THE GLOBE AND MAIL

April 5, 2011

Major law firms fall victim to cyber attacks

By JEFF GRAY
From Wednesday's Globe and Mail

The law business gets a nasty reminder of the perils of the computer age after hackers breach defences at four Bay Street firms

Hackers have penetrated four major Bay Street law firms in the past seven months with highly sophisticated cyber attacks designed to destroy data or to steal sensitive documents relating to impending mergers and acquisitions.

Daniel Tobok, president of Toronto-based Digital Wyzdom Inc., who investigated the attacks, would not name the firms. The attacks, which he said appeared to originate from computers in China, show that Canadian law firms are a target for hackers and potentially, state-sponsored cyber espionage. They follow similar attacks on governments and major corporations in recent years.

"They were harvesting information," Mr. Tobok said of the hackers who penetrated the computers of the four Toronto law firms. He said it was hard to say if any sensitive data actually went missing, but said the attacks were at least successful at getting inside the firms' systems. "This was probably one of the most sophisticated attacks we have seen."

In the most devious attacks, Mr. Tobok said, lawyers at a major Canadian law firm working on a proposed deal involving the acquisition of a Chinese company received e-mails that appeared to be from a partner working on a deal. The e-mail was a fake, and its attachment launched a hidden computer program known as malware that infected dozens of the law firm's computers.

The attack was traced to computers in China, but Mr. Tobok said it was not possible to be certain that the Chinese government, or an element of the Chinese government, had a hand in the attack.

Malware of this kind can sit in a target's computers undetected for months, Mr. Tobok said, stealing reams of information before anyone realizes security has been breached. And there is no question that sensitive information stolen from a law firm's files on an impending merger deal has value: It could be used to sabotage a deal, it could sold to give rival bidders an advantage, or it could be used to conduct illegal insider trades.

Mr. Tobok said some in the legal world have been slow to realize just how serious the hacking threat is, although he said IT departments are doing the best they can. "Sometimes they have a false sense of security," he said of companies in general. "After they get attacked, they understand that they have to invest a little more."

Hugh MacKinnon, chief executive officer of Bennett Jones LLP, said he was not aware of his firm ever falling victim to a hacking attack. He said the growing importance of keeping the firm's data safe has prompted it to take a number of measures, including the recent move of all of its computer servers to a third-party, off-site security facility.

He said Canadians in general tend to underestimate the threat from malicious threats such as cyber attacks: "We're Boy Scouts, right? We tend to think that the rest of the world is comprised of Boy Scouts, and it's not."

David Craig, national information security practice leader for PricewaterhouseCoopers Canada, said law firms are a natural target for hackers because they are storehouses of information of interest to everyone from organized crime to spouses in marital disputes. But he said law firms tend to be extra careful about confidential information. Large firms usually have sophisticated IT staff and policies in place to try to keep data secure.

"Problems typically arise when those policies are violated for expediency, such as copying data to a flash drive and then misplacing it, or using a commonplace password that can be easily guessed," Mr. Craig said.

Of course, law firms are not alone when it comes to cyber attacks. On Tuesday, for example, word emerged that e-mail addresses of millions customers of major retailers had been compromised when a Dallas marketing firm, Epsilon, was hit by hackers. Best Buy and the Air Miles Reward Program were among companies sending out warnings to customers.

Earlier this year, it was revealed that several federal Canadian government departments had been hacked. Oil companies, the Pentagon, even Google Inc., have been hit. China's government has denied any involvement, but defence and security experts have long speculated that the Chinese military or other Chinese agencies could be behind such attacks.

The U.S. Federal Bureau of Investigation has repeatedly warned law firms that they are a target. Last year, a Los Angeles law firm representing a U.S. company in a $2.2-billion suit against the

Chinese government and two Chinese computer firms said it was hit by hacking attacks from China.

Hackers have also targeted law firms and others engaged in the fight against websites that offer access to pirated movies, music and video games. Last year, a British law firm that was targeting illegal file-sharers was hounded by cyber-attacks.

For now, IT experts and hackers are engaged in a computer-code arms race. Mr. Tobok's firm, which has 80 employees in Toronto, stores malware that it finds in its clients' computers in its lab and tries to analyze just what the hackers were trying to do.

"We contain them and we play around with them," Mr. Tobok said of the malware programs. "It's like having a cobra in a cage. ... We actually try to see what it's going to do."