to dangerous sites; you will never find them all. Instead, "white list" acceptable sites and limit access to other sites.

Jay L. Hack, Esq. is a partner in the law firm of Gallet Dreyer & Berkey, LLP. The firm has a substantial real estate practice and represents the owners of hundreds of commercial properties and more than 200 condominium and cooperative buildings. Mr. Hack's practice focuses on the regulation of banks and other financial institutions. He is the Chair of the Business Law Section of the New York State Bar Association, which is the second largest section, with over 4,400 members. He is also a member of its Banking, Securities and Derivatives committees. He is a graduate (with honors) from the University of Michigan and a cum laude graduate of Boston University School of Law. His article on the Federal Rules of Evidence in the Boston University Law Review has been cited as authority by the United States Supreme Court.

Jay L. Hack, Esq.
Gallet Dreyer & Berkey, LLP
845 Third Avenue
New York, NY 10022

jlh@gdblaw.com
www.gdblaw.com
(212) 935-3131
(212) 935-4514 (fax)