CERIAS Tech Report 2001-37

Information Assurance in Networked Enterprises: MICSS Class Experiment and Industry Survey Conclusions

Thomas Bellocci, Chwee Beng Ang,
Parbati Ray, Shimon Y. Nof
Center for Education and Research in
Information Assurance and Security
&
School of Industrial Engineering, No. 01-08
Purdue University West Lafayette, IN 47907

MICSS Class Experiments and Industry Survey Conclusions[1]

Parbati Ray, Advisors: Thomas Bellocci and Shimon Y. Nof

ABSTRACT

Two surveys have been developed to ascertain the information assurance requirements of networked enterprises. The surveys give an insight into how inter-networked companies use their ERP systems, what their current policies maybe with respect to information management, and what their security and assurance problems maybe.

The surveys focus on the views of the information manager of the firm and on the department managers of those departments that depend mostly on their information systems for smooth running.

The survey questions have been based on quantitative analysis done by experiments using an ERP software simulator, MICSS (Management Interactive Case Study Simulator). The logic and procedures used to develop the surveys has been presented. The results obtained from the analysis of the survey replies will enable the design of autonomous agents and active protocols to help companies automatically assure their information.

[1] This work was supported by sponsors of the Center for Education and Research in Information Assurance, Purdue University

TABLE OF CONTENTS

1. Introduction:

Companies today, find it difficult to decide whether the information they have is reliable or not. Security was one issue, however now the concern is not merely security, companies need the assurance that information bears its integrity, is significant and secure. Although networks have revolutionized the exchange of information; they have failed to ensure that the customer receives secure and assured data. With the advent of technology, the concept of sharing information within an organization is increasingly gaining importance. Companies are now seeking new approaches regarding the administration of distributed information systems. At the same time, workers need more and repeated training to operate with increasingly complex information systems; they look upon security practices as a factor in slowing them down in performing their jobs. Hence, it is necessary to automate the required assurance practices as much as possible, and to expect the information system to apply them, not the workers who interact with the system as part of their job. In other words, information assurance tasks must be handled in the background, in parallel with the users working with the system's information.

The aim of this research project is to design autonomous agents and active protocols to help companies automatically assure their information. In order to do so, it was necessary to first identify information assurance requirements for an ERP system, the parameters that could significantly affect information assurance and the potential consequences of assurance failure on the performance of a company. This research memo covers a part of the above aim: a detailed analysis of the parameters and variables that may significantly affect information assurance. An elaborate survey has been developed to understand how inter-networked companies use their ERP systems, what their current policies regarding information management maybe, and what their security and assurance problems are.

2. Literature Review

In order to completely understand the concept of information assurance for this research, a number of relevant articles were read.

Time and Intranets: Time is an important factor in information systems and needs to be harnessed. The importance of improving communications and compressing time has become vital for the smooth functioning of a company. Hence the goal is to come up with a system that shall not only allow on-time exchange of information, but also ensures that it is reliable and accurate. Intranets are the best solution. The impact of modern information technology via intranets has proved to be major in terms of speeding up activities [8]. Intranets provide a perfect solution as they ensure accuracy in addition to security. A secure Intranet can be built easily with the existing technology and can be replicated and scaled throughout an organization to provide a set of managed information services. Focus needs to be put on the main security issues, which are in the policy and procedural areas, rather than technological ones [11].

Agility: Information Technology has helped enterprises by the way of introducing more flexibility, increasing productivity and agility. Today, enterprises are considered to be internet-worked and enterprise agility is the main concern of the global market. Agility is thought to be an important factor of economic competitiveness and has been viewed from two perspectives: business and organizational agility and operational and logistics agility. From the business and organizational agility perspective an analytic method called the distributed parallel integration evaluation model (DPIEM) has been developed. In terms of operational and logistics agility in such distributed organizations, the connection between the autonomy functions and agility requires significant functions of error detection and recovery (EDR), and conflict resolution (CR).

DPIEM assists designers in determining the number of resources required in each organization for effective execution of given interrelated tasks, while keeping the total integration cost minimal [9].

TQM Approach:

Businesses today have become so dependent on IT that even a short non-availability of a critical system may result in huge losses [2]. Realizing their importance it is necessary to ensure that they are appropriately secured. It is however very rare to find such a method that will take care of *all* its requirements. No particular method is absolutely correct.

