CERIAS Tech Report 2001-57

Context Of Information Assurance In Inter-Networked Enterprises

Thomas Bellocci, Shimon Y. Nof
Center for Education and Research in
Information Assurance and Security
&
Department of Industrial Engineering
Purdue University, West Lafayette, IN 47907

Context Of Information Assurance In Inter-Networked Enterprises

Thomas Bellocci and Shimon Y. Nof
Center for Education and Research
in Information Assurance and Security
and
Department of Industrial Engineering, Purdue University
West Lafayette, IN 47907-1398 USA

Abstract

The development of inter-networked enterprises created a new computing environment in which information assurance is critical. The objective of this article is to investigate the information assurance needs of today's companies. For this purpose, the literature dealing with information assurance is reviewed. A new definition of information assurance is also introduced following the TQM approach to better fit the needs of inter-networked enterprises. A list of requirements for information assurance is developed. The critical aspects of information assurance failures in ERP systems are also investigated using MICSS lab experiments and an industry survey.

Keywords: Information assurance, ERP, Requirements, TQM, MICSS, Industry survey

1. INTRODUCTION

Companies' organization and functioning have changed dramatically under the influence of information technology. Information systems have evolved from a centralized to a distributed organization. This change has enabled the development of inter-networked enterprises.

In these companies, information systems do not only support business functions but they are also integral parts of the business operation. For example, ERP systems (Enterprise Resource Planning) are essential for organizations and their supply chains. Companies completely rely on their information system for the execution and coordination of daily business operations.

Critical issues, however, are facing nowadays the enterprise information systems. Companies often have trouble obtaining valuable, timely information and exchanging correct data between different departments of the company. The distribution of information sources, and the high speed of data transfer have increased the vulnerability of companies to information failures and the impact of these failures on the performance of organizations. Incorrect information in ERP systems can have serious consequences for inter-networked companies. These problems become even more critical when a company tries to manage its supply chain. As a consequence, it is necessary to develop a definition of information assurance that fits the actual needs of inter-networked companies, and discover if there exist specific information assurance failures that are critical for the performance of a company.

2. INFORMATION ASSURANCE: DEFINITION AND REQUIREMENTS

2.1. Literature review

a. Information assurance and security

The topic of information assurance and security has been originally described mainly by computer scientists. Their approach of information management focuses on information security from internal and external threats (e.g., Longley and Shain, 1986; Shirey, 1995; Finne, 1997; Voas, 1999).

Network security management is defined by Shirey (1995) as "supporting security policies by monitoring and controlling security services and mechanisms, distributing security information, and reporting security events." The functions associated with network security management are: controlling access to resources, retrieving and archiving security information, and managing and controlling the encryption process.

Automated information system security implies "the totality of security safeguards needed to provide an acceptable level of protection for the system and for data handled by it" according to the definition proposed by Longley and Shain (1986). Information assurance in computer security has also been defined. A clear distinction is made between information security and information assurance by Dobry and Schanken (1994). Information security is a feature of the functional components of a product or system, whereas information assurance refers to the quality of the development and testing process, of the development environment, and of the operational support for the product or system. Information assurance is defined more synthetically by Longley and Shain (1986): "it is a measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce the security policy." A slightly different definition is provided by Jelen and Williams (1998): "Assurance is a measure of confidence in the accuracy of a risk or security measurement". This traditional definition of information assurance, however, does not fit the current needs of industrial applications. Today's networked enterprises are primarily concerned with the quality aspects of their information for the purpose of achieving their performance goals, and with reaching a global improvement in the trustworthiness and value-addition of information.

b. TQM, quality assurance and information systems

In the literature dealing with information management, different approaches to information can be found. On the one hand, an approach focusing on information security

from internal and external threats, described in Section 2.1.a., and on the other hand, there is an approach emphasizing information's accuracy, value-addition and related features.

Several articles show that companies are now seeking new approaches regarding the administration of distributed information systems. Ford Motor Co. has developed automated features to monitor and maintain its distributed information system as described by Schwartz and Zalewski (1999). The goal is to detect security weaknesses, for instance in the definition of a given user rights, and correct them before anyone can use it to perform malicious actions. British Airways has also started to think about the value-addition of information in its distributed information system. This reflection has been coupled with consideration of security at the physical level, as described by Steinitz (1998). These efforts show that companies seek new approaches for information system administration. They are concerned with quality assurance related features.

