World Bank Under Cyber Siege in 'Unprecedented Crisis'

Friday, October 10, 2008

By Richard Behar

FOX NEWS

The World Bank Group's computer network — one of the largest repositories of sensitive data about the economies of every nation — has been raided repeatedly by outsiders for more than a year, FOX News has learned.

It is still not known how much information was stolen. But sources inside the bank confirm that servers in the institution's highly-restricted treasury unit were deeply penetrated with spy software last April. Invaders also had full access to the rest of the bank's network for nearly a month in June and July.

In total, at least six major intrusions — two of them using the same group of IP addresses originating from **China** — have been detected at the World Bank since the summer of 2007, with the most recent breach occurring just last month.

In a frantic midnight e-mail to colleagues, the bank's senior technology manager referred to the situation as an "unprecedented crisis." In fact, it may be the worst security breach ever at a global financial institution. And it has left bank officials scrambling to try to understand the nature of the year-long cyber-assault, while also trying to keep the news from leaking to the public.

The crisis comes at an awkward moment for World Bank president Robert Zoellick, who runs the world's largest and most influential anti-poverty agency, which doles out $25 billion a year, and whose board represents 185 member nations. This weekend, the bank holds its annual series of meetings in Washington — and just in advance of those sessions, Zoellick called for a radical revamping of multilateral organizations in light of the global economic meltdown.

Zoellick is positioning himself and the bank as an institution that can help chart a new path toward global financial stability. But that reputation, more than ever, depends on the bank's stable information infrastructure.

The fact that the information vaults of the World Bank have been repeatedly pried open won't help Zoellick's case.

While it remains unclear how much data has been pilfered from the bank, it's a lot. According to internal memos, "a minimum of 18 servers have been compromised," including some of the bank's most sensitive systems — ranging from the bank's security and password server to a Human Resources server "that contains scanned images of staff documents."

One World Bank director tells FOX News that as many as 40 servers have been penetrated, including one that held contract-procurement data.

Despite the gravity of the break-ins, the bank is trying hard to pretend to outsiders it didn't happen. "There were attempts to hack the bank's computer systems last summer," says a World Bank spokesman. "However, there was no compromise of confidential information." Requests for on-the-record interviews with Zoellick and other top officials were declined.

Meanwhile, the bank's treasurer, Kenneth G. Lay, has been briefing Zoellick's senior management team regularly on the situation since April.

Other bank officials are also sleuthing. The bank's chief information officer, Guy De Poerck, has engaged Price Waterhouse Coopers to do a confidential million-dollar assessment that is expected to tell him what's going on in his own department. And a 22-page internal report by a computer security company named MANDIANT, dated August 18, fleshes out many details of the June-July breaches. But very few people have ever seen the report, and nobody has been permitted to retain a paper copy.

At the same time, De Poerck has been downplaying the problem to the bank's 10,000 rank-and-file staffers as mere intrusion "attempts" in his e-mails. Yet most of those staffers have been asked to change their password three times in the past three months.

"As previously reported in mid-July," CIO De Poerck and a senior bank treasury official wrote in an August announcement to employees, "we would like to reassure you that there is no evidence that Bank staff personal information is at risk from the recent external attempts."

It's unclear how that statement squares with an internal memo to De Poerck a month earlier revealing that a sensitive Human Resources server "that contains scanned images of staff documents" had been successfully breached. De Poerk declined to comment to FOX News about any of these details.

• Click here to see De Poerck's memo.

In reality, the situation is serious enough that federal investigators have been called in. "We're not talking about hackers playing games or messing up our website," insists a senior member of the bank's IT department at its Washington headquarters. "It's about the **FBI** coming last summer and saying, 'You should take a look at your systems because we think something weird is going on.' It's about the intruders knowing what information they wanted — and getting to it whenever they wanted to. They took our existing data stores and organized them in a way that they could be easily accessed at will."

In plainspeak: "They had access to everything," says the source. "They had the keys to every room at the bank. And we can't say whether they still do or don't until we fully and openly address what's happening here."

The data raids are not a matter of stealing inconsequential bits and bytes. The World Bank's data center is literally a treasure trove of vital financial information from around the globe. As a clearinghouse for financial data from both governments and companies, the bank's computers could provide intruders with both a financial and intelligence gold mine — from inside information on bids and contracts to the minutes of confidential board meetings.

If the bank takes a position in a **currency**, for example, that currency usually moves in response to the bank's actions. Stocks and bonds can also swing up and down based on World Bank announcements. "If you know beforehand that the bank is going to put an order in for oil pipelines in Chad or healthcare systems in India, you can actually make a good amount of money," says one insider.

Although the bank typically provides only a fraction of the financing for a project, its influence on those projects is immense. Private corporations see the bank's stamp of approval as a guarantee that their own larger investments will be safe — and profitable. Knowing in advance what projects the bank's board will reject could be just as profitable.

