Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1998 Proceedings

Americas Conference on Information Systems (AMCIS)

December 1998

Errors in Detecting Financial Deception: A Cognitive Modeling Approach

Stefano Grazioli
University of Texas at Austin

Errors in Detecting Financial Deception: A Cognitive Modeling Approach

Stefano Grazioli
MSIS Department
The University of Texas at Austin

Abstract

Organizational agents often need to determine whether business information provided under conflict of interest is intentionally misleading or false. Detecting strategically manipulated information is in general difficult and prone to failure. This research explores the errors made by 18 loan officers when examining misleading financial information. The process traces of the loan officers are compared with the behavior of a cognitive model of detection success derived from Social Contract Theory and the Theory of the Detection of Deception. The results show that one of the keys to successful detection is the ability to 'coming to think' about deception, i.e., the ability to begin interpreting perceived anomalies in the received information as generated by the sender's malicious manipulations. The findings on the distribution of different error types are consistent with the theory, statistically significant, and pragmatically meaningful.

Modeling the Detection of Deception

The increasing diffusion of electronic commerce practices has brought an increased sensitivity to the security and quality of financial information communicated among business parties under conflict of interest. A great deal of work is done to understand, design and build secure information architectures that are able to insure the identity of those involved in the communication, as well as to protect the communication contents from third-parties tampering.

By contrast, relatively less attention (March, 1990) has been paid to the problem of evaluating whether the received information has been maliciously manipulated *by the sender*. Such manipulations are designed to foster misrepresentations of crucial aspects of business transactions and in this way influence the behaviors of the information recipients (e.g., Hansen et al., 1996; Lucas, 1993). Business instances of this 'deception detection' problem include the detection of manipulated insurance claims, applications for loans, and financial reports.

In general, detecting strategically manipulated information is difficult (Ekman, 1995). Failure occurs even when the detectors are trained professionals using sophisticated information technologies and motivated by high stakes (Albrecht et al., 1995). The research presented here is a part of a larger investigation of the determinants of performance at detecting deception in financial settings (Grazioli, 1997). Here we focus on comparing the behavioral trace of a sample of organizational agents with the behavior of a cognitive model of successful detection.

The model is based on the integration of Cosmides' Social Contract Theory (1985; 1992), with Johnson's (et al., 1992, 1997) Theory of Fraud Detection. It implements a psychologically plausible strategy for detecting misleading financial information. The strategy consists of interpreting perceived anomalies in the received information in the light of the goals and possible actions (manipulations) that can be ascribed to the information provider. Processing is composed of four steps: (1) the detection process is triggered by the identification of anomalies, defined as observations that violate their expectations; (2) these anomalies prompt a search for hypotheses that explain them, including the hypothesis that the anomalies result from malicious manipulations; (3) the selected candidate hypotheses are then evaluated and (4) combined to form an overall assessment.

The theory has argued that a key step for success is the generation of the hypothesis that information has been manipulated by its provider (as opposed to - say - identifying anomalies in the provided information, or evaluating candidate hypotheses). Detection failure is explained as the selection of alternative and incorrect hypotheses. These alternative hypotheses explain manipulation-related anomalies as the results of circumstances independent from the information provider (e.g., a low market demand), or as the result of the deceiver's unintentional action (e.g., an accounting mistake).

A Field Experiment on Deception Detection

The banking industry offers an excellent setting to investigate how organizational information recipients (commercial loan officers) detect intentionally incorrect or misleading information communicated under conflict of interest (applications for a business loan). An increasing number of banks accept electronic filings of loan applications and feed the provided financial information into decision support systems used by loan officers to make a decision about the loan.

Eighteen loan officers from a large national bank volunteered in a field experiment designed to study the effect of various levels of knowledge of the goals and possible actions of the information provider on detection effectiveness (Grazioli, 1997). The subjects averaged 15 years of experience in the financial industry, of which 9.5 as a loan officer (std.dev. 5.4 and 7.3,

respectively). All subjects were paid for their participation and performed the experiment in individual sessions during normal business hours. No time limits were imposed. Only data from the control condition (no treatment, first experimental task) are presented here.

Each loan officer received one of three realistic loan application cases and was asked to risk rate it (credit risk rating is part of the officers' routine duties). Each case describes a company applying for a $5 million commercial loan and is based on original documents (SEC filings, newspaper articles, bank procedures manual). Unknown to the subjects, these companies intentionally misstated their financial reports to appear substantively more profitable than they actually were. The manipulations ranged from overstating the prices of inventory, to creating fictitious assets. Arguably, these manipulations (if undetected) give to the companies have a better chance of obtaining an otherwise uncertain loan.

