MIS Quarterly Executive

Volume 4 | Issue 1 Article 6

2-8-2008

Inside the Fence: Sensitizing Decision Makers to the Possibility of Deception in the Data They Use

David P. Biros
Oklahoma State University, birosdp@cox.net

Joey F. George
Florida State University, jgeorge@cob.fsu.edu

Robert W. Zmud
University of Oklahoma, rzmud@ou.edu

MIS QUARTERLY EXECUTIVE

INSIDE THE FENCE: SENSITIZING DECISION MAKERS TO THE POSSIBILITY OF DECEPTION IN THE DATA THEY USE[1]

David P. Biros
Oklahoma State University

Joey F. George
Florida State University

Robert W. Zmud
University of Oklahoma

Executive Summary

While there are various forms of computer attack, this article deals with the growing trend of hackers and insiders manipulating data they are unauthorized to see or change. As employees and managers increasingly rely on information systems to make decisions, others can influence those decisions, and even the decision-makers' behavior, by manipulating the data the decision makers use. While organizations typically rely on intrusion detection systems and firewalls to protect their information assets, employees must also be made aware that data deception is possible, so that they realize the information they depend on might have been manipulated.

This article describes a field experiment that analyzed the effectiveness of alternative approaches to sensitizing decision makers to the possibility of manipulated data. Once sensitized, they may either truly discover data manipulation (detection success) or falsely discover manipulation (false alarm).

We found that traditional classroom training had no effect on raising the decision makers' sensitivity, while warnings of possible poor data quality did lead to higher detection of the erroneous data. However, warnings combined with just-in-time training resulted in better detection success but also in more false alarms. But even the best detectors were only able to spot 25 percent of the manipulated data. Nonetheless, the study underscores the need for both strong perimeter defenses as well as a sensitized workforce when a data manipulation incident is suspected.[2]

DATA MANIPULATION IS A GROWING SECURITY PROBLEM

As organizations conduct more and more transactions using e-business or e-government platforms, their need to secure their networks and protect their information increases correspondingly. Each year, private industry and governments spend millions of dollars to protect their information and information technology (IT) assets. Today, in fact, the information security industry is booming, and the number of IT security vendors continues to grow.

How big an issue is computer and network security? The answer seems to be "very big and getting bigger." Based on current data from the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University, [3] the number of incidents in the latest reporting period of 2003 was 137,529 – compared to 2,340 incidents in 1994, just ten years earlier, and only six when CERT/CC was established in 1988.

Companies are devoting major resources to computer security training, certification and accreditation of systems, and intrusion detection tools. Yet, security incidents are still rising. Of the many forms of security breaches, our study focuses on the problem of data manipulation. Data manipulation is especially a threat from insiders because they understand the organiza-

[1] Allen Lee was the accepting Senior Editor for this article.

[2] Some of the material in this article was adapted, and in some cases, updated from David P. Biros, Joey F. George, and Robert W. Zmud, "Inducing Sensitivity to Deception in Order to Improve Decision-Making Performance: A Field Study." *MIS Quarterly*, 26(2), June 2002, 119-144.

[3] The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University is on the Web at http://www.cert.org/stats/cert_stats.html.

tion's information domain. Consider, for example, a case recently described by the National Threat Assessment Center and the CERT/CC:[4]

> *For several months, beginning in the fall of 1996, two credit union employees worked together to alter credit reports in exchange for financial payment. As part of their normal responsibilities, the employees were permitted to alter credit reports based on updated information the company received. However, in exchange for money, the employees intentionally misused their authorized access to remove negative credit indicators and add fictitious indicators of positive credit to specific credit histories. The total amount of fraud loss from their activities exceeded $215,000. The risk exposure to the credit union was incalculable.*

Following are three more examples of the potential for insider data manipulation. They demonstrate how easily individuals with just a little technical knowledge can manipulate the data in an organization's information systems:

