SFBW
SOUTH FLORIDA BUSINESS & WEALTH
http://sfbwmag.com/2016/07/how-to-reduce-the-odds-of-a-cyberattack/

How to reduce the odds of a cyberattack

TECHNOLOGY | JULY 7, 2016
By Martin Lenkowsky

If you're worried about hackers launching a cyberattack against your business, your concerns are far from unfounded. In our increasingly high-tech world, there are too many bad guys out there devising myriad ways to infiltrate your company's most valuable information.

Cybersecurity experts advise businesses not to wait for a data breach to occur, but to start implementing battle plans in advance.

"There are many things you can do to reduce the likelihood of cyberattacks happening," says Marcum LLP's IT Risk Assurance Senior Manager Jose Antigua, who participated in a recent webinar entitled, "Cybersecurity: An Integral Approach." "The key is awareness, and that awareness should be taken into action."

Antigua encourages employers to involve all their employees in playing an active role in their security plan. "All positions with a job description should be made part of it," he says. "It should also be a part of their performance evaluation."

Reasons why hackers might want to infiltrate a business' stored data range from the most likely, economic, to even social or political causes.

Antigua says a "black market" exists for unscrupulous individuals to access stolen personal data. "Social Security numbers can be sold for $30," he says. "And credit card data is available for $12." Those two types of stolen personal data pale in comparison to a hackers' most coveted prize: a "full identity kit," which can bring in $1,200. "All information about an individual, including health information, bank accounts, even personal relationships, are included," Antigua explains.

Companies in the finance industry as well as retail chains have been the targets of choice for cyberattacks. Also, organizations storing huge amounts of personal data, such as health care providers, have also made tempting targets for hackers. Recent victims have included Staples, Home Depot and Anthem (Blue Cross). Two banking giants, Bank of America and Chase, were forced to retreat offline when they discovered a breach was ongoing.

The ability of a company to continue operating after being the victim of a cyberattack can be difficult. In addition to monetary loss, a business' reputation can suffer as well. "Sixty-four percent of small companies go

out of business six months after a data breach," Antigua says, adding that hackers take advantage of small companies with limited security resources.

Small companies should never consider themselves immune to attack. "Some people might think because they are small, they are not subject to an attack," Antigua says. In other words, all businesses are vulnerable.

As a crucial first step in reducing risk, a company needs to conduct a self-assessment. "What is the risk you have?" Antigua asks. "Hackers are not only out for money, but for information. You might have a lot of personal information."

He says a risk assessment is a necessity. Larger companies with bigger budgets can afford to hire a full-time risk manager, whereas smaller companies will not have that luxury. However, there are preemptive measures even a company with limited resources can implement. "You hire someone to do a risk assessment, including a vulnerability assessment," Antigua says. "You try to identify all your points of entrance. What are the ways hackers can get in?"

When business leaders realize their data systems are exposed, the next step is to determine how exposed they are and how they can defend themselves. "It could be a configuration issue," Antigua says. "You might need employee training."

"It's important to be proactive," says Stefan Chin, an attorney with the construction law firm of Peckar & Abramson. "It takes a team to put up a good cybersecurity fence. You need an IT department. Employers have got to get all employees involved."

Cybersecurity experts say once a breach is discovered, the first 72 hours are crucial to mount a counterattack. "You need to plug the hole first," Chin says. "Then you need to figure out what happened to the data. You can do most damage control early on."

Chin also says once a company discovers it has been the target of a cybersecurity breach, it should seek outside legal counsel to review all contractual obligations. Most states have stringent rules and regulations for companies whose data has been compromised. Customers often need to be notified immediately.

Hackers continue to devise new and devious methods of cyberattacks. A South Florida construction company was hacked last year. "They locked all the company's information and held it for ransom," Chin says. "They lock it so you can't get into it. They tried everything, but ultimately had to pay a ransom."

Another type of cyberattack is the changing or altering of information, says Jorge Espinosa, a partner in the Miami IP (intellectual property) law firm of Espinosa Trueba Martinez. An example of such an attack might be adding a few zeros to a bank account.

Espinosa says a company needs a "redundant security system" to combat cyberattacks. "You can't just rely on one," he says. "You want to make sure you have independent systems. Hackers are smart, they will keep trying."

Experts continue to warn that no matter how seemingly tough and impenetrable one's cyber defenses appear to be, there's a weak link in the chain, notably human beings. Some examples might be an employees who don't change passwords frequently, if at all, or choosing obvious ones.

Antigua says hackers have lists of commonly used password. In a "brute-force attack," hackers use software to try every possible alphabetical and numerical combination.

Hackers may pretend to be someone inside the company and send an official-looking email to a fellow associate asking for a money transfer between accounts, or possibly to a scam vendor account. However, they are not always successful. One of his clients had a simple safeguard in place to prevent falling for such an attack, he says. “They had a policy to call before any money was transferred to a vendor.”