

San Francisco Hack: Where Was the Oversight?

By Andy Patrizio

July 23, 2008

San Francisco Childs Hack

If the City of San Francisco were a public corporation and allowed a blunder on par with the recent Terry Childs case, it might find itself facing federal investigation and Mayor Gavin Newsom might be fighting to stay out of jail, experts said.

Security experts contacted by InternetNews.com expressed dismay at the apparent lack of best practices in the city's IT department -- practices commonplace in the corporate world that they think may have stopped the debacle from happening.

Childs, a 43-year-old computer network administrator for the city's Department of Technology, was arraigned on four counts of computer tampering more than a week ago.

He faces allegations of tampering with the city's FiberWAN (Wide Area Network) network, which holds records such as e-mails from city officials, city payroll files, confidential law enforcement documents and jail inmates' bookings (presumably now including his own).

Childs reportedly created a password that gave him exclusive access to the system. When the police demanded the password, he gave them a fake one, and later refused to give the proper password even when threatened with arrest.

At his arraignment, Childs's attorney, Erin Crane, told the San Francisco Chronicle he was prepared to give up the password last week.

Childs finally gave up the password on Monday, July 21, when Mayor Newsom went to the jail himself to meet with Childs and his attorney. Since then, according to Ron Vinson, chief administrative officer and deputy director of the San Francisco Department of Technology, the city has been able to regain full access of FiberWAN and change the passcodes Childs put in place.

Childs is still being held on \$5 million bail, a sum his attorney has called "crazy." A spokesperson for District Attorney Kamala Harris declined to comment when contacted by InternetNews.com. Crane did not return repeated messages seeking comment.

Worst practices?

Raffael Marty, chief security strategist for security and compliance provider Splunk, said security best practices were clearly not applied to the city systems.

“You don't want to have a single person holding the key to the kingdom,” he told InternetNews.com.

“I have heard that he was the focal point for everything, and that's incredibly bad practice to put everything in one person's hand,” Marty added. “It seemed no one else had the information he had. There seems to be no emergency planning. What if he was hit by a bus? From a security standpoint, this is horrific.”

The sentiment from Gartner security analyst Avivah Litan is “we told you so.”

“It just goes to show everything Gartner's been trying to tell its clients is true,” Litan said. “You've got to lock down privileged users' activities. You've got to monitor them.”

“There isn't sufficient monitoring of employees,” she added. “Most want to look the other way when it comes to employee activities, whether it's fraud or malicious activities. They don't want to admit they have a problem, so they don't want to work at solving a problem.”

How Childs got away with so much is still unclear. In a Chronicle story, Mayor Newsom said Childs “got a bit maniacal.” Vinson declined to comment on that statement, but did say that the city was attempting to implement best practices to prevent such a problem, “however, it appears that he was rebelling against them,” he told InternetNews.com

Indeed, while most companies fear the external hacker breaching their walls, employees are often the ones to blame -- whether it's activities by someone like Childs or sloppiness as in cases like TJX, where files containing millions of customer records were breached due to weak security.

“The problem with this high risk-user group [IT professionals] is 86 percent of all internal attacks come from a current or ex-technical employee,” said Cheryl Traverse, CEO at security appliance vendor Xceedium.

Traverse said companies often take a walled approach to security -- keeping outsiders locked out, but letting those within that wall roam freely, rather than being kept in place. The Childs case was an example of that, she said.

“You have to be able to create a compartment where people can work and do the job they are supposed to do, then you need to contain those people to the compartment they are supposed to be in,” she added.

“It all comes down to access and enforcement of the policy and alerting and containment,” Traverse said. “If they had containment and alerting, he wouldn't have gotten to where he got, and if he did, it would have said ‘Oops!’ and alerted his bosses.”

Childs, described as very adept in the Chronicle reports, was a go-to guy for all kinds of problems and thus had a great deal of access. Splunk's Marty wonders if anyone else in the city department even knew what was going on.

“It seemed to me that they don't have the slightest idea what is happening on their networks -- they don't know how to go about cleaning things up,” he said. “And it scares me a little because it seems the information on that network seems to be fairly important.”

Marty added that if another user can get physical access to a network infrastructure, it is possible to safely reset systems and services.

But he adds the city doesn't seem to know which systems are impacted, making this task difficult.

Cisco Systems (NASDAQ: CSCO), which provided the networking infrastructure, declined to comment on the story beyond acknowledging that it is working with the city to restore its access.

More security, more accountability

Even after other network administrators get access to the network, Gartner's Litan noted the systems will need a complete rebuild because there's no way of knowing what booby traps Childs may have left behind.

“Even if they get the password, they can't use the systems as they are,” she said. “They are going to have to rebuild those from scratch because who knows what he left behind, and that can get really, really expensive.”

The city is doing just that, Vinson said. “Our major concern is making sure that we have everything under control, keeping the system fully functional and operable,” he said.

The City will also continue to look into improving its internal security practices. “I think as part of our ongoing efforts to beef up our security, this is something we will look at,” he added. “We will look at best practices as relates to the network and monitoring the network. We have embarked with outside vendors on a vulnerability study and are looking at an architecture study as well.”

So far, however, the costs to the City of San Francisco, high-tech capital of the world, seems to have been limited to making it something of a laughingstock -- or a cautionary tale.

But the impact of a similar incident on a public company would have been much more devastating, experts said.

“If it's a public company, your reputation goes down the drain and your stock price will go down,” Marty said. “Your executives would be held responsible and could possibly go to jail.”

Litan thinks more people than just Childs needs to be held responsible.

“It should be the whole organization,” she said, adding that Child has been used as a scapegoat. “He shouldn't be allowed to get away with this,” Litan added. “I don't understand how someone could get so much access.”

Update adds comments from the city's Department of Technology office.