Cyber-security The real estate industry is also at risk - Protecting your company

May 11, 2015 - Design / Build

Large multi-national corporations like Sony, Target, Home Depot, JPMorgan Chase and Anthem Health are recent victims of highly publicized data breaches but the threat is not limited to the retail, financial services or health industries.

The real estate industry is also at risk.

It's no longer a matter of if a company gets hacked, it's only a matter of when. My company, a New York-based cyber-security firm, specializes in computer and Internet security using many of the same techniques that the "bad guys" use to find data/security weakness in organizations. We help companies fix it and prevent security breaches.

It's our job to know what the bad guys are doing and how. I advise my clients to take more aggressive measures rather than merely react to events after the "worst scenario incident." Given the endless arms race between hackers and defenders, all businesses, large and small need to be proactive in securing the confidential information they maintain.

As a London native, I have over 16 years' experience in IT security, operations, control assessment and reengineering. Today, OccamSec's clients include a long list of prestigious clients including: Fortune 500 Companies and small to mid-sized companies in real estate, finance, entertainment, education and healthcare.

Here in New York, we recently worked with real estate company, ViewTheSpace, to improve the cloud-based office leasing and portfolio management company's organizational security and help further protect their data. The industry's increasing reliance on technology, such as commercial owners making portals available for rent payments, makes real estate players prime targets for hackers. Leasing agreements, rental applications and credit reports are just a few of the types of documents stored and shared by property managers, brokers, developers and appraisers that contain the sort of information cyber criminals target.

Cyber criminals can compromise an organization's information in multiple ways, including, hacking systems, installing malicious software, hijacking websites and phishing attacks.

On extreme cases, my OccamSec team and I have posed as bad guys and physically broken into clients' offices or placed an "undercover" team member inside a company's office to gain access to a client's computer to steal important corporate data. Since we were hired by clients to do the above, it's all legal, but the job has its own risks. We have been pulled over by law enforcement with firearms drawn, chased through stores and stopped at airport security. My luggage - overloaded with technical equipment (two laptops, antennas, wires, etc.) - often gets a second or third view.

OccamSec challenges the conventional approaches to information security. Our services are tailored for each client; we do not believe one size fits all since each organization is different. While OccamSec specializes in offensive techniques, we also provide defensive services as well because,

if we find a problem, we should have some idea of how to fix it.

Prior to founding OccamSec in 2010, I worked for UBS AG as the director of threat and vulnerability management and also at KPMG where I was a senior penetration tester and managed a variety of security engagements.

Before coming to the United States, I worked at a financial services company in London. My love for computers started when I was eight- years old. At eleven I saw the definitive "hacker" movie "WarGames" with Matthew Broderick as a young computer whiz who hacks into a government supercomputer. I thought hacking/security looked more interesting than just writing code, although I had no intention of trying to start a war.

Today companies employ a number of strategies to try to ward off attacks. There's no single solution. Every business needs to find its own configuration.

Mark Stamford is the CEO of OccamSec LLC, New York, N.Y.