Louis
Manager, IT Security
PNC Bank, Pittsburgh

The Story: "These aren't kids on a digital joyride. Their motive is financial gain."[3]

PNC Bank has been the victim of an insidious—and sophisticated—attack. An online organized crime group, probably in Russia, has turned PNC's corporate home page into source of digital infection.

The hackers have broken into PNC's Web server and inserted a Trojan virus. When visitors come to PNC's infected home page, the virus attaches a JavaScript code to the visitor's browser. The code then downloads a program that takes control of the visitor's computer. The program records the victim's keystrokes and opens a back door into the system's security to allow the attacker access to the computer.

The virus is particularly insidious because a visitor's computer can become infected by merely visiting PNC's home page. Visitors have no way of knowing they've even been broken into.

The attack has created a two-fold problem for PNC. The first is trust. Thousands of visitors come to PNC's site each day for a host of reasons. Now they just don't know if that's safe. Worse, tens of thousands of PNC's customers use its online banking service. They rely on the security of the Web site to conduct their banking with confidence. They have no idea if their passwords, account numbers, and other sensitive information have been compromised.

The second—and far more serious issue—is that PNC's own employees' computers were infected when they visited the corporate site in the course of their jobs. There's evidence that employees' passwords were pilfered and have been used by the attackers to access the corporate network.

[3] Adapted from "Trojan virus attacks popular Web sites", CNN.com, June 26, 2004.
http://www.cnn.com/2004/TECH/internet/06/25/internet.attack/
And from "Researchers warn of infectious Web sites", CNET News.com, June 25, 2004.
http://news.com.com/Researchers+warn+of+infectious+Web+sites/2100-7349_3-5247187.html

Questions, needs, tasks
▸ Can VeriSign help us figure out where our network is vulnerable so we can find out how this happened? ▸ Can they tell us how to fix this? Is it an equipment problem? Do we have our network configured wrong? Is our architecture wrong? ▸ How much does VeriSign know about worms and viruses and Trojans? Do they know enough to really fix the problem right? ▸ Can VeriSign help us to implement the solution if we don't have the expertise? ▸ Can VeriSign help us detect when someone is trying to break into our system so we can stop it before it happens? ▸ Is it possible to make our network impenetrable? Can we afford it? Can VeriSign help us to figure out how to get the best security for what we can reasonably spend? ▸ If we don't catch an attack before it happens, can VeriSign help us figure out how to stop is as soon as possible? ▸ What does that take? More people? Is there something wrong with the way we go about things? How can we monitor what's going on better? Can VeriSign help us figure that out? ▸ If organized crime was behind this attack, is there any way to recover evidence of who it was and how they did it? Can the evidence be documented in a way that can be presented in court? Does VeriSign know about that? ▸ We've stopped the attack and we've got the network running again, but it's pretty kludgey. Can VeriSign help us put our network back together in coherent way that makes sense? ▸ We think we've recovered all the data—but what a nightmare. Can VeriSign help come up with a better way of protecting our data and getting it back if something goes wrong?