: Is security important for decision support applications?

by Daniel J. Power

Editor, DSSResources.COM

Decision support applications often contain sensitive data that should be secured. Also, a common source of decision support functionality, an analytical model, may be important to protect as well. Sadly security may be an afterthought that is not addressed until a problem arises. Organizations need to secure and protect decision support capabilities in advance as forethought not as an afterthought. Security is an important issue for creating, managing and using decision support. How important is security? How much should be spent to secure decision support capabilities?

Reports of computer crime and security breaches are increasing. Security is an ongoing concern that will not go away. Also, identity theft from phishing and system break-ins is occurring and creating security problems. Hackers can and do disrupt Web sites, including web-based decision support applications. Viruses and software worms attack computers from email message attachments. Customer and credit card data have been stolen from Web servers. Company and customer data is valuable to competitors and thefts by unhappy employees and hackers of company data do occur. Security for decision support applications **IS** important, but some data and applications are more important than others.

Managers need to prioritize security concerns and evaluate threats. Security has a cost that must be considered and risks must be evaluated in the context of consequences and costs.

Information systems and especially decision support capabilities can be made very secure if enough effort is expended. However a very secure system is usually too inconvenient for managers to use. According to Jones (1998), when implementing a security plan both System Administrators and managers must weigh the importance of the system, the effort required to secure it and the inconvenience caused. Managers should ask the following questions:

1. How important is the application, its availability and the data stored on it to the organization? Is it mission critical?

2. How much effort is required to make and keep the system secure? What is the cost of enhanced security? and

3. How will enhanced security features affect the users of the system? Is the inconvenience really necessary?

A computer server containing the plans and designs for Intel's next computer chip or sensitive financial data in a forecasting DSS should be very carefully secured. On the other hand, it may not make sense to spend hundreds of thousands of additional dollars securing a computer system used for email by business students. A system can be made as secure as is necessary, but in doing so you might lose the ability to make effective use of the system. Managers and Systems Administrators must balance the need for convenience against the need for security.

Once the importance of security for an application or system is determined, improving security involves addressing a number of issues. First, managers and MIS staff must determine security needs. Managers should ask what are the current security problems, and hence the needs. This initial task is often called **security evaluation**. Based on a problem and threat analysis in the evaluation stage it is important to **implement required security measures** and fix any security problems. These two tasks -- evaluation and implementation -- start a security improvement process. Once appropriate security is implemented one must **monitor** the system and any new security problems that are identified need to be fixed to close a feedback loop. Finally, managers and MIS Staff need to **stay informed** about new security problems and methods for breaking into decision support and information systems. Both managers and MIS staff need to assume shared and equal responsibility for the security of decision support applications.

To secure means to make data and applications safe from theft, to make data and applications safe from tampering, and to insure the integrity of the computing, data and decision support environment. Managers must believe that decision support capabilities for important decisions have not been tampered with and altered.

One can not guarantee a decision support capability is secure. "The only highly secure system is one that's unplugged, turned off, and in a locked room." Managers and MIS staff can however improve security and they often should.

References

Jones, D., "A University Course on Systems Administration", Department Math and Computing, Central Queensland University, The Study Guide, 1998 at URL: http://www.infocom.cqu.edu.au/Units/aut98/85321/Study_Material/Text_Book. (See

http://davidtjones.wordpress.com/publications/teaching-systems-administration-ii/).

Olszewska, K., "Evolving IT Security Trends and Challenges Within Today's Organizations: IT Decision Makers' Perspective," Frost & Sullivan, December 26, 2012, press release at .

Power, D. J., Decision Support Systems Hyperbook. Cedar Falls, IA: DSSResources.COM, HTML version, 2000, accessed on 3/7/2012 at URL http://dssresources.com/subscriber/password/dssbookhypertext.

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

Power, D. J. "How can managers and technology staff secure decision support data and decision support systems?" DSS News, Vol. 8, No. 11, June 3, 2007 at URL http://dssresources.com/newsletters/191.php .

"Why Awareness Is Important," Native Intelligence, Inc. at URL http://www.nativeintelligence.com/ni-programs/whyaware.asp

"Why is Information Security Important?", Mindful Security, 07/01/2009 at URL http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/

"In today's world, Distributed Denial of Service (DDoS) attacks on organizations are becoming more prevalent. The number of attacks are increasingly annually with no end in sight, and the damage these attacks inflict grows more severe. Because these attacks essentially disconnect an organization from the Internet, the after affects can be ruinous, particularly if these attacks are staged to cover other malevolent acts going on in the background. Who should be concerned? Any organization with a website and/or Internet-based service. (from ComputerWorld, April 1, 2013 'An Interactive eGuide: DDoS Attacks'"

Cite as:

: Is security important for decision support applications?

Author: Daniel Power
Last update: 2013-04-14 03:41