- A Charles Schwab investment specialist manipulated the accounts of his clients and wired himself thousands of dollars of their account funds.[5] He used his access to his organization's information systems and his knowledge of that information domain to exploit the accounts of his clients.
- The 2004 audit by the school district in Alachua County, Florida, reported on the vulnerability of information systems to "…unauthorized manipulation of data files, unauthorized or incorrect use of computer programs, or improper use of computer resources…."[6] The audit noted that a lack of adequate access controls and security mechanisms could allow perpetrators to conduct unauthorized manipulations of systems files. Fortunately, the audit caught the discrepancies before the vulnerabilities could be exploited.
- The National Threat Center report noted that, "…a foreign currency trader with an investment bank used a range of tactics, including changing data in various trading systems, so it appeared that he was one of the bank's star producers.[7] In actuality, he lost the bank over $600 million." Simply put, the man used his access rights to influence the beliefs of his superiors with respect to his trading skills. His goal was to get his superiors to recognize (i.e. make a decision or draw a conclusion) that he was one of the bank's best performers even though he was losing them money.

This article now examines the vulnerabilities of systems to perpetrators who are already 'inside the fence.' Then it reports on a study we conducted to uncover how companies might protect themselves from such vulnerabilities. Finally, it concludes with lessons learned from the study.

Strategic Information Manipulation

If the short history of the Internet tells us anything, it tells us that hackers – if they are persistent enough – will eventually get in. Once inside, they find it rather easy to maneuver about. On the other hand, organizational insiders are already inside and have the same ease of maneuverability. Many organizations focus on securing the perimeter of their networks, not unlike how military organizations secure the perimeter of their positions. However, because the focus is on keeping adversaries out, securing the inside is often overlooked. Once inside, hackers can exploit weaknesses to conduct Web page defacements, denial-of-service attacks, and information manipulation. An insider with knowledge of the information domain poses the same level of threat, if not more threat.

The focus here is information manipulation, that is, where a perpetrator (a hacker or malicious insider) gains access to and manipulates data within a database maintained 'inside the fence.' Zmud posited that, aside from using such access for fraudulent purposes, a perpetrator might conduct an act of *strategic information manipulation*,[8] where the goal is to influence users to change their decision-making behaviors. In many cases, such an attack can go unnoticed by system security personnel because it can be below the threshold of concern. For instance, if a hacker were to gain access to a human resource specialist account, he or she would likely also gain access to the personnel database. If top management used that database to

[4] Randazzo, M.R., Keeney, M.M., Kowalski, E.G., Cappelli, D.M., and Moore, A.P., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," US Secret Service and CERT® Coordination Center, 2004.

[5] "Montgomery Man Given Prison Time For Committing Computer Fraud and Stealing From Investors," Press Release from the Office of the United States Attorney, Middle District of Alabama, Laura Gannett Canary. January 22, 2004, http://www.usdoj.gov/usao/alm/Press/Cobb_sentence.htm.

[6] Alachua County District School Board – Financial, Federal Single Audit, Report No. 2004-157, 2004, http://www.state.fl.us/audgen/pages/summaries/d_alachu.htm.

[7] Randazzo, M.R., Keeney, M.M., Kowalski, E.G., Cappelli, D.M., and Moore, A.P., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," US Secret Service and CERT® Coordination Center, 2004.

[8] Zmud, R.W., "Opportunities for Strategic Information Manipulation through New Information Technology." *Organizations and Communications Technology*, J. Fulk and C. Steinfield, Eds. Newbury Park, CA: Sage, 1990, pp. 95-116.

obtain background information on personnel they were considering for promotion or assignment, a few changes to the database could easily influence their decisions.

All an unauthorized person needs for strategic information manipulation is user-level access to an information system and a little knowledge of both the information domain and the data architecture. While such data manipulation is relatively easy to accomplish, it can be very difficult to combat. Generally, database systems are not designed with such attacks in mind, and adding sophisticated edit checks or cross-checking mechanisms after the database has been built costs more money than many organizations are willing to spend.

