Code Green: Goldman Sachs & UBS Cases Heighten Need to Keep Valuable Digital Assets From Walking Out The Door. Millions in Trading Profits May Depend On It.

Securities Industry News
July 20, 2009
By Katherine Heires

Both Goldman Sachs and UBS have filed charges against former employees they allege stole proprietary computer code key to their high-speed trading programs, now the most tactical and strategic weapons on Wall Street.

The two cases raise questions about the need for increased security to prevent employees from literally walking out the door with valuable digital secrets. And they shine a spotlight on the need to protect profits by preventing the copying and reuse of these codes and the trading strategies they embody

In the Goldman case, charges were brought against a former vice president for equity strategy and computer programmer on July 3 for allegedly copying 32 megabytes of the bank's trading codes and uploading them to an encrypted server before sending them to a home computer and other devices. In the instance of UBS, the firm confirmed on July 13 that it filed papers in March charging three ex-employees with "misappropriation of trade secrets," specifically the misappropriation of 25,000 lines of source code for the firm's high-speed, algorithmic trading programs.

These two events have not only highlighted the value of these codes to the firms' bottom line-in the case of Goldman, "many millions of dollars of profits per year," according to court papers-but, in the assessment of security experts, they have also brought out the need for proper policies and even more rigorous security programs in place to protect financial firms from data breaches caused by trusted employees with access to highly profitable but microscopic assets. At a security desk in a trading firm's lobby, there's not a lot of checking of what goes in and out of the building on memory sticks, cell phones, iPods or in paper notebooks.

To date, security experts have largely praised Goldman and UBS for their ability to detect breaches to their systems fairly quickly.

In the instance of the Goldman Sachs case, "it appears that they are already doing a lot that is right," says Daivd Etue, a vice president of products & markets at Fidelis Security Systems, a Waltham, Mass. based provider of data leakage prevention (DLP) software designed to prevent the loss of corporate data or critical intellectual property at corporations.

"They had a pretty comprehensive security program in place. We know from the court filings that they were able to detect that a data breach had happened; they were monitoring email; they had blocked ftp file transfers to make it more difficult for people to send things out of the network, and they had started to monitor the use of secure Web browsing; it's just not clear whether or not or not they had the ability to actually stop the data breach from occurring," Etue said. In most instances, companies that experience data breaches do not discover until many months later that a breach has actually occurred, according to Etue.

"Hats off to Goldman and UBS. Obviously they have some good security procedures in place," said Larry Ponemon, founder of the Ponemon Institute, an independent research and consulting firm based in Traverse City, Michigan. But the leaks indicate the need for tighter security.

The fact that Goldman's proprietary code was sent to another, password-protected site raises questions about the scope of a possible data breach, said George Wade, a director of computer forensics at consulting firm Sobel & Co. in Livingston, N.J.

"The moment it gets out, all that you need to do is pass the password to someone else; someone can even access the information from a mobile phone so it's not just a matter of closing the barn door on your intellectual property but determining, what other doors and windows may still be open," he said.

Ponemon points out that employees leaving a firm may not even see themselves as thieves. "We increasingly see people thinking that intellectual property they have worked on at a company is theirs and so, they will simply try to remove it," Ponemon said.

Breaches are widespread. According to a study released in July by Ponemon and PGP Corp., 85% of the 997 U.S organizations surveyed had at least 1 data breach in the last 12 months. Companies suffering more than five data breaches rose to 22 percent in 2009, up from 13 percent in the 2008 study.

Additionally, Ponemon reports that 59% of ex-employees admit to stealing confidential company information when leaving or losing a job; 53% said they had downloaded employer information onto a CD or DVD; 42% onto a USB drive and 38% sent attachments to a personal email account. Also, 79% percent said they took data without an employer's permission and 24% said they continued to have access to their employer's computer system or network after leaving.

Kevin Rowney, founder of the data loss prevention division at security software company Symantec, says developers of high-value, intellectual property such as quantitative trading strategies "consider their work-the code they worked on or the models that they have developed-as theirs and not the property of the bank; It's a blurry line for many employees as to who is the actual owner of intellectual property."

The answer is to raise the level of security procedures and training in place.

"Events such as these show how you really need to put multiple layers of protection in place because any one technology can be circumvented," says Paul Giardina, president of Protegrity, a Stamford, Conn. security consultancy that works with many financial service firms.

For John Calvin Slemp, managing director for global security at Protiviti, a consulting subsidiary of Robert Half International, it all starts with having a comprehensive security policy and making sure that everyone in your organization-including your vendors and partners-understand what the firm considers to be sensitive information, how people should deal with this information and what tools should or should not be used. "In an environment where employees are constantly concerned if they have a job the next day, people start to look for opportunities to help market themselves with a new employer and may do stupid things," Slemp said.

