GlobeSt.com™

# How Should The Industry Approach Cybersecurity?

AUGUST 16, 2016 | BY CARRIE ROSSENFELD

IRVINE, CA—The best defense against a security breach is prevention, which starts with eliminating your business as a target by controlling access to sensitive information, Manly, Stewart & Finaldi's Morgan Stewart tells GlobeSt.com in this **EXCLUSIVE** story.

*Stewart: "There are many ways to control access to electronic information, eliminate risk and prevent a security breach."*

IRVINE, CA—Security-breach prevention starts with eliminating your business as a target by controlling access to sensitive information, **Manly, Stewart & Finaldi** partner **Morgan Stewart** tells GlobeSt.com. We spoke with Stewart, along with **Elliot Vermes**, CEO of **ResiModel**; **Norm Miller**, **Hahn Chair** of real estate finance at the **Burnham-Moores Center for Real Estate** within the **School of Business** at the **University of San Diego**; **David Tobin**, founder of **Mission Capital Advisors**; **Charles Clinton**, CEO of **EquityMultiple**; **Michelle Schaap**, a member of **Chiesa Shahinian and Giantomasi**'s media and **technology**, **construction** and corporate and security practices; and **Jorge Rey**, director of information security and compliance for CPA firm **Kaufman Rossin**, about how the industry should **cybersecurity**. Stay tuned for a more in-depth treatment of cybersecurity and big data in real estate in the July/August issue of ***Real Estate Forum***.

***GlobeSt.com: How should the industry approach cybersecurity when more and more of our industry is embracing technology and therefore open to risk?***

***Stewart:*** The best defense against a security breach is prevention, which starts with eliminating your business as a target by controlling access to sensitive information. Strategies might include holding sensitive materials in a separate, non-networked database; limiting employee access to sensitive information; disallowing the transmittal of sensitive information over electronic communications; and creating an employee manual that details the use, possession and protection of sensitive information.

There are many ways to control access to electronic information, eliminate risk and prevent a security breach. Computer hacker **Kevin Mitnick**, in his book *Ghost in the Wires*, offers these tips.

- Make the right IT investments to protect information, including firewall, virus protection and monitoring software.
- Update apps regularly.
- Secure laptops, mobile phones, tablets and other mobile technology with encryption software.
- Enable remote wiping, which allows your provider to erase information on mobile devices when lost or stolen.
- Establish strong passwords.
- Backup regularly to an external drive.
- Be smart when surfing the Web and downloading information: every “warning box” that appears should be taken seriously, and understand that every new piece of software comes with its own set of security vulnerabilities.
- Educate employees. They need to understand the importance of your company’s data and consequences of a breach, measures they can take to protect it and what they may be doing that is dangerous.

“One of the most difficult things to do is protect end users against themselves,” Watchinski concluded, “but ultimately, prevention is the best approach to handling your data security.”

***Hitchens:*** Companies need to understand that cybersecurity is a core component of the implementation of new technology. If you're employing technologies as a central component of your business, then you are, for all intents and purposes, a technology company. As a result, businesses should specifically seek out and hire technology professionals that focus on keeping information safe and secure.

***Vermes:*** One thing that is important to remember is that it is not only online applications that are at risk. Unless your computers are literally off the grid and completely disconnected from the Internet, your files are always vulnerable to hackers. It is extremely easy (and common) for hackers to send malware to PCs. The reality is that your data is much safer stored in a responsible **SaaS** application that is serious about security than it is when stored locally.

***Miller:*** There are several firms in Israel that have proven to be great at countering cyber-attacks, and there are a few in the U. such as **McAfee**. I suspect we will need to have numerous layers of safeguards and security to run the systems of the future. Many new firms will likely emerge to provide cyber safeguards and users will need to perform **due diligence** to determine which one to use.

***Tobin:*** Going forward, I think the standard for access to smartphones, laptops and desktop systems should be biometric, and we will likely see more fingerprint and retina logins. Similarly, transaction security will be enhanced with technologies such as **blockchain**. Systems are only as safe as the weakest link, and passwords are a weak link for a variety of reasons: written on paper, stored in an unsecure password manager or simply too simple and easily figured out. You cannot, however, steal someone's fingerprint or eyeball! Substantial resources have been dedicated to developing these technologies, and we'll likely see more implementation of these innovative approaches to cybersecurity in the near future.

