

Fighting Phraud

First Horizon National Corp. chooses a global approach to fix phishing attacks

Christopher Leach, the chief information technology risk officer at First Horizon National Corporation in Memphis, Tennessee, didn't need to read the reports by the industry groups and analysts to know that phishing attacks were increasing. Complaints from customers and noncustomers were escalating, and the emails bouncing back to the bank's mail gateways due to invalid addresses were choking the system.

Soon, the IT workload at the bank—which employs 13,000 people at hundreds of branches in more than 40 U.S. states—surpassed the staff's ability to keep up.

By David Geer

At times, it seemed to Leach as if the majority of the 15,000 to 17,000-plus phishing reports filed monthly with the Anti-Phishing Working Group involved First Horizon. "What we're really selling is trust," he says, "so we had to do something. The nature of phishing attacks is global so we knew we needed a global approach to succeed."

Leach signed on for a month trial of Symantec's Online Fraud Management Solution. The result: Phishing attacks went from five million emails monthly to several hundred, only a few of which were ultimately received by customers.

"Symantec got in front of the attacks," Leach says. "For those few that did get through, we were able to focus our time and energy on remediation." More than one-and-a-half full-time employees, previously



Christopher Leach, Chief Information Technology Risk Officer, First Horizon National Corporation

deployed to manage phishing fraud, are now redirected to more valuable activities.

Moving forward

Now, with an ever-evolving threat landscape that not only includes spear-phishing (attacks targeted at specific companies) but also vishing (attacks on VoIP), First Horizon has

developed its own metric matrix to assess and manage risk. The matrix measures the customer impact should a system, application, or similar resource fail. Included are the legal and regulatory risks and impacts, risks to reputation, and overall threat environment, Leach says.

"The threat environment includes electronic threats such as active

virus and worms as well as political and geopolitical threats, such as Homeland Security threat levels,” he says.

Business processes are categorized. Within the categories, each technology is placed into criticality tiers.

“The higher a business process falls into a specific tier, the more controls are put in place to minimize and reduce any impacts,” Leach explains.

Some risk is acceptable. “We work with the business to identify risks and determine what the company is willing to accept. We then work with the business to put mitigating controls in place to minimize and reduce any customer impacts,” Leach says. With respect to law and regulation, risks are addressed by compliance.

It used to be that a safe perimeter meant a safe enterprise; now you must look inside, says Leach. It’s not enough to use firewalls, intrusion detection, and anti-malware tools at your doorstep.

“We continue to develop access and identity management and application security programs to address our inward view,” he says. “Historically, we have tended to trust our employees and contractors because we knew them. I don’t think we have that luxury anymore. Most root-cause analyses after a security breach show there is an insider component to the incident.”

In order to mitigate potential insider threats, First Horizon is deploying access and identity management (specifically, role-based identity management capabilities) and has already instituted some of this functionality.

To illustrate, when you are hired by First Horizon to fill a certain role—say as a bank teller—you gain access to a certain set of applications



Top 5 worries for Christopher Leach, First Horizon National Corporation’s Chief IT Risk Officer:

1. Budgets and staffing

2. Draining of limited resources by increasing regulatory oversight

3. Awareness of the abilities of technology

“Many business executives feel that technology should always be able to solve security issues when, many times, the human component would work better.”

4. Endpoints

“PDAs, cell phones, wireless, and

memory sticks have all changed the endpoints to our infrastructure and are almost impossible to secure entirely. The tighter our grasp, the more that will slip between our fingers.”

5. Staying ahead of the bad guys

“Zero-day vulnerabilities, phishing, and now vishing are among the new threats. What is next? That brings me full circle to budgets and staffing. Will I have the right people in place to address these emerging threats and will I have the budget to do it?”

necessary to do your job. You don’t get access to anything you don’t need as part of your role at the company. “This access is set up automatically,” says Leach.

If you are then promoted to another position, say in mortgage operations, you have new access needs and your old access needs are no longer valid.

“Rather than having to manually turn off certain access and turn on other access, it changes automatically based on your job code,” Leach says. This kind of identity management is being put in place first for critical and Sarbanes-Oxley (SOX) applications.

In relation to application security programs, First Horizon provides a tool for developers to run on any program code while it’s still in development to search for vulnerabilities, such as SQL injection vulnerabilities, which could allow a hacker to manipulate the database, leaving data open to theft or destruction, and buffer overflows.

During compilation (a process for putting the program into code computers can understand), First Horizon and developers run a more robust tool on the entire program looking for similar vulnerabilities that can find their

way into the application at this stage. During the life cycle of the application, the same tool is run on the program again once a year, depending on how critically important the program is.

Where the human element is concerned, insider threats haven’t changed much. According to Leach, most insider abuse comes about by one of two means: either someone accesses the data, writes it down or prints it out, and then sells it, or multiple people are involved in a conspiracy.

“Those continue to be the norm,” says Leach. “That’s not to say that we’re not concerned about key loggers (programs that log every keystroke for later retrieval) or other things that people could be using. We do scan for those types of things, but I don’t think I’ve seen a change in how people are taking or trying to take data.” ■

David Geer is an Ohio-based technology writer whose work has appeared in Computerworld and CSO magazines.



Online Extra

See First Horizon’s Risk Model

Go to www.symantec.com/ciodigest/firsthorizon

Read Online:

www.symantec.com/ciodigest/firsthorizon