Cyber Security – Guess What? You're the Target!
By Howard Green

What's an example of a cybercrime? The break-in happened on a Friday night. It always does. And by 5 am Saturday morning the damage had been done. A 100 employee Canadian retail-related company was mercilessly hacked. It was a five-day horror show for management and almost wrecked the company. Computer systems were no longer operational and everything was gone. The crooks even compromised the backups. In the ever-expanding annals of cyber-crime, it was a so-called "brute force" attack. The company's servers had been exposed and were directly accessible. The hackers kept assaulting the system, "guessing" at countless passwords with automated attacks until finally they "got in", giving themselves system access. The crooks then took control of the company's computers by encrypting critical systems---including the backups---and demanded ransom of approximately $30,000. They wanted a "donation" in impossible-to-trace bitcoins. But bitcoins aren't easy to access, particularly on a weekend. You have to go to an exchange and prove you're not laundering money or engaged in other illegal activities. Inside this all-too typical case, it felt like strangulation.

Then what? Eventually, after paying ransom in painful increments, the company got bits and pieces of its system back. But each time it paid, the crooks wanted more money. Unfortunately, the welcome mat had been visible.

So, it cost the company $30,000? No. The ransom was just the tip of the iceberg. The company then had to pay an IT company to deal with the hack. It lost business for five days, lost a major executive, suffered a reputational black eye and legal costs. It could have gone under. And it's not alone. Every company is under attack---all day, every day. According to cyber expert Brian Everest of cyber724.com, there may be 65 000 or more attempts per day by hackers to get into *your* system. Losing your business or your job are very real potential outcomes. "Cyber threats are the biggest off-balance sheet liabilities that organizations of all sizes have ever faced" Everest added.

Why would anyone hack me---aren't the bad guys after big companies with lots of money? Fact: more than half of cyber crimes are committed on insurance claims come from small and mid sized enterprises according to specialist global insurer Hiscox. And many crooks are satisfied with a $30,000 take rather than $30 million. If they can extort $30,000 from a handful of small or medium-sized businesses every day, all month long, year after year---that's a lot. And it's easier to hide if you steal modest amounts.

What are the characteristics of cybercrime? Up to 45% percent of cybercrimes involve a human element, allowing thieves to break in. It can be as simple as someone calling and masquerading as someone they're not---like a phone company employee---and asking for your password. People are caught off guard and simply reveal their passwords to the fraudster on the other end of the line---or to the distraught "pregnant" woman who shows up at their office "needing" to plug-in her smartphone. Over fifty-percent of people will let it happen. Managers will reveal administrator passwords, without verifying the identity of the person who asked for it. Sometimes the crooks will direct you to people who'll do the fix. And those "good guys" are actually in on the heist and get a cut. Sometimes it's the latest ransomware---software that hops from computer to computer, locking your system with the highest levels of encryption, giving hackers a vise-like grip on your business.

What are some of the simplest mistakes that make you vulnerable? Some people put up post-it notes by their desks---*with their passwords on them.* Not only that, they have the word "password" written there too, like a big fat arrow! Talk about a welcome mat. People also use ridiculously simple passwords, such as "password" or "abc123", or some variation of that. Passwords should be at least 16 characters, with all sorts of variations and symbols within them. Sometimes even well-disguised webpages fool us, almost perfectly falsified to look like the real thing. Amazon look-alike pages, for example. You enter your username and password and they've got you.

Will I know if hackers get into my computer or server? The scary thing is they might be there for months---watching, observing, casing the joint, so to speak, before they attack, take you hostage and ask for payment. And they can hide. The crooks' faces don't get caught on security cameras like when a 7-Eleven is robbed.

How sophisticated are these hackers? Very. Many hacking "firms" run their operations as "legit" businesses, believe it or not. "They have *divisions*---hunters who prospect for new targets, others who mastermind two million password guesses a week," said David Poulson, President of Starport Managed Services

in Toronto. Those are the break-in specialists. Then there's the division that tries to shake you down for the money. They're very systematic, Poulson said, "they even have 'help desks'!" In many cases, these are state-sanctioned operations. At the other end of the spectrum, biker gangs are hiring online goons to steal from you online.

Why are many small or medium-sized businesses hesitant or resistant to get protection---or follow advice about cyber security? They don't think they have the budget for it. And they don't want to inconvenience their users or customers because the more secure you are, the more inconvenient it is when users or customers try to log-in. Often businesses view themselves as generic---not banks with big vaults of money---and they can't imagine being targets.

How can I protect myself and my business? First of all, awareness. Accept the reality that you're vulnerable. Learn what *not* to click-on, make passwords more secure and don't give them out to anyone. And remove the welcome mat. The fact is, most hackers are lazy. They want hassle-free heists. Think about it. If a thief comes down your street, he'll go for the house with the welcome mat, rather than the moat. Same with your computer or server. Everest also said "You don't need perfect security, but enough to convince the crook that his time is better spent elsewhere". In the old days, people never locked their doors. Now everyone does. Your computer systems should be like your home: secure.

Isn't it expensive to protect yourself? Basic cyber security can be very affordable, Poulson said, particularly when compared to the alternative. "Companies of all sizes need to secure their data, monitor and report on network traffic, train and educate all their staff and securely and reliably back up their data with advanced appliances like Datto's dedicated backup products," he added. Cyber security should be viewed as prudent risk-management to protect against a potentially devastating crime that could wreck your business over the span of a weekend. Your business requires that protection, by the way, to qualify for cyber insurance. Best not to wait for the Friday night when all hell breaks loose.

Howard Green is a Toronto based broadcaster, author and business journalist. He can be reached at: howardgreen.com