Some research work has already tried to apply a TQM approach to data management. A description of data characteristics has been developed from a user-centered approach by Wang (1998). He explains that any piece of information has the following quality dimensions: intrinsic quality (accuracy, objectivity, believability, reputation), accessibility (access, security), contextual value (relevancy, value-added, timeliness, completeness, amount of data), and representational value (interpretability, ease of understanding, concise representation, consistent representation). According to Wang, the quality dimensions must be taken into consideration in the TDQM (Total Data Quality Management) approach.

c. Information assurance survey of requirements

Without clear knowledge of the true needs for information assurance, a company may employ local, specialized solutions that are too restrictive, or not comprehensive. The challenge is to ascertain what the true assurance requirements are for given industries, in order to develop the most effective means to address the problem.

There are two ways of surveying requirements. On the one hand, people can use literature review and experts' knowledge to analyze their problem and see what the key issues are. On the other hand, people can conduct surveys among information systems' users to understand what the key issues are from a description of the system routine use.

Several articles summarizing experts' knowledge in the field of security requirements can be found. Dobry and Schanken (1994) explain that security requirements have started with the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), also known as Orange Book (originally defined in 1985). These criteria were meant to provide software manufacturers with a standard to assess the security level of their products. They have been updated to become the Federal Criteria in 1993. Nevertheless, these criteria were not able to encompass distributed systems in the rating scheme. Efforts to develop criteria to assess distributed systems are continuing. Dobry and Schanken develop, however, useful information about distributed systems security requirements, which can be categorized as either functional, or assurance related. The functional requirements are: Identification and Authentication, Trusted recovery, Security management, Trusted path, Access control, Audit, Availability, Cryptography, Data confidentiality, and Data integrity. Assurance requirements are also presented. Their objective is to make sure that developers have kept in mind the functional requirements in every step of the development process. These assurance requirements are not included in the scope of this research.

Network management functions were described by Shirey (1995). Shirey also lists the security requirements for network management data. They are: confidentiality, integrity, authentication, access control, non-repudiation and availability. Some security requirements for intranet applications are described by King (1997). A checklist is provided. In particular, it comprises: information classification (datasets), employee identification (identification and definition of user groups), firewall, backups, intrusion detection tools, and encryption. Another field is described by Pfleeger (1991), who focuses on the requirements leading to security certification of software applications. Pfleeger provides a complete framework to carry out a quantitative assessment of software application security. In particular, the framework reduces security requirements into three categories:

a. *Confidentiality*, the state that exists when data are held in confidence and are protected from unauthorized disclosure,

b. *Integrity*, the state that exists when computerized data are the same as those in the source document, or have been computed correctly from source data,

c. *Availability*, the state that exists when automated data processing services can be obtained within an acceptable period of time.

These articles, dealing with requirements surveys, prepared a starting list of security requirements. This list was completed to match the problem of information assurance (see Section 2.3.).

2.2. TQM-based definition

As indicated above, companies require more than information security. Wang (1998) pointed out the need for companies to have information that has intrinsic, access, contextual, and representational dimensions by applying Total Quality Management to data. In this thesis, Wang's useful work is combined with further consideration of security aspects. When information systems become the spinal cord of modern companies, these companies must have a reliable system that provides secure and useful information, and these systems have to manage security and assurance problems by themselves.

Based on this initial work, it has been concluded that an information system is worthwhile if it can ensure that its information is secure, keeps its integrity, and maintains its significant value for users. As a result, information assurance (Figure 1) can be defined as the combination of:

1) Information security
2) Information integrity
3) Information significance

Information security means protecting information from malicious threats and damage due to external or internal sources.

Information integrity should be understood as permanency of the information during communications and storage.

Lastly, *information significance* refers to the value that the intended user can get out of the information when s/he receives it.