To trace cognitive processing, the loan officers were asked to think-aloud while performing each task. Their verbalizations were recorded, transcribed, segmented and coded according to a reliable coding procedure (Cohen's Kappa = 0.83). Codes were assigned to segments when a subject 1) identified a manipulated piece of information as inconsistent with expectations; 2) generated specific hypotheses about the identified information; 3) accepted a generated hypothesis, and 4) used the generated hypotheses as a basis to form a final evaluation about the creditworthiness of the company.

A model of deception detection (a production rule system) was built according to the theory summarized above. (Johnson et al., 1997) has shown that the model succeeds at detecting the manipulations in the cases used as experimental material. The process traces of the model on the cases were coded using the same scheme employed to code the subjects' protocols. The differences between the process traces of the model and of the subjects define four types of errors, corresponding to the four steps in the detection process:

Error A (Activation error) - This type of error is defined as missing a manipulated cue, or dismissing it early (i.e., after attending to it, but without apparent violation of expectations).

Error B (Hypothesis generation error B1 and B2) - B1 is defined as accepting a manipulated cue as a valid description of the company's circumstances (explain away). B2 is defined as interpreting a manipulated cue as a symptom of a specific adverse economic circumstance (e.g., stagnating demand for the company's products) and/or a cause of adverse financial results (e.g., receivables are absorbing significant amount of cash flow);

Error C (Evaluation error) - This type of error is defined as failing to confirm a generated (correct) hypothesis.

Error D (Assessment error) - This type of error is defined as selecting a final outcome for the task that fails to take into account the hypotheses that have been previously generated.

The results of the comparison between the model and the subjects is presented next.

Results

Only four subjects out of 18 (22 percent) succeeded at identifying the loan applications as misleading. The remaining fourteen officers either concluded that the company is a viable business partner (six) or concluded that the evaluated company is experiencing some economic hardship (eight), which lowers its credit rating.

Forty-seven instances of the five types of errors were identified. The most frequent error is the activation error A: 24 occurrences out of 48 opportunities to err, or 51 percent of the total errors observed in the experiment. The least frequent error is evaluation error C: no occurrences were observed in this sample (a few were observed in the cited larger study). Fifteen hypothesis generation errors were found: 10 B1s and 5 B2s. Finally, eight assessment errors D were identified. The subjects in the sample had 24 opportunities to make error B and as many opportunities to make error C and D.

The errors made by the loan officers who succeeded were compared to the errors made by those who did not. A statistical analysis of the distribution of the errors concluded that the subjects significantly differ in terms of average errors/opportunity-to-err ratio. On average, successful subjects made 0.18 hypothesis generation errors B per opportunity. By comparison, unsuccessful subjects made 0.91 errors per opportunity ($p < 0.000$). Very consistently with the theory, successful and unsuccessful subjects were not significantly differentiated by the frequencies of activation, evaluation, and assessment errors (A, C, and D; $p > 0.55$).

Conclusions

On average, the loan officers that participated in the experiment were not very accurate in detecting financial deceptions. While the field experiment is vulnerable to criticism based on the nature of the experimental procedure employed (e.g., no face-to-face communication with management, no established history with the client, reliance on information provided by management), the reported results are consistent with the detection rates found in the literature, as well as the electronic commerce practices that are becoming more popular in the banking industry.

While in principle any one of the sub-processes composing the detection of deception can go wrong, it was found that this is not the case. Errors do not distribute homogeneously. A general lack of sensitivity to the clues to deception (error A) was observed. Also, and consistently with the theoretical expectation, it was found that the ability to generate the hypothesis that information is intentionally false or misleading is a key for success.

These findings can be straightforwardly translated into simple design principles for improving the information technology currently used by the bank. The high frequency error A may be reduced by a procedure that highlights key ratios or balances

when they violate industry and history expectations *and* are functional to the opportunistic goals that can be ascribed to management (e.g., overstate profitability to obtain the loan). Error B may be reduced by a procedure that suggests interpretive hypotheses for the detected anomalies based on the notion of deception, similarly to what the model described here does. Interestingly, although the loan officers in the study used a decision support system for financial analysis, their system did not provide either one of these functionalities.

References

The list of references can be obtained by sending a request to grazioli@mail.utexas.edu.