

# technology

## protecting against identity theft

By Barry Harkness



For any company that maintains a database containing consumer-oriented sensitive data (social security numbers, credit card accounts, banking information, etc.), it has to be of great concern to see how much media attention is focused on those organizations that have had potential exposure to identity thieves. And bad publicity is just the tip of the iceberg. Potential liability and compliance with federal and state regulations could make the loss of sensitive data a costly mistake.

### Types of Exposure

Sensitive data can be exposed to identity thieves in three ways: *Intrusion*, where a person accesses your systems from external networks – generally from the Internet; *Accidental Data Loss*, where tapes, files, or hardcopy/reports are misplaced or stolen; and *Internal Threats*, where sensitive data is stolen by an employee, or some other trusted person who is given access to sensitive data.

Protecting against intrusion is most commonly addressed by using password protection, and also by placing a firewall between your network and the Internet. More advanced strategies involve using intrusion detection software that monitors network traffic and system log files, looking for suspicious activity.

Protecting against accidental loss of data is no simple task. Backup tapes are made, reports are printed, and files are copied. One common approach is to encrypt the sensitive data at the database level, and remove sensitive information from all reports and data feeds, except where it's absolutely necessary. Removing sensitive data from all files is not always practical. For example, ACH files sent to the bank for debiting bank accounts cannot be transmitted without including sensitive consumer bank account information. In these cases, the number of people who have access to the data must be kept to a minimum, and regular audits should be performed to ensure that procedures are

being followed.

Internal threats may be the most difficult type of exposure to protect against. Employees at many levels need access to sensitive data, including your Information Technology (IT) staff. Programs can be written that prevent unauthorized access by users, but software developers have always had unimpeded access to the raw data. Total isolation of sensitive data is required to truly protect it from unauthorized access by trusted users.

### The Black Box

So how do you isolate sensitive data and yet still allow limited access to it? Some security experts recommend implementing a concept called a Black Box. A Black Box is a system with input and output characteristics that are well understood, but where the inner workings and means of operation are deliberately hidden. In the application of sensitive data isolation, a Black Box is implemented by creating a system with the specific job of storing and retrieving sensitive data without disclosing how and where the data is stored. This system would require authentication, and it would create a log entry each time data is accessed. More advanced features would include sending alerts when data is being accessed after hours, or in unusually high volumes. Reports back to department managers would list summaries of data being accessed by their employees.

Physically, the Black Box could be a remotely hosted server which is under administration of the Security Officer, or even an outside vendor. Even though its inner workings are not exposed to the trusted employees of the company, it is still protected from intrusion and accidental loss by use of firewalls, intrusion detection software, password protection, and data encryption. Once implemented, the inner workings of the black box can be reengineered as needed, so long as the interfaces for input and output are not changed. However, great care should be taken to ensure that the work done to the black box

by programmers and technicians is thoroughly audited to prevent "Back Doors" – deliberate holes in the security system left in place by designers.

There is a downside to this protection – cost. In addition to the cost of creating and maintaining the Black Box, costs are also incurred in the effort of converting applications so that they are compatible with it. Performance costs are also increased due to the additional overhead of encryption/decryption, logging, and monitoring. And because of the complexity of using a black box (as opposed to the old simple way of retrieving data), the cost of creating new programs that access sensitive data will be modestly higher.

However, the costs of your sensitive consumer data being compromised may be much higher. The implementation of a Black Box acts as both a deterrent and an alarm. It protects against internal threats, and also creates additional protection against intrusion and accidental loss of data. And with proper logging, the Black Box will let you know who is using sensitive data.

If you chose not to isolate your sensitive consumer data with a Black Box system, you never really know when your data has been compromised. You may have hundreds of users and programmers who have varying degrees of access. And some of them may have easy to guess passwords, or passwords written down where they are easily found. Most systems do not have the detailed logging you will need to determine when sensitive data has been accessed, and even fewer have logs that programmers cannot circumvent. A Black Box system protects your consumers, your employees, and your peace of mind. **D**

---

*Mr. Barry Harkness is the Director of Software Development for Concord Servicing Corporation and can be reached at [bharkness@concordservicing.com](mailto:bharkness@concordservicing.com)*