: How can managers and technology staff secure decision support data and decision support systems?

by Dan Power

Editor, DSSResources.com

Using computers to support business decision making is mission critical in many companies, but security for such systems is often an after thought. Data security and privacy are also important but often neglected concerns related to computerized decision support. A data-driven DSS used for performance monitoring or ad hoc business intelligence queries should be secure and the data should be protected. Many of the interchanges facilitated by a communications-driven DSS are sensitive and should be kept confidential. The knowledge bases of most knowledge-driven DSS are proprietary and should be protected. The models in model-driven DSS describe important relationships that should be kept secret from competitors. Finally, document-driven DSS often access, analyze and monitor sensitive documents.

Privacyrights.org maintains a chronology of major data breaches that have been reported since January 10, 2005. By July 2007, more than 700 incidents had been reported, approximately 23 per month. A data breach occurs when there is unauthorized access to sensitive data. DSS of all types use, transmit and generate sensitive data.

The following examples highlight some common problems. On January 9, 2007, 5 laptops were stolen from Towers Perrin, allegedly by a former employee, that contained names, SSNs, and other pension-related information of Altria and United Technologies. In December 2006, MoneyGram, a payment service provider, had a company server unlawfully accessed over the Internet. The server contained information on about 79,000 bill payment customers. In mid-December 2006, a laptop computer containing taxpayer data was stolen from the car of a North Carolina Department of Revenue employee. On February 2, 2007, an employee of the New York Department of State posted commercial loan documents to a Website that mistakenly contained Social Security numbers. The forms are posted to the Web to let lenders know the current financial status of loan recipients. On February 9, 2007, a programming error resulted in personal information of 65,000 individuals being exposed on the East Carolina University's Web site. On February 10, 2007, a hacker gained access to the official Indiana State Web site and obtained

credit card numbers of individuals who had used the site's online services and gained access to Social Security numbers for 71,000 health-care workers. On February 19, 2007, credit and debit card account information including PIN numbers was stolen by "high-tech thieves" who apparently broke into checkout-line card readers and PIN pads at Stop & Shop Supermarkets (in Rhode Island and Southern Massachuesetts) and tampered with them. On March 12, 2007, a former contract worker of Dai Nippon, a Japanese commercial printing company, stole nearly 9 million pieces of private data on customers from 43 clients, including Toyota Motor. On April 9, 2007, a Nebraska woman using Turbo Tax online was able to access tax returns for other Turbo Tax customers in different parts of the country. On May 15, 2007, an unnamed vendor lost computer tapes containing information on IBM employees.

So what are major security problems for computerized decision support? Stolen computers, especially laptops and handhelds, hacking and unauthorized access to servers, mistaken public postings of information to Web sites, programming/software errors, data theft using technology, data theft by former employees, inadvertant/unauthorized access to Web-based systems, and lost/missing data. We have been dealing with some of these problems for many years, but the development of the Internet has significantly increased the likelihood that a network accessible DSS will be breached.

Most managers realize that security for DSS is an important topic. The problem is actually determining how to secure the systems and avoid data breaches. Improving security for decision support applications involves addressing a number of issues. First, managers and MIS staff must determine DSS security needs. Based on the needs identified by managers and staff, we should implement any required security measures and fix any technical problems. Once appropriate security is in place, someone must monitor the system and any new security problems that are identified should be fixed quickly.
Finally, both managers and MIS staff need to stay informed about new security problems and methods for breaking into information systems. Both managers and MIS staff need to assume shared and equal responsibility for the security of Decision Support Systems and decision support data (cf., Jones, 1998, Power, 2002).

A recent CIO Insight research study on IT security (May 31, 2007) "shows increased spending on anti-virus/spyware/malware software,

identity management and authentication, encryption, security education and training and security consulting services." The danger is that the focus will be on infrastructure and transaction processing and that decision support applications will receive insufficient attention.

According to Wikipedia, application security "encompasses measures taken to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, or deployment of the application." Decision support applications should be audited using a protection profile that is appropriate. The protection profile should vary for the 5 different types of DSS! Also, managers should specify the security requirements for the DSS they regularly use.

I'm a DSS generalist, so I decided to get some help for this column from a security specialist, David Friedland, Vice President of Business Development for Innovative Routines International, CoSort/IRI, Inc. He responded by email to four more specific questions relevant to DSS security. David has a business degree from University of Albany (SUNY).

Why use ETL tools to encrypt and protect data before it is moved to a data warehouse?

Friedland: "ETL tools can encrypt data before it moves into a data warehouse when there is a need to protect specific database columns from hackers."

What can managers do to maintain the security of decision support data?