A Deloitte report on "The People Dimension of Security and Privacy" issued earlier this year suggests that organizations make security training a quarterly event, to keep security at the forefront of people's minds.

However, multiple layers of technology are also an approach that security experts see as effective in thwarting data breaches of a highly sensitive nature.

"Organizations need to consider new and enabling technology that can at least provide alerts when something screwy is going on," Ponemon said. He cited three categories of technology as essential to protect against intellectual property theft:

1. Data loss prevention software that allows firms to assess the movement of information leaving the corporate perimeter or being moved by a trusted employee, for example, when it is downloaded to a disk or a memory stick. "These types of systems are very accurate and are extraordinarily helpful to companies trying to protect against the loss or theft t intellectual property," Ponemon said. Firms such as Fidelis Security Systems, McAfee and Symantec are providers of such software.

2. Correlation management software that constantly monitors and assesses unusual events on a network can be helpful as well. "Such tools allow you to create a surveillance record of the environment in which people operate, functioning as a kind of private CIA force within your company," Ponemon said. "If you're a programmer and you decide to try to send the trading system you have been working on to your home computer at an unusual time of night, the system will be able to detect that," he added. He mentioned ArcSight as a provider of such software.

3. Compartmentalization, using software provided by firms such as Compuware that can control the level of access that company employees can have to important code. "The software has a way of masking and disguising information so that if you are on the IT testing side, you don't have full access to the company's crown jewels," Ponemon said. His company's research shows that IT departments are responsible for more than half of all data breach threats caused by insiders.

Cyber risk intelligence units are yet another approach companies are employing to protect against the theft of intellectual property, says Ed Powers, a principal in the security & privacy services practice at Deloitte & Touche LLP.

"These are investigative units in organizations that actively monitor the actions of privileged users who have access to intellectual property," Powers said. Such teams often have backgrounds in computer forensics and behavior modeling capabilities and will study patterns so that they can tell when an event is likely to occur and can block that event beforehand.

"An individual really has to do a lot of work to cover their tracks when they try to remove information from a computer," according to Keith Jones, a founder of Jones, Dykstra & Associates, a digital forensics investigation firm in Columbia, Maryland. "There are so many spots on computers today where evidence is hidden that even experienced programmers might not think about or keep in mind."

For example, someone copying information from a company laptop to a thumb drive might unknowingly leave a record of their network access logs, link files and registry settings as well as a record of the date and time of a specific thumb drive connection.

Charges of code theft at Goldman Sachs and UBS have also brought to light the high value placed on proprietary trading code used for algorithmic trading as well as high frequency trading activities by Wall Street firms.

Algorithms account for over 25% of all shares traded by the buyside today. More telling, 73% of US equity trading volume can now be attributed to the activities of high-frequency trading firms, which

include divisions of Goldman Sachs and UBS but many more obscure, startup firms such as Archelon, EWT Trading, Getco and Peak6.

Court filings related to the alleged code theft at Goldman Sachs claim that the code is worth "many millions of dollars of profits per year" and imply that Goldman will pay dearly for their loss.

"Such codes are extremely important because if you know the strategy of when a firm buys and sells, their logic and trigger points you can effectively preempt their moves, trading either against them or ahead of them" said Professor Bernard Donefer, a risk management consultant and distinguished lecturer with the City University of New York, Baruch College.

He noted that such codes indeed are potentially worth millions of dollars, assuming that one has the high-speed trading infrastructure and connectivity to multiple markets in place to truly exploit the value of these codes in a timely manner.

But the timely manner is key. According to Bob Iati, a partner with the Tabb Group consulting practice, "Any algorithmic code has a limited shelf life whose "competitive advantage is diluted with each second it is outstanding."

The speed and volatility of today's markets are such that algorithmic strategies often change within seconds. "As a result, any firm acquiring "stolen" code would gain benefit from it for no more than a few days before the firm would need to adjust the code to the dynamic conditions," Iati said.

Katherine Heires (www.mediakat.com) is an independent business & technology journalist based in New York;

GUARDING THE CODE

Security experts suggest the following processes and technology to help prevent the loss of valuable digital assets:

1. *Identify assets* with highest risks and most unique value.
2. *Dress in layers.* Use correlation management software, access control software and other technologies to prevent breaches.
3. *Organize.* Consider creating a cyber risk intelligence unit to study, monitor, anticipate and address problems.
4. *Train.* Assign a visible, senior executive to train employees on correct security practices.
5. *Throw a wide net.* Hold partners and third-party vendors accountable to the same security standards through agreements and oversight.
6. *Go by the numbers.* Measure the results, starting with breaches attempted, breaches caught – and breaches not caught, until after the fact.

/Source: Deloitte, Ponemon Institute and Protegrity/