It is common sense that if a set of assets is of *high* value to an organization and if the likelihood of a threat occurring is *high* and if there is a vulnerability that can be very *easily* exploited by the threat then the level of risk is high [7]. We must however understand what is *high*, *low*, *easily*, and this leads to the debate about qualitative as opposed to quantitative methods. Clearly there will be a combination of values and hence various possibilities when classifying the data into a certain risk level.

Irrespective of the range of risk levels, it is obvious that with the increase in risk, the protection should increase. And hence there should be an effective countermeasure (an application to detect and remove the risk) too.

Enterprises can now collaborate with each other to best adapt to various customer's demand changes in tastes, design, time, and quantity, while keeping the cost at a reasonable level. Information Technology has increased the speed of activities, provided intelligent and autonomous decision-making processes and enabled distributed operations with collaboration along communication networks.

3. Problem Introduction

3.1. Purpose of the experiment

Assurance as defined in [12] includes information security, integrity and significance. The functioning model of people using a distributed information system can be of two types: collaborative and non-collaborative. On collaborating, three levels of information are obtained: correct, correct but delayed and wrong (Fig. 2).

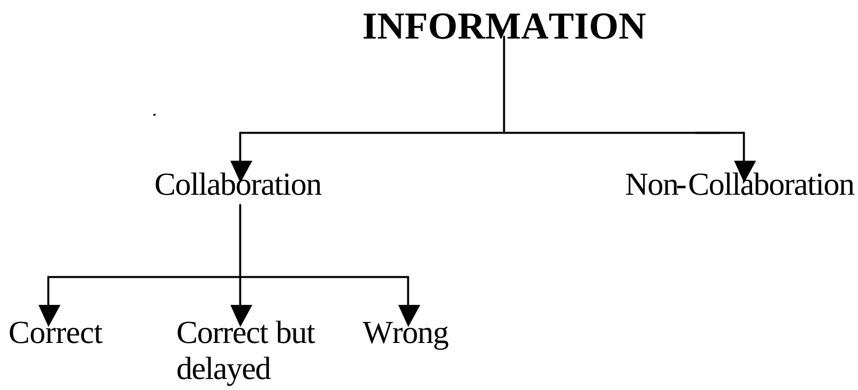


Figure 1. Communication Scenarios in Distributed Information Systems

It was decided to study the influence of dataset, length of delay and error size (difference between the correct data and the wrong value) for the three scenarios described above, namely correct, correct but delayed, and wrong information.

3.2. Hypotheses

The hypothesis of the experiment was that the profits and DDP of the company in the case of delayed and wrong information would be different from the case of correct information.

H_0 = Performance (Profit or DDP) in the case of information failure (delayed or wrong information) is similar to the performance of the correct information.

H_1 = they are significantly different.

$\alpha = 0.05$ (a 95% confidence interval to prove the hypothesis.)

if p val ≤ 0.05,we can conclude with 95% confidence that we reject the null hypothesis H_0

To verify the above hypothesis, the data was analyzed using single factor ANOVA, an analysis tool in EXCEL.

4. Method

4.1. Equipment

MICSS (Management Interactive Case Study Simulator) [16] is an ERP simulator that has been developed to simulate the functioning of a company with a team-oriented view.

MICSS has four views of a company, namely Marketing, Production, Purchasing and Finance. Each of these views has certain policies, which combine in an optimal way in order to be profitable for the company. However often the four departments of the company are unable to communicate properly and this creates discrepancies in the policies developed and hence, in information assurance.

MICCS enables us to simulate the functioning of a company through one year.

4.2. Design of experiment

We have decided to study 4 factors in this experiment.

Factor 1:
Dataset; with 4 levels: Prices, QLT (Quoted Lead Time), Batch Size, and Order Levels.
Factor 2:
Failure type; with 2 levels: “wrong information”, and “delayed information”
Factor 3 (nested in “wrong information”):
Error size; with 2 levels “value doubled”, and “value halved”.
Factor 4 (nested in “delayed information”):
Length of delay; with 2 levels “1 quarter”, and “2 quarters”.