The computer security industry has developed some tools to combat insider threats, but they have yet to be widely employed, and they have limitations. Many insider threat tools, for instance, monitor user behavior (log-on/log-off times, file access, etc.). If a user should venture outside the threshold deemed "normal" by the monitoring tool, an alarm sounds and system security personnel are alerted. If, however, the user stays within the norm, then no alarm will sound. Thus, if a hacker gains access to a user account and stays within parameters assigned for that account, the security staff receives little or no indication that illicit behavior is taking place. Thus, malicious insiders can easily thwart a monitoring tool by simply staying within the bounds of normal behavior for the account.

Strategic information manipulation, thus, is a low-level attack aimed at decision makers. It involves identifying the information the decision makers might use to make critical decisions and then aims to influence the decision outcome, making it sub-optimal or even harmful. Because most organizational systems are not designed to mitigate such attacks, and because few automated information security tools can detect data manipulations by authenticated users, the most effective defenses can be the database users themselves. Perhaps they can spot tainted data elements. Unfortunately, research has shown that humans are not the best detectors of deception, even in face-to-face conditions where they receive behavioral cues.[9] Yet a field study we conducted demonstrated that people can be sensitized to detect deception.[10] We report on that study next.

[9] Miller, G. and Stiff, J., *Deceptive Communication*. Newbury Park, CA: Sage Publications, Inc, 1993.

[10] Biros, D., George, J F., and Zmud, R.W., "Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study." *MIS Quarterly*, 26(2), June 2002, 119-144.

THE FIELD STUDY

Security issues such as the detection of intruders, erroneous data, and deceptive communication share a common underlying structure. In each case, an unusual event occurs amongst a myriad of everyday events. Those concerned with security want to be able to determine that something unusual has indeed occurred.

The Theories Tested in the Study

A useful frame for understanding this problem is signal detection theory.[11] Basically, signal detection theory reframes the security issue in terms of separating out an unusual event (a deceptive or harmful signal) from an everyday occurrence (noise). Signal detection theory has long been used as the basis for error detection research, that is, detecting inappropriate signals. For example, it underpins work on the accuracy and biases of internal auditors' risk judgments,[12] human attention,[13] and vigilance.[14]

Signal detection theory recognizes two possible outcomes when individuals strive to differentiate a signal from background noise: (a) a successful detection (i.e., the inappropriate signal is correctly identified), and (b) a false alarm (i.e., noise is misidentified as an inappropriate signal).

A high incidence of false alarms is a serious issue for intruder detection for the obvious reasons of cost and lost opportunities.[15] One popular approach to detecting network intrusions is rule-based intrusion detection systems, but these systems tend to generate a high number of false alarms. Researchers have been working to find new computational approaches, such as using the Median Polish Procedure.[16] But computational approaches are even less mature in detecting erroneous data and deceptive communications. Hash algorithms have used a computational approach, but they often rely on file size differences before

[11] Klein, B.D., Goodhue, D.L., and Davis, G.B., "Can Humans Detect Errors in Data? Impact of Base Rates, Incentives, and Goals." *MIS Quarterly*, 21(2), 1997, pp. 169-194.

[12] Blocher, E., Moffie, R.P. and Zmud, R.W., "Report Format and Task Complexity: Interaction in Risk Judgments," *Accounting, Organizations and Society*, (11:6), November 1986, pp. 457-470.

[13] Sperling, G., "A Unified Theory of Attention and Signal Detection," in R. Parasuraman and D.R. Davies (Eds), *Varieties of Attention*, London: Academic Press, 1984, pp. 103-177.

[14] Davies, D.R. and Tune, G.S., *Human Vigilance Performance*, NY: American Elsevier Publishing Company, Inc., 1969, pp. 53-79.

[15] Levera, J., Barán, B., and Grossman, R., "Experimental Studies Using Median Polish Procedure to Reduce Alarm Rates in Data Cubes of Intrusion Data," *Proceedings of the 2nd Conference on Intelligence and Security Informatics*, Tucson, AZ, 2004.

[16] Levera, J., Barán, B., and Grossman, R., "Experimental Studies Using Median Polish Procedure to Reduce Alarm Rates in Data Cubes of Intrusion Data," *Proceedings of the 2nd Conference on Intelligence and Security Informatics*, Tucson, AZ, 2004.

