KeyBank
Real Estate Capital

Cyber Security Threats in the Real (Estate) World

KeyBank Real Estate Capital® presents this summary of the keynote presentation given by cyber security expert Eric O'Neill, Founding Partner, The Georgetown Group, at the 2016 National Investment Conference for Seniors Housing and Care (NIC).

What can a famous former spy teach the seniors housing industry? Turns out, quite a bit. Cyber security matters for all industries, and all executives—even those working in sectors like seniors housing. The last few years have seen dozens of high-profile server breaches of banks, retailers, healthcare systems, political organizations and government agencies. The personal and financial records of millions of Americans have been exposed; no site, no business, and no person are immune.

So explained Eric O'Neill, former FBI Counterintelligence operative, in remarks delivered at the 2016 National Investment Center for Seniors Housing & Care (NIC) National Conference.

Key takeaways

Espionage and cyber fraud are close cousins; the latter is a known real estate industry risk.

Cyber security impacts all industries, including seniors housing.

Typical cyber threats include spear-phishing, ransomware, fake emails, and social engineering.

Seniors housing organizations can reduce risk by educating employees about online fraud.

O'Neill, founding partner of investigative and security services consulting firm The Georgetown Group and national security strategist for Carbon Black, is a leader in next-generation endpoint protections. He drew from recent examples of security breaches to explain how highly protected corporations and organizations—and their customers' sensitive personal information—continue to be vulnerable to professional hackers.

On a more personal level, he also described his own experience working undercover as a member of the FBI Information Assurance division to expose and apprehend Robert Hanssen, who perpetrated the biggest security breach in U.S. history. Analysis of these notorious examples can help make your business and client records more secure.

Hackers aren't a Hollywood myth

O'Neill, whose own story was told in the 2007 feature film "*Breach*," told audience members not to accept Hollywood's depiction of hackers as unsophisticated, overweight loners who are pounding at their keyboards in their parents' basement. Instead, he said, "There are no hackers, there are only spies."

"Hanssen was the first U.S. hacker spy, says O'Neill. He exploited neophyte information systems at the FBI and CIA from the inside to trade secrets with first the Soviet Union, and then Russia, for more than 20 years."

> Today's hackers are part of highly intricate and interconnected networks of spies who are working from inside and outside organizations to identify vulnerabilities and use the information gleaned for financial and political gain.

The cyber "arms race"

O'Neill explained the inherent problem with the way companies approach cyber security, comparing it to physical security efforts after terrorist attacks. Following an onslaught of attacks using the same method—explosive devices planted in vehicles that were rammed into buildings—security efforts were focused on stopping future attacks of the same kind, by installing physical barriers around the perimeters of buildings.

In the same way, cyber security measures are caught in the same perpetually reactive loop. As information technologists develop ways to combat the types of cyber-attacks that have already happened, and companies address post-breach communications and fixes, hackers are actively identifying new vulnerabilities and developing new ways to attack.

It's important to understand what attacks are being used and empower security and information experts to develop ways to combat future attacks. Government and corporations need to "flip the script" to be proactive and stop future attacks. Below are some cyber threats O'Neill discussed:

"Spear-phishing" (e.g., Anthem attack, DNC hack)

Spear-phishing is a form of phishing that preys on familiarity—hackers scan social media for names, emails, and events that will be familiar to you, and send emails that look like they're from your legitimate contacts. For the Anthem attack, hackers were able to mine past LinkedIn data to determine the identities of data analysts at the second largest U.S. health insurer and targeted them to gain access to the system. The personal information of more than 80 million customers was compromised. The hack on the Democratic National Committee's email system during the 2016 election is another high-profile example of this type of attack.

Ransomware (e.g., Hollywood Presbyterian Hospital)

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money—typically bitcoin, which is untraceable—is paid. In 2006, Hollywood Presbyterian Medical System was the victim of such an attack that prevented hospital staff from being able to access records systems. In the interest of restoring its system as quickly as possible to not jeopardize patient care, the hospital paid the equivalent of $17,000 in bitcoin to the attackers. Ransomware is often used in targeted attacks on individuals and small companies, who will pay to release their systems and not report to law enforcement.

Fake emails (e.g., fake letters from CEOs, IRS authorities)

Other common scams being used by hackers include fake CEO emails, which are sent to employees of a company and look like they're from the executive's account; IRS scams, in which hackers pose as the IRS to get filing numbers and other financial information; and "grandchild hacks," in which the elderly are targeted by hackers who impersonate their family members.

Social engineering: Hacking people, not computers

O'Neill observed, "Amateurs hack computers, professionals hack people." He explained that hackers are using social engineering to cultivate targets and exploit vulnerabilities. By mining social media profiles and other publicly-available information, hackers learn their targets' routines, interests, locations, what they do for work, and what information they may access.

Ultimately, social engineering was also how O'Neill and an FBI team brought down Hanssen. By disrupting his routine and exploiting his hubris, they gained access to a device with evidence that eventually led to his arrest.

The work of seniors housing, investment, and real estate executives may not be as Hollywood-ready as that of a former covert agent like O'Neill, but cyber security is an issue that impacts everyone. Educating employees and clients about cyber threats can help prevent breaches. They should be aware of how the information they share online can be used to target them and should be diligent about making sure emails, "friend" and follower requests, and links are from legitimate, known sources.

In the facilities themselves, as smart building systems are implemented, new technologies offer sophisticated new functionality—but with it, some cyber security risks, as well. As this new era unfolds, commitment to securing systems must be a priority from the C-suite down at every organization.

To learn more about how KeyBank helps our clients guard against fraud with actionable suggestions, contact your Relationship Manager. You can also visit key.com/security or key.com/phishing

KeyBank
Real Estate Capital