So, we finally had 17 scenarios to simulate:

<u>List of all the scenarios:</u>

-*Correct information:*

(1) Baseline policy

-*Wrong information:*

(2) QLT doubled
(3) Prices doubled
(4) Batch Size doubled
(5) Order Level doubled
(6) QLT divided by 2
(7) Prices divided by 2
(8) Batch Size divided by 2
(9) Order Level divided by 2

- *Delayed information:*

(10) QLT delayed 1 quarter
(11) Prices delayed 1 quarter
(12) Batch Size delayed 1 quarter
(13) Order Level delayed 1 quarter
(14) QLT delayed 2 quarters

(15) Prices delayed 2 quarters
(16) Batch Size delayed 2 quarters
(17) Order Level delayed 2 quarters

4.3. Metrics

To assess the performance of the company, the Profit and the Due Date Performance (DDP) values were recorded. These 2 parameters were chosen since profit represents how the whole company is performing, and the DDP gives an idea of how well the company is organized.

4.4. Experimentation Procedures

Wrong information scenarios

In order to make the data 'wrong', correct data was either doubled or halved. This was done separately with each of the four variables to be tested, giving 8 scenarios to be analyzed.

10 runs of one year are performed for each scenario.

Delayed information scenarios

In order to 'delay' information, the correct data item of the baseline policy was randomly modified by the students. After 1 or 2 quarters, the correct information was entered and the experiment was run for the remaining year.

10 runs of one year are performed for each scenario.

N.B. For each scenario 10 runs per year had to be conducted in order to have a representative sample of results on which statistical analysis maybe conducted. Unfortunately, due to the lack of control on the way the class conducted the experiment, some sets of datasets had 15 runs for some scenarios and 5 runs for others, which reduced the accuracy of the experiment.

5. Results

The observations haven't been analyzed like a nested design. We didn't need all the information given by a nested design analysis. For simplicity and time saving, we have used single ANOVAs to compare each time two different scenarios.

For each dataset, the following comparisons are presented in [14]:
Dataset delayed 1 quarter / Baseline policy (for profit).
Dataset delayed 2 quarters / Baseline policy (for profit).
Dataset wrong half / Baseline policy (for profit).
Dataset wrong double / Baseline policy (for profit).

The datasets are presented in this order: Prices, QLT, Batch Size, Order Level.

Summary of the figures available in [14]:

Prices

Fig.A1 - Dataset delayed 1 quarter / Baseline policy (for profit).
Dataset delayed 2 quarters / Baseline policy (for profit).

Fig.A2 - Dataset wrong half / Baseline policy (for profit).
Dataset wrong double / Baseline policy (for profit).

QLT

Fig.A3 - Dataset delayed 1 quarter / Baseline policy (for profit).
Dataset delayed 2 quarters / Baseline policy (for profit).

Fig.A4 - Dataset wrong half / Baseline policy (for profit).
Dataset wrong double / Baseline policy (for profit).

Batch Size

Fig.A5 - Dataset delayed 1 quarter / Baseline policy (for profit).
Dataset delayed 2 quarters / Baseline policy (for profit).

Fig.A6 - Dataset wrong half / Baseline policy (for profit).
Dataset wrong double / Baseline policy (for profit).

Order Level

Fig.A7 - Dataset delayed 1 quarter / Baseline policy (for profit).
Dataset delayed 2 quarters / Baseline policy (for profit).

Fig.A8 - Dataset wrong half / Baseline policy (for profit).
Dataset wrong double / Baseline policy (for profit).

Notations:

"D" means: The two scenarios give significantly different results.
"D –" means that the performance with information failure, for profit or DDP, is worse than with the baseline policy.
"D +" means that the performance with information failure, for profit or DDP, is better than with the baseline policy.
"S" means: The two scenarios give significantly similar results.

Due to inconsistencies in the way the class performed the experiment, results for DDP are not available.

Only the results concerning Profit are presented below.