Figure 1: Sample scenario and its deceptive data

Scenario

Four service members are up for below-the-zone promotion. Review their records and ensure they each have at least two years time in service, a decoration, and at least a 4 rating on their performance reports Run an inquiry on their time-in-service, decorations, and last performance report. Report to your commander the names of the members eligible for promotion below the zone.

Name	Time in Service	Decoration	Rating
Ahlberg, Keri L.	2 yrs, 8 months	2 Achievement	4
Balakit, Macario, B. Jr.	2 yrs, 4 months	2 MSM	4
Chaptman, Joseph E. Jr.	2 yrs, 1 month	1 Achievement	4
Dimauro, Patrick, M.	2 yrs, 6 months	1 Commendation	4

Description of Deception

If selected for BTZ promotion, they may 'pin on' the rank of Senior Airmen (SrA) six months earlier than their peers. Often commanders review the records of their eligible service members to help determine the few to be selected for this opportunity. Ensuring they have adequate time in service, checking to see if they have decorations, and reviewing the ratings of the candidates' performance reports are part of the selection process. Human resource specialists are often required to collect and summarize this data for the commanders and highlight any information that may look out of the ordinary. In this scenario, Balakit has two Meritorious Service Medals (MSMs) in his records. This is not possible for a member of his rank. An MSM is a difficult decoration to achieve and usually requires years of service. In a taxonomy of deceptive practices, this might be considered "inventing."[18] While this should be an easy deception to detect, fewer than one-half the HR specialists detected it. In truth, Balakit had no decorations. He should not even be considered for promotion.

and after data manipulation, so they may not be sensitive enough to detect small changes in data.

We believe that sensitivity to possible deceptions can be conceived as a continuum of awareness, with various detection mechanisms (including humans) used along this continuum. On the basis of signal detection theory, it is unclear, though, where 'ideal' interventions (detection approaches) lie on this continuum. For example, people may become so sensitized to the possibility of deception that they trigger many false alarms. Thus, it is important to characterize interventions by their likelihood of producing the desired results – successful detections, not false alarms.

Two types of interventions are likely to increase individuals' sensitivity to deceptive data: general training on deception detection[18] and issuing explicit warnings about the likelihood that deceptive data has been embedded in a database.[19]

The Study's Experiment.

To test the effectiveness of such training and warnings in improving employees' ability to detect deceptive events, we conducted a study at a military training base in the southeastern US. The study involved 205 military human resources specialists whose normal occupational role involved querying a human resources database for information and advising their superiors on human resource decisions.

With the permission of the unit commander, we gained access to the human resource system and created an exact replica of the database for our experiment. We strategically manipulated the contents of the database by changing some data to influence the "students" in the experiment to select the wrong answers in a scenario, in keeping with Zmud's position that incorrect data can influence decisions.[20] All manipula-

[17] Johnson et al, 1993 …...

[18] Zuckerman, M., Koestner, R., and Alton, A.O., "Learning to Detect Deception,"*Journal of Personality and Social Psychology*, (46:3), March 1984, pp. 519-528.

[19] Parasuraman, R., "Sustained Attention in Detection and Discrimination," in Parasuraman and Davies (Eds.), *Varieties of Attention*, London: Academic Press Inc., 1984.

[20] Zmud, R.W., "Opportunities for Strategic Information Manipulation through New Information Technology." *Organizations and Communications Technology*, J. Fulk and C. Steinfield, Eds. Newbury Park, CA:

Figure 2: Detected Data Manipulations, by Group Type

Group Type	Intervention Type	Number of Detected Manipulations	
		Inexperienced	Experienced
Control Group	No Training	.72	1.9
Traditional Training-only Group	Specialized Training	.89	2.1
Warning-only group	Told that database had been hacked	1.4	3.8
Warning and JIT-Training Group	Told that database had been hacked and received JIT specialized training	2.6	5.4

tions were below the threshold that would trigger a typical automated security alarm.