***Clinton:*** Adopting something new always involve some level of risk; the question is whether the pros outweigh the cons. I don't think anyone is questioning the huge benefits that technology will bring to the industry. The necessity for cybersecurity will vary from business to business, but for those portions of the industry that hold valuable proprietary data, the first step is recognizing the value of that data and then taking the necessary steps to protect it. Luckily, there's already an entire industry dedicated to cybersecurity, so the **infrastructure** is already there. One very small example is web hosting—our platform is hosted by **Heroku** within**Amazon**'s secure data centers. Amazon has a level of security in their data centers that very few companies could hope to replicate, so leveraging their infrastructure is an enormous advantage.

***Rey:*** As the **commercial real estate** industry increases its reliance on technology, companies should start incorporating cyber security risk within their risk-management framework. For example, companies should consider the potential impact of sensitive information being stolen, whether it is tenant information or other sensitive information such as investment strategies, business plans, current or future investors lists and engineering drawings. The industry should start look to best practices from industries such as **financial services** and **healthcare** that have long been addressing cyber security. Best practices may include periodic risk assessments, vulnerability assessments, employee training and information-security programs tailored to the risks facing each company and the information they want to protect.

***Schaap:*** It goes without saying that any responsible company should (and, by law, is required to in many cases) implement appropriate security procedures—including both cyber- and physical security measures. Companies should ensure that they not only have firewalls and antivirus software, which offer protection against certain types of threats, but also that they have their sensitive data encrypted both at rest and in transit. Companies should audit their existing systems with qualified, outside vendors—not the personnel or vendors that designed the subject systems—to understand what sensitive data the company has, where it resides—physically and electronically—and how it is stored in relation to other company systems. Such outside vendors should also ensure that there is not already an undetected "presence" in the company's systems. Once tested (and redesigned, if appropriate), systems should be tested regularly (by "white hat" hackers) to test vulnerabilities. Where vulnerabilities are detected, measures must then be taken to redress them (consider the **Target** losses due to Target's failure to respond to its own notices that its systems are vulnerable).

Security efforts should also include people: Personnel must be trained to recognize **phishing**,**spearfishing**, and other improper efforts to gain unauthorized access to a company's systems. Employees should not be permitted to use unsecure devices (e.g. cellphones, PDAs and/or tablets) to transmit information of a sensitive nature. Proper personnel training on these critical security issues will thwart many bad actors' efforts to access company records and systems. Vendors that service a company must also be carefully vetted to ensure that, to the extent such vendors have access to company systems and confidential information, they, too, take appropriate security measures. If companies use “data rooms” and data-sharing cloud providers to facilitate the exchange of documents in due diligence, they must carefully review the terms and conditions of the sites and systems used to make sure that security is assured and that the company will remain the owner of its data at all times. Companies should also ensure that information is fully backed up, stored and quickly retrievable. If a company is hacked, or the subject of a ransomware attack, it must be able to restore business records and resume “business as usual” quickly. Absent such measures, companies may find themselves compelled to pay ransom to regain access to their valued data. Additionally, companies should invest in cyber insurance. But purchasing insurance without understanding the coverage and exclusions may leave the company unprotected—or without the level of protection it thought it had. Business-interruption coverage that is not part of a cyber-risk policy may not cover the losses incurred in a cyber-attack.

Companies must have an action plan for the “when” (and not the “if”). If a cyber-attack occurs, the date the attack is discovered is not the time to develop a plan of response. A comprehensive response plan should clearly identify all the necessary players, escalation procedures and outside parties—including law enforcement, insurance carriers, legal professionals and technology/forensic experts—so that the company can react immediately and responsibly. Having proper procedures, protections and action plans in place in advance can protect the company from a world of hurt. The last thing a company executive wants to explain is why the proceeds from a multi-million-dollar transaction have just been wired to an untraceable account in Russia