Table 1

		Baseline Policy			
		Period 1	**Period 2**	**Period 3**	**Period 4**
Delayed 1 quarter	Prices delayed	D -	D -	D -	D -
	QLT delayed	D -	D -	D -	D -
	Batch Size delayed	D -	S	D -	D -
	Order Level delayed	D -	S	S	S

Table 2

		Baseline Policy			
		Period 1	**Period 2**	**Period 3**	**Period 4**
Delayed 2 quarters	Prices delayed	D -	NA	NA	D -
	QLT delayed	D -	D -	D -	D -
	Batch Size delayed	D +	S	S	S
	Order Level delayed	D +	S	D -	D -

Table 3

		Baseline Policy			
		Period 1	**Period 2**	**Period 3**	**Period 4**
Wrong Half	Prices wrong	S	D +	D +	D +
	QLT wrong	S	S	D -	D -
	Batch Size wrong	D +	D +	D +	D +
	Order Level wrong	S	S	S	S

Table 4

		Baseline Policy			
		Period 1	**Period 2**	**Period 3**	**Period 4**
Wrong Double	Prices wrong	S	D +	D +	D +
	QLT wrong	D -	D -	D -	D -
	Batch Size wrong	S	S	S	S
	Order Level wrong	D -	D -	D -	D -

For profit:

- In case of delayed information: Price and QLT effects are significant, however they persist only for short periods of time, after which the profit decreases are reduced, implying information delayed for long periods of time have relatively less drastic effects.
- In case of wrong information: QLT and order level failures show the most negative profits for values that are wrong only by half the amount of the correct value. Wrong information for prices and Batch Size seem to be profitable for the company.