To keep the task relevant for the students, we developed 20 scenarios. In each, the students were to look at the records of one to four airmen and make decisions that might influence these airmen's career. Of the 20 scenarios, 15 contained at least one manipulated record. Overall, three-fourths of the scenarios involved deceptions, but only 22 percent of the records contained manipulations. Figure 1 shows an example of one scenario and its strategic data manipulation.

The students participated in this study while taking a military human resources course, but they were unaware they were part of a field study. The training unit commander required the training and test to take only 90 minutes each. To discern whether those with more knowledge of human resources would detect more deceptions than those with less knowledge, the test was given in both beginner and refresher courses. The experienced members had from 5-7 years of experience, on average.

Specifically, we wanted to learn:

- Would the subjects notice our manipulations?
- Would traditional training help them improve their ability to detect the deceptions?
- Would warning them help them spot the bad data?
- Would a combination of a warning and just-in-time (JIT) training improve their overall vigilance?

We divided the military personnel into four groups: a control group, a training-only group, a warning-only group, and a warning and JIT-training group.

1) *The control group* received no training in error detection or other information about errors in the database.
2) *The traditional-training-only group* received the 90-minute training on deception methods and how to detect their use via a lecture and presentation slides. This training was given two weeks before the test, when students returned (without warning) to test their ability to detect deception
3) *The warning-only group* was told just prior to the test that someone (e.g., a hacker, a disgruntled student) had been tampering with the course data. They were told to work alone but to record any problems they spotted on a discrepancy-recording sheet.
4) *The warning and JIT-training group* received the same warning as the warning-only group and received the same training as the training-only group, but that training was given just prior to the test.

The Study's Findings

Overall, the human resources specialists were not successful at detecting unauthorized data manipulations. In the control group, the experienced specialists spotted only about two of the 20 pieces of bad data. The training-only group did no better. However, both the warning-only and the warning and JIT-training groups outperformed the controls. Nonetheless, even the best performers only identified six to eight of the deceptions. Figure 2 summarizes the findings for these four groups.

Sage, 1990, pp. 95-116.

Lessons on Traditional Training: Training the human resource specialists two weeks prior to the test proved unsuccessful for both the novice and experienced respondents. Like the control group, the experienced participants in the training-only group found only 2.1 deceptions, on average. The students either apparently forgot or did not use what they had been taught. With all their other duties, and all the other information they were given in their course, this finding is not surprising.

Lessons on Issuing a Warning: The human resource specialists, especially the experienced ones, responded well to the warning that the system had been "hacked." While both the novice and experienced specialists showed promising results, the experienced specialists found significantly more deceptions – on average, 3.8 manipulations – than their counterparts in either the control group or the training-only group.

Lessons on Warning and JIT-Training: Of the three interventions studied, the most successful was to both train and warn employees just prior to the test. Both the novice and experienced specialists detected more deceptions. The experienced specialists found 5.4 deceptions, which was the highest rate, but it was only slightly better than the warning-only group. However, coupling the warning and training also resulted in more false alarms than in any other group. Perhaps their sensitivity was heightened so much that they identified good data as bad.

LESSONS ON DEALING WITH DATA MANIPULATION

In our study, the students could only locate 25 to 30 percent of the deceptive data. Thus, perimeter IT security tools continue to be vital in securing an organization's information and its IT assets. Without these and related defenses, organizations can become 'sitting ducks,' even to novice outside hackers. However, because nearly all these defense mechanisms can be breached, organizations need to take other measures to mitigate their vulnerabilities. One measure is to use their most valued assets: their employees. We offer the following suggestions to managers and CIOs.

Lesson 1: Network Security Tools are Only Part of the Solution; Preparing Employees is Also Necessary

While denial-of-service attacks, Web defacements, and other computer security incidents are indeed problems that can be mitigated, in part, by network security tools; hackers and malicious insiders can manipulate data in a network. Some security tools focus on insider attacks, but these products only catch data manipulations above preset thresholds. Changes made under these thresholds escape detection.