Some insiders fear that contractors — perhaps even governments — might be seeking advance knowledge on the status of the bank's anti-corruption probes. "The bank knows the books of countries almost as well as the countries do — including the corruption at times," says one insider.

The first breach of the bank's secrets was discovered in September, 2007, after the FBI —while at work on a different cybercrime case — notified the bank that something was wrong. The feds pointed to a part of the bank's network that led out of the Johannesburg hub of the International Finance Corp. (IFC), a bank arm that lends to the private sector.

Within a week of the tip, teams of bank investigators sent to Johannesburg discovered that intruders had gained full and total access to all of IFC's worldwide information — including all incoming and outgoing e-mail — for at least six months. "They were downloading everything and anything," says one insider, who says that IFC's monitoring systems were extremely weak. "They [intruders] had full access."

Investigators discovered that the intruders were using a so-called "cluster" of IP addresses from Macao, China. But since those addresses can be spoofed (i.e., disguised) the discovery doesn't prove that the breaches actually originated in China. Nonetheless, bank officials and its executive director for China clashed behind closed doors over whether or not China's government is involved in the break-ins.

Bank sources tell FOX News that Johannesburg is one of several secret "hubs" containing a "common data store" (or CDS) that the World Bank Group has established around the globe. In layman's terms, a CDS is the cyber-world's version of a bomb shelter where every piece of an organization's data is replicated and backed up in case of a data-

wipeout at headquarters in Washington. While it's known that IFC data was accessible at the hub, it remains unclear if all World Bank Group data was compromised there.

The second major breach — of the bank's treasury network in Washington — was discovered in April 2008. The World Bank's Treasury manages $70 billion in assets for 25 clients — including the central banks of some countries. It carries out substantial collaborations with the world's finance ministers on public wealth and debt management, runs an active bond-trading desk in Washington, and does everything from currency trading to capital markets financings.

After a forensic analysis of the treasury breach, bank investigators discovered that spy software was covertly installed on workstations inside the bank's Washington headquarters — allegedly by one or more contractors from Satyam Computer Services, one of India's largest IT companies.

The software — which operates through a method known as keystroke logging — enabled every character typed on a keyboard to be transmitted to a still-unknown location via the Internet.

Upon its discovery, insiders report, bank officials shut off the data link between Washington and Chennai, India, where Satyam has long operated the bank's sole offshore computer center responsible for all of the bank's financial and human resources information.

Satyam was also banned from any future work with the bank. "I want them off the premises now," Zoellick reportedly told his deputies. But at the urging of CIO De Poerck, Satyam employees remained at the bank as recently as Oct. 1 while it engaged in "knowledge transfer" with two new India-based contractors.

Satyam — one of the largest and most prestigious IT companies in India — is publicly listed on the NYSE and boasts having $2 billion in sales and more than 150 Fortune 500 companies as clients. In 2003, Satyam — it means "truth" in Sanskrit — won a much-heralded and lucrative five-year "sole source" contract to design, write and maintain all of the World Bank's information systems.

The contract — which began at $10 million and grew to more than $100 million by 2007 — was suddenly not renewed this year. Satyam so far declines to comment.

Then came the June-July breaches in Washington. They were similar to the Johannesburg attack, as the same group of IP addresses from Macao were used.

This time, however, the cyber-burglars used a different spyware. They broke into an external server run by the bank's private sector development unit. They were able to acquire passwords — including the password for the systems administrator.

That enabled them to jump into the servers at MIGA, the bank's giant insurance arm. It was there that they captured the security administrator's password as he was logging on to his computer.

It took ten days for bank officials to detect that they'd been invaded. Once they did, they shut down all external servers, except for e-mail — which it turns out the invaders were already using as their entrance point. By the end of July the invaders "had completely mapped out the topography of the bank's information systems," says one expert — "where everything was, the types of servers, and the types of files on the servers."

What the intruders did with all that information is the World Bank's most sensitive and painful mystery. It has clearly left the institution in a highly vulnerable position.

And the same may go for bank president Zoellick. Bank insiders say that he needs desperately to get the security of his own house in order. Despite the vast sums that the Bank spends on data and data storage, its information systems are deeply in disarray.

Today the total cost to maintain the bank's information infrastructure is at least $280 million per year. But according to one disgruntled bank staffer, "We don't even have an internal search engine that works."

The truly alarming fact, however, is that someone — or many people — seem to know their way around the bank's most valuable resource very well, even though they aren't supposed to be there at all.

UPDATE: After FOX News published its story, a World Bank spokesman issued the following statement:

"The Fox News story is wrong and is riddled with falsehoods and errors. The story cites misinformation from unattributed sources and leaked emails that are taken out of context.

"Like other public and private institutions, the World Bank has repeatedly experienced hacking attacks on its computer systems and is constantly updating its security to defeat these. But at no point has a hacking attack accessed sensitive information in the World Bank's Treasury, procurement, anti-corruption or human resources departments."

FOX News stands by its story.