Friedland: "They can protect it at the physical level to some extent with special access rules and procedures, including database and disk encryption. But those methods are often overkill because they cut off access to all the data from decision support systems, including the safe data. They can instead ... protect data at its source (in files)

during ordinary processing and reporting, by specifying a security function."

What is the role of access security to limit use of decision support capabilities?

Friedland: "Tools like CoSort's Logon Security restrict and audit on-line access according to business rules. Similarly, field level protection rules can be assigned by the data governance office and applied via different security functions (e.g. encryption libraries and pass keys) to limit the access to, and exposure of, sensitive data flowing through decisioning systems."

Friedland: "To the extent that protected data limits the use of data for decision support because it was morphed prior to, or removed from, analytic applications, the protection scheme can surely interfere with decision support jobs. It is another reason why we offer a choice of protection functions to preserve the look and feel of the original data, and why CoSort's encrypted output displays with only printable characters."

Who has responsibility for preventing security and privacy breaches?

Friedland: "The chief information security officer (CISO) or head of the data governance office is usually responsible for identifying and securing personally-identifying "data at risk." That said, privacy legislation in effect for various industries (like HIPAA for healthcare) may hold higher level executives accountable for non-compliance, and it they don't, shareholders reeling from lawsuit and remediation expenses ultimately will. For these reasons, it is important that companies not only take steps to protect data at rest and in motion (preferably at the source), but that their tools provide an audit trail so compliance activities can be specifically verified. It is not enough to protect -- you must be able to prove proper steps were taken to protect the data."

: How can managers and technology staff secure decision support data and decision support systems?

What about other actions?

Power: Companies can implement a virtual private network (VPN) to communicate confidentially over a public network. A VPN can be a cost effective and secure way for a corporation to provide users access to the corporate network and for remote networks to communicate with each other across the Internet.

Power: Companies can also implement proxy based firewalls. An application layer firewall actually inspects data packets prior to interaction with a Web-based DSS.

Wikipedia: "Social engineering awareness - Keeping employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers. ... Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information."

In general, a company needs a Computer Security Policy (CSP) to ensure the safe and organized use of IS/IT resources. A CSP is a document that sets out rules and principles that affect the way an organization approaches security problems. A company should specify security policy for each specific DSS.

The DSS security problem is expanding. In a May 30, 2007 Computerworld article, David Haskin writes "Mobile security threats are a relatively minor annoyance to a handful of users in Europe and Asia. However, conditions are rapidly ripening for these threats to start overwhelming both companies and individual users in North America." He quotes Kris Lamb, director of the Xforce team at Internet Security Systems. Lamb said "The trend toward making mission-critical data available to mobile users is just starting and will grow rapidly ... and some of the factors contributing to that growth will also benefit hackers."

: How can managers and technology staff secure decision support data and decision support systems?

Security should be a proactive rather than a reactive issue in companies.

As always your comments and suggestions are welcomed.

References

Chabrow, E., "CIOs Set IT Spending Priorities," CIOInsight.com, May 31, 2007,
URL http://www.cioinsight.com/article2/0,1540,2139505,00.asp?kc=EWWHNEMNL053107EOAD,
last accessed June 3, 2007.

Conway, R. W., W. L. Maxwell, H. L. Morgan, "On the implementation of security measures in information systems," Communications of the ACM, v. 15 n.4, p.211-220, April 1972.

Friedland, D., Email Interview on DSS Security, May 29, 2007.

Haskin, D., "Five reasons to prepare -- now -- for more mobile security threats," Computerworld.com,
URL http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9022099&source=NLT_AM&nlid=1,
last accessed June 3, 2007.

Jones, D., A University Course on Systems Administration, Department of Math and Computing, 1998.

Privacy Rights Clearinghouse, "A Chronology of Data Breaches," URL http://www.privacyrights.org/ar/ChronDataBreaches.htm,
last accessed June 3, 2007.

: How can managers and technology staff secure decision support data and decision support systems?

Power, D.J., Decision Support Systems: Concepts and Resources for Managers, Westport, CT: Quorum/Greenwood, 2002.

Power, D.J., Decision Support Systems Hyperbook, Cedar Falls, IA: DSSResources.COM, HTML version, 2000, URL http://dssresources.com/subscriber/password/dssbookhypertext , last accessed June 3, 2007.

The SANS Institute, URL http://www.sans.org/ .

Wikipedia, "Application Security," URL http://en.wikipedia.org/wiki/Application_security , last accessed June 3, 2007.

Wikipedia, "Computer Security," URL http://en.wikipedia.org/wiki/Computer_security , last accessed June 3, 2007.

Wikipedia, "Social engineering (security)," URL http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29, last accessed June 3, 2007.

Thanks to Betsy Scherzer for arranging the email interview with David Friedland.

Author: Daniel Power
Last update: 2007-11-15 10:47