Organizations also need security measures that target users and their data-use behaviors because unauthorized changes to data can cause a range of damage – from the relatively minor damage of having to scrub a tainted database to the potentially significant damage of incorrect tactical and strategic decisions, including the loss of life. Stated simply, building employee vigilance into IT security is the right thing to do.

Lesson 2: Coupling Employee Training With Warnings is Prudent

Our findings do not generate much confidence in traditional training. Formal classroom training for all employees (such as in an annual IT security training session) will probably not lead to more deception detection. Therefore, we recommend coupling short-and-to-the-point training events with warnings during times when deceptive incidents are suspected. Providing a small amount of training at the time of a warning may familiarize employees with the tactics and techniques perpetrators use.

Lesson 3: Simple Warnings Work Amazingly Well

The warned groups in our study did twice as well as the control and trained-only groups, demonstrating that warning employees of potentially tainted data at suspected times can be quite effective. Employee vigilance is likely to wane after a period of time, though, so follow-on warnings may be needed. However, issuing too many warnings may cause a "cried wolf" effect.

However, although coupling warnings with JIT training does produce increased awareness and better deception detection, it also leads to more false alarms. So the most effective intervention strategy is likely to involve periodic warnings and JIT training so that employees are vigilant but do not overreact.

Lesson 4: There's No Substitute for Experience

One of the more valuable assets in an organization's information security arsenal is its employees' experience. We found the experienced human resource specialists twice as successful at spotting deceptive information as the novices. When deceptive information is suspected, novices should therefore consult their experienced co-workers.

CONCLUSION

As organizations increase their dependency on information assets and IT-enabled work processes, they need multi-faceted IT security programs to protect these vital resources. They should augment traditional security mechanisms – those that address networks and data – with programs that address employees as well. Attacks on information from 'inside the fence' are real and can result in costly decision-making errors. Once perimeter security devices have been breached, employee vigilance can become the last line of defense. We found that employees warned at the time of a suspected incident were effective at detecting tainted data elements. This simple warning was more effective, and far less expensive, than formal training. Just as IT security tools need to be kept current, so too do employees need to be continually sensitized to security threats, just not too often to desensitize them. This on-going management responsibility cannot be abdicated to infrequent formal training.

ABOUT THE AUTHORS

David P. Biros

David P. Biros (birosdp@cox.net) is Assistant Professor in the Management Science and Information Systems Department in the Spears College of Business at Oklahoma State University. He earned his Ph.D. from Florida State University in 1998. He retired as a Lt. Colonel from the United States Air Force in 2005. His final duty assignment was as Chief Information Assurance Officer for the Air Force's CIO. His research interests included deception detection and information system trust. He has been a reviewer for *MIS Quarterly* and *Group Decision and Negotiation*. He currently serves as a review panel member for the NSA Centers of Academic Excellence in Information Assurance Education Program.

Joey F. George

Joey F. George (jgeorge@cob.fsu.edu) is Professor of Information Systems and the Thomas L. Williams Jr. Eminent Scholar in Information Systems in the Management Information Systems Department in the College of Business at Florida State University. He earned his bachelor's degree at Stanford University in 1979 and his Ph.D. in management at the University of California at Irvine in 1986. His research interests include detection of deceptive computer-mediated communication, computer-based monitoring, and group support systems. He currently serves as a Senior Editor for *MIS Quarterly* and *e-Service Journal*.

Robert W. Zmud

Bob Zmud (rzmud@ou.edu) is Professor, Michael F. Price Chair in MIS, and Director, Division of MIS in the Michael F. Price College of Business at the University of Oklahoma. His research interests focus on the organizational impacts of information technology and the management, implementation and diffusion of information technology. He currently is a Senior Editor with Information Systems Research, Journal of AIS, and MISQ Executive. He currently sits on the editorial boards of *Management Science*, *Academy of Management Review*, and *Information and Organization*. He previously was the Research Director for SIM's Advanced Practices Council. He is a fellow of both AIS and DSI. He holds a Ph.D. from the University of Arizona and an M.S. degree from MIT.