CLAUDIA IMHOFF

Reprinted from DM REVIEW

The BI Watchdog – Security and Privacy in Analytics

Business intelligence's central mission is to provide the business with the best quality data available for all forms of analyses, queries, reports, etc. It promises reasonable performance and response times, as well as easy or intuitive access to these analytic capabilities from nearly anywhere in the world. Of course, such a storehouse of immensely valuable information must have the highest security placed on it.

Let's look at a common scenario. Your sales representative is on the road. He (or she) is about to call on his customers and would like to know their history with the company and their overall profitability before calling on them. He accesses the corporate data warehouse and downloads the top 100 profitable customers' information as well as specific data on his customer calls. To access the data warehouse, he had to go through the usual procedures of logging in, entering his ID and password, having them authorized and so on, all to protect the precious information about the corporation's most valuable customers. Then what happens?

He performs his queries, stores the results on his PC, unplugs from the intranet, and goes his merry way. How he uses the information that was downloaded and whom he may give it to is completely unknown and uncontrollable at this point. If he resigns from the company, he could take the information with him (a simple e-mail to his personal account with the customer information as an attachment is all that is needed), or he could perform unauthorized contacts with customers, thus violating the corporation's privacy policies. Security and its close relative, privacy, have been compromised in both cases.

This scenario is not so far-fetched. It could be executed by anyone in your organization – a financial analyst who publishes sensitive financial data, a marketing employee who divulges upcoming promotional plans or an operations person who shares supplier information with the company's suppliers.

What should your corporation do to protect itself and mitigate such unwanted actions? My suggestions fall into two categories – procedural and technological. Procedural suggestions include education, prosecution of offenders and special limitations placed on user access. Technological suggestions include encryption of data, usage of time-sensitive downloads and periodic "snooping" on the content of employees' PCs.

From a procedural point of view, following are more details:

- Education: Often, security and privacy breaches happen because employees simply do not know the proper (and safe) procedures when handling sensitive corporate data. They may not even realize that they have access to "sensitive" data when downloading a result set. Every corporation with a BI environment must create curricula that cover the privacy and security policies of the enterprise. These courses must be made mandatory for anyone with access to the BI databases. The courses should cover the general and specific procedures for handling such data including proper usage, storage and disposal of the results sets. Obviously, these courses must also cover what happens if an employee disregards or violates these procedures or causes a security or privacy breach through his/her negligence or intentions.
- Discipline of violators: It is unfortunate, but along with the training must come the inevitable steps to take when procedures are not followed or the employee displays malicious behavior. While not usually criminal in nature, there are various levels of disciplinary action that should escalate depending on the severity of the breach, the final one being termination of employment. These "punishments" should be as well understood as the reasons or behavior that generated them.
- Special limitations on some users' access: Not all data in the BI environment should be made accessible to all of its users. That should be obvious; however, it may not always be obvious where to draw the line. Should a sales manager have access to all sales data or to only his region's data? Should operations personnel have access to all orders or only a portion of them? It depends. One operations person may need to plan production based on the total number of products that have been ordered. Another may only be responsible for a particular product. The sales manager may need to create a commission plan based on the total sales revenues, thus requiring access to the total sales information (but perhaps not to the total *customer* and sales data). A careful study of what data is really needed by each individual may save you a lot of anguish later on. Another limitation may be to restrict where certain data can be accessed. Data miners and statisticians are particularly problematic. They require access to massive amounts of very detailed (and usually sensitive) data. It may be that the organization determines that these analysts may only access their data from within the corporation's walls.

We also have options from the technological point of view.

- Encryption: For highly sensitive data such as credit card numbers and social security numbers, you may choose encryption. This adds overhead to the overall environment, but

it may also be the only way to truly ensure that the data cannot be misused. For individuals who need to see the unencrypted data, you may limit their access to that occurring within the corporation's four walls. In addition, you may want to deny the ability to download any of the unencrypted data to anyone's PC.

- Creation of time-sensitive downloads: This is an interesting idea that our vendor community is offering or considering including in their packages. Can they develop time-sensitive markers or tags that are attached to the results sets of data? When the time limit is up, the results sets (e.g., cubes, data sets, flat files) self-destruct. This technique also helps with the overall cleanup and maintenance of the users' PCs!
- Periodic monitoring of PC contents: A final suggestion – and perhaps the most repugnant to the user community – is the use of "spyware" or software that periodically peers into the business user's PC to determine what has been downloaded. If a determination is made that certain data is sensitive or should not be on the PC, the software either deletes it or sends the employee a message reminding him or her to delete it.

I hope that you have already considered these options and have put some or all of them into place. It is important to note, however, that regardless of what you put into place, you will still have security or privacy breaches. Once someone has downloaded his or her desired data and unplugged from the mother ship, there may not be a lot you can do to prevent misbehavior. If the person is truly unscrupulous or determined to cause maximum damage to the corporation, it is still possible and your only recourse may be legal action.

Claudia Imhoff, Ph.D., is the president and founder of Intelligent Solutions (www.intelsols.com), a leading consultancy on CRM and business intelligence technologies and strategies. She is a popular speaker and internationally recognized expert and serves as an advisor to many corporations, universities and leading technology companies. She has coauthored five books and more than 50 articles on these topics. She may be reached at cimhoff@intelsols.com.