6. Conclusions and Discussion

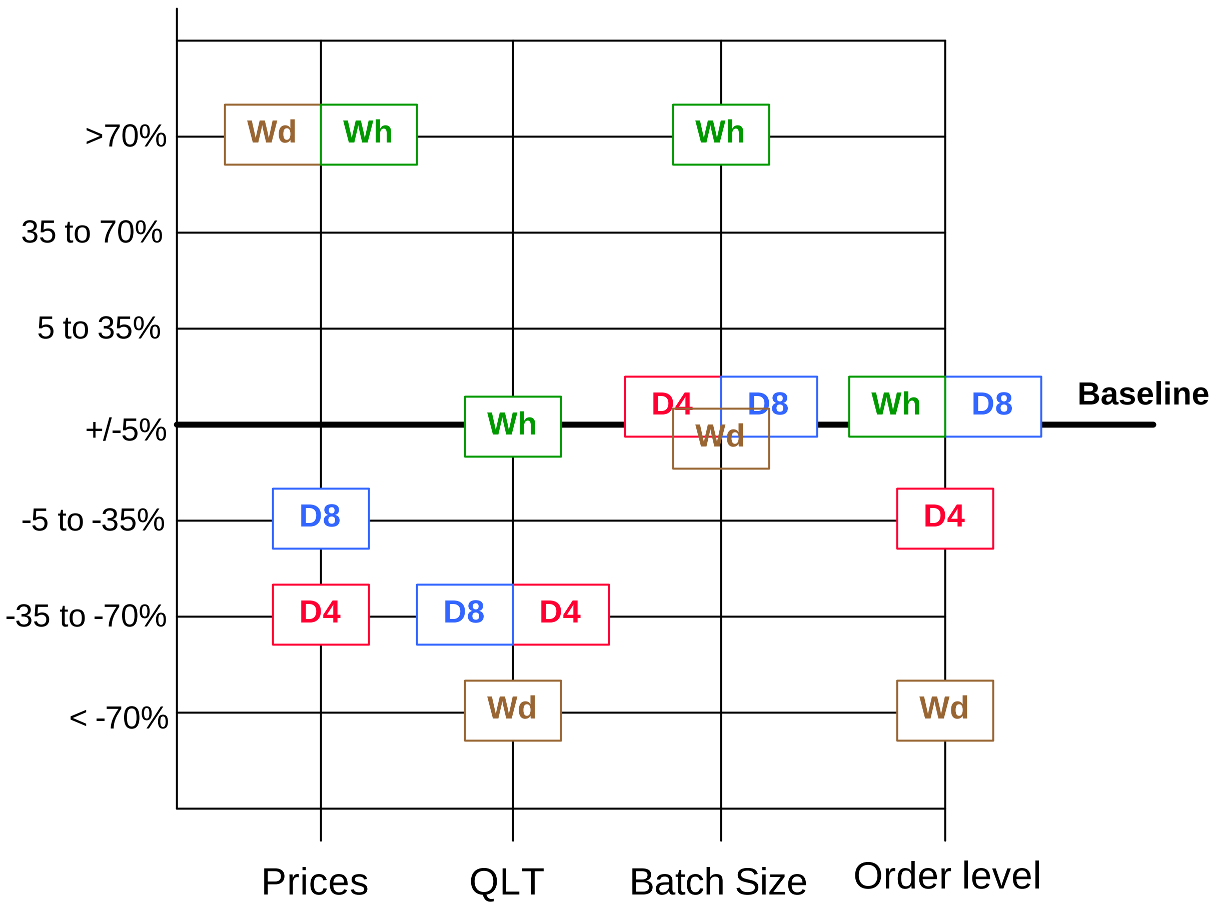
6.1. Impact Graphs

This graph summarizes the impact of each information failure type by dataset.
The relative difference:
(Profit with information failure – Profit with baseline policy) / (Profit with baseline policy), is represented.
The differences are shown using levels: [> 70%; 35 to 70%; 5 to 35%; +/- 5%; -5 to –35%; -35 to –70%; < -70%]

The following notations are used:

D1: scenario with information delayed 1 quarter
D2: scenario with information delayed 2 quarters
Wh: scenario with information wrong half
Wd: scenario with information wrong double

Figure 2 - Information Failure Impact on Profit



6.2. Conclusions

The experiment led to the conclusion that companies should be able to differentiate between some of the variables that may affect their ERP systems. It can be detected as seen from the experiment that effects due to changes for some of the variables are significantly different.

On the basis of the sensitivity analysis of the research experiment, it was seen that prices were most sensitive to any change. It is followed by Batch Size, QLT and then Order Level.

This experiment allowed the team to understand that different variables effect the performance of a company, the may effect significantly or insignificantly.

The class experiment performed by IE 332 gave a general idea of the results. However inconsistencies in the way the groups performed the experiment made it necessary to run a research group experiment described in [12, 13].

6.3. Comparison of the class and the team experiment

The two sets of experiments are not fully comparable. For the class experiment one year was divided in 4 periods of 3 months, whereas for the team experiment one year was divided in 6 periods of 2 months. Moreover, the class experiment results did not have the same number of runs for each scenario and the students may not have been consistent in their methods of conducting the experiment.

As mentioned earlier it is difficult to compare the two sets because the profits of the company were not recorded in a similar manner during the two experiments. The variability between correct, wrong and delayed information was observed to be much more important in the class experiment than in the team experiment [13]. This was certainly due to variability in experimenting methods between students groups. Nevertheless, "Order Level" appeared to be much more sensitive to information failure in the class experiment than in the team experiment. Experience tends to prove that wrong order level have influence on the performance of a company. This was not the case in the team experiment. This result can depend on the simulation model used in the MICSS software.

7. Industry Survey

7.1. Description

On the basis of the lab experiments an industry survey was conducted to assess the information assurance requirements of the corporate world.

Two surveys were designed. One was sent to the information system manager of a given company, and another one to the department managers of the same company (e.g. Production manager, Marketing manager…). The objective of the first survey was to assess the equipment and general approach of the company regarding information security and assurance. The second survey was designed to study the actual information assurance problems encountered by user of the company's information system.

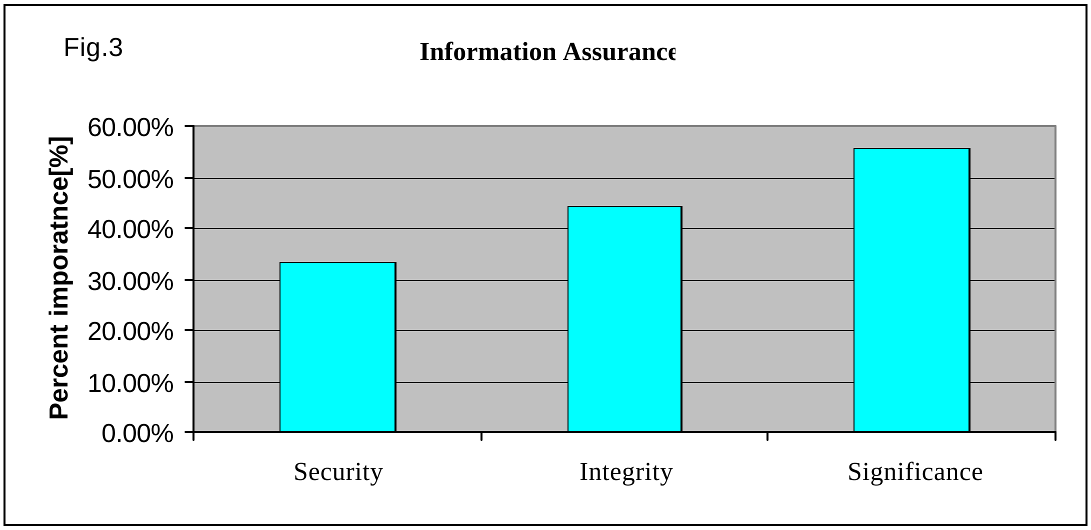
The cover letter, as well as the 2 types of survey that were sent to companies, may be found in [14].

7.2. Results

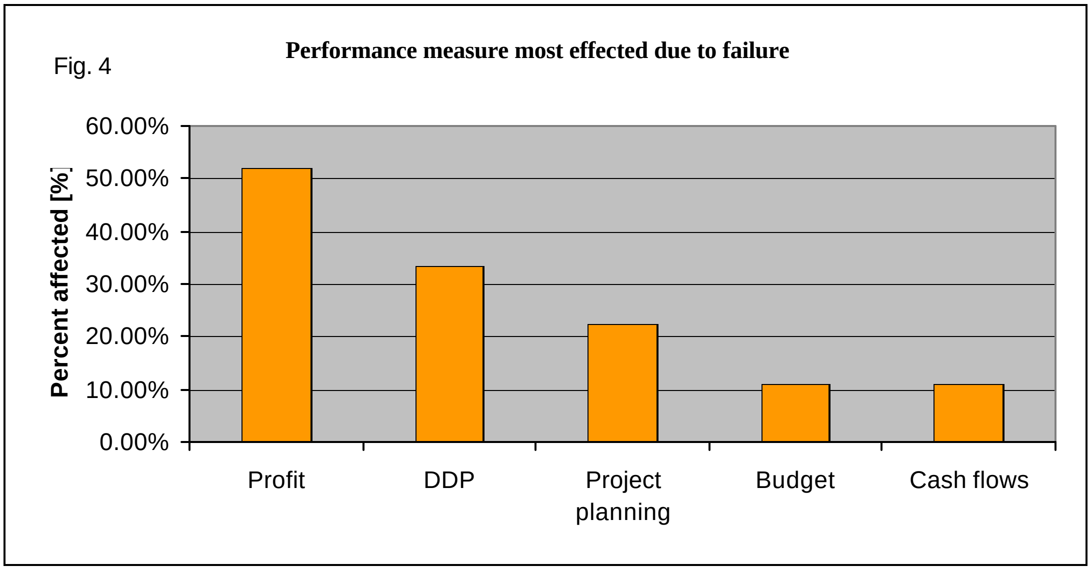
19 survey replies were obtained and analyzed (9 from information systems managers, and 10 from department managers). They are presented in [14].

7.3. Conclusions

- From the analysis of the survey it is inferred that companies are looking for information significance more than information security or integrity (Fig. 3).

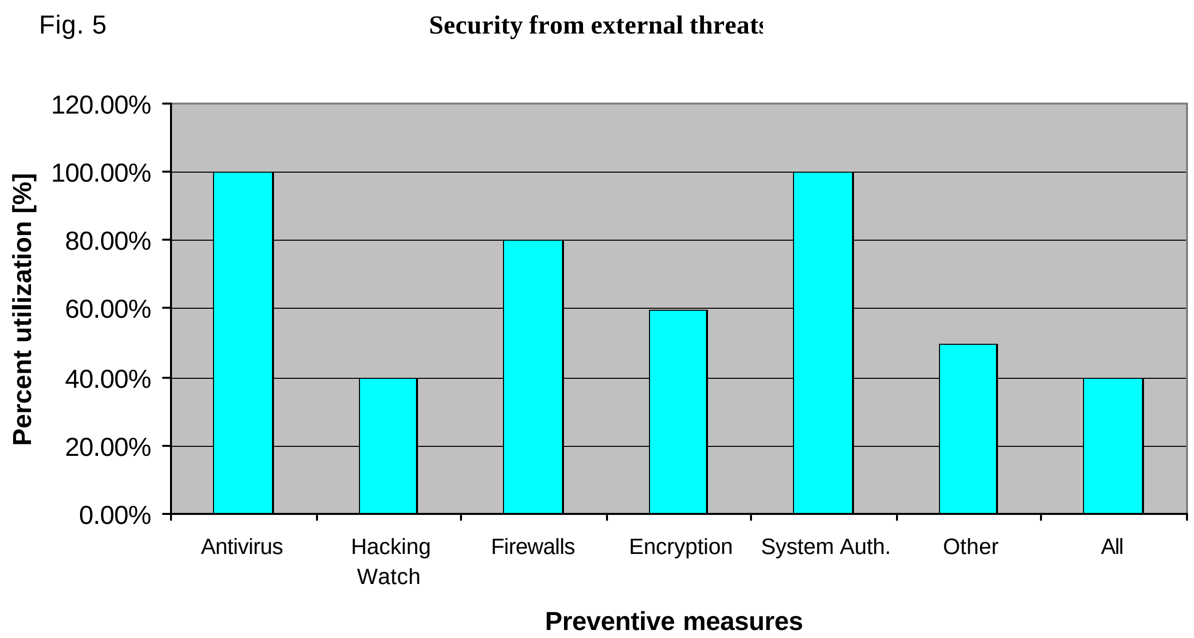


- Further analysis shows that indeed Profit and Due Date Performance (the reputation of the company) are the parameters that are the most affected by information failure (Fig. 4). This result justifies the use of Profit and DDP as metrics in our Lab and Class Experiments [13,14].



- At present, System Authorizations, Firewalls and Antivirus are the most popular preventive measures that the companies have. (Fig. 5). This shows that companies are equipped to handle information security and integrity problems, but not to handle information significance problems yet.

Fig. 5



REFERENCES

[1] Wang R.Y., Total Data Quality Management, *Communication of the ACM*, v.41, n.2, February 1998

[2] Schwartz A.P. and Zalewski M.A., Assuring Data Security Integrity at Ford Motor Company, *Information Systems Security*

[3] Steinitz D., Information Security Management at British Airways. Implementing a Strategic Security Program, *15th World Conference on Computer Security*, November 1998

[4] Voas J., Protecting against what? The achilles heel of information assurance, *IEEE Software*

[5] King C., Intranet Application Security Checklist, *Computer Security Journal*, 1997, Vol. 13

[6] Finne T., What are the information security risks in decision support systems and data warehousing?, *Computers & Security*, 16(3), 1997, 197-204

[7] Ciechanowicz Z., Risk analysis: requirements, conflicts and problems, *Computers & Security*, 16(3), 1997, 223-232

[8] Mercer E., Getting time on our side, *Manufacturing Engineering*, 77(4), 1998, p 174 – 175

[9] Huang, Chin-Yin, Ceroni, Jose A., Nof, Shimon Y., Agility of networked enterprises – parallelism, error recovery and conflict resolution, *Computers in industry*, v 42 n 2 2000. p 275 - 285.

[10] Sutterfield L. and Schell T., Corporate Information Protection Program: Concept of Operations, *Computer Security Journal*, 13(1), 1997, p 31 – 38.

[11] Collins, B., Designing secure intranets, *Manufacturing Engineer*, 77 (6), 1998,264-268

[12] Bellocci, T. Ang, C.B. Parbati, R. and Nof, S.Y., Information Assurance in Networked Enterprises: Definition, Requirements, and Experimental Results, *CERIAS Technical Report 2001-34, Research Memo School of Industrial Engineering No. 01-05*, Purdue University, January 2001

[13] Bellocci, T. and Nof, S.Y., Information Assurance: MICSS Lab Experiments, Results and Analysis, *CERIAS Technical Report 2001-35, Research Memo School of Industrial Engineering No. 01-06*, Purdue University, January 2001

[14] Ray, P., Bellocci, T. and Nof, S.Y., Information Assurance in Networked Enterprises: MICSS Class Experiments and Industry Survey Analysis, *CERIAS Technical Report 2001-38, Research Memo School of Industrial Engineering No. 01-09*, Purdue University, June 2001