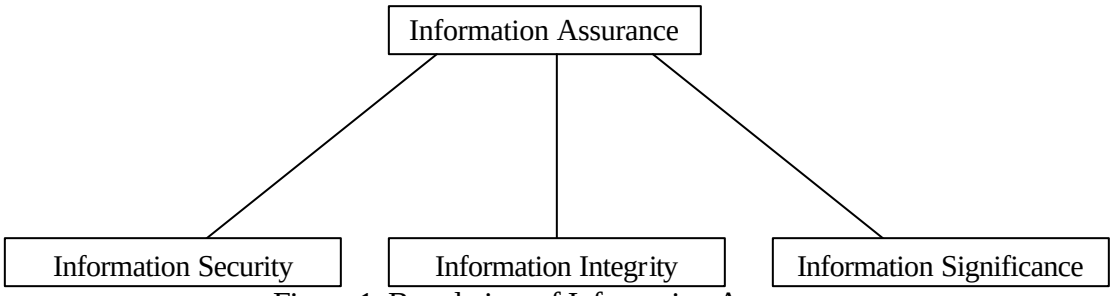


Figure 1. Broad view of Information Assurance

The definition traditionally used in computer science (e.g., Longley and Shain, 1986; Jelen and Williams, 1998) states that information assurance is "a measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce the security policy".

However, this definition does not fit the broader view of the information assurance problem. The broader view considers assurance from the viewpoint of "quality assurance". The broader definition is proposed as follows:

- Information assurance combines the requirements of information security, integrity and significance.
- Assuring information means having a safe information system, which guarantees that information is secure and at the same time keeps its integrity and its significance during its lifetime.
- The goal of information assurance is to provide trustworthy and significant information to users in operational, service systems that rely on the information for the fulfillment of their objectives.

2.3. Requirements for information assurance

A preliminary analysis generated a list of all the requirements a company must fulfill if it wants to assure its information (Table 1). For each category, a non-exhaustive list of measures is shown that can guarantee that the category is fulfilled. Currently, the examples (in italics) are technical issues that may change with the state of the art.

One must understand that Table 1 points out comprehensive requirements (non italic) that must be fulfilled to assure information in networked enterprises. It can be noticed that some of the requirements specified for information security have been previously described by Schwartz and Zalewski (1999) regarding the RACF parameters (Resource Access Control Facility) developed by IBM.

2.4. MICSS lab experiments

As a step in refining the assurance requirements derived from the literature, and showing the variable needs in information assurance, experiments were conducted with an ERP software simulator called MICSS (Management Interactive Case Study Simulator) [http://www.mbe-simulations.com/, June 2001]. MICSS was used to simulate the functioning of a company with a team-oriented view. There are four views of a company, namely Marketing, Production, Purchasing and Finance. Each of these views can combine to operate the company to be profitable.

Table 1. Requirements of information assurance
(based on literature review, lab experiments and an industry survey)

Information Assurance		
Information Security requires:	**Information Integrity requires:**	**Information Significance requires:**
Protection against external threats: • *Anti-virus* • *Intrusion detection* • *Firewalls* • *Encryption, personalization* • *System authorizations (login + password)* **Access profiles management:** Profiles and attributes definition: • *Users groups*	**Data integrity:** • *Preventing data decay* • *Preventing accidental loss of data* • *Updating and maintenance* **Communications integrity:** • *Assuring quality of communications links* • *Recovering from*	**Intrinsic value of information:** • *Accuracy* • *Objectivity* • *Believability* **Contextual value of information:** • *Relevancy* • *Value-added* • *Timeliness* • *Completeness*

• *Class authorizations* • *Attribute of groups* Profiles and attribute maintenance: • *No user with non-standard password intervals* • *No inactive user IDs* **Data logging:** • *Global access table entries* • *Started task table entries* • *Class descriptor table entries* • *Dataset name table entries* • *Range table entries* • *Inbuilt audit trails* **Data management:** • *Definition of sensitive dataset profiles* • *Definition of general resources profiles*	*transmission failures* • *Ensuring that the data of receiver and sender map correctly* **System recovery:** • *Restarting the system after it crashes* • *Reverting to stable state after system interruption*	• *Correct amount of data* **Representational value of information:** • *Interpretability* • *Ease of understanding* • *Concise representation* • *Consistent representation*

In an ERP system, a company enters an operational policy P to ease and automate some of the basic functions of the business, such as production planning. A policy can be described as a k-tuple recording the value d_i of each data item D_i composing the policy; e.g. $P = (d_1, d_2, \ldots, d_k)$. Often the company follows a baseline policy BP, recognized to provide good performance results regarding profits π and due-date-performance DDP.

As a consequence, three typical scenarios regarding information can be encountered in an ERP system. When the company whishes to input its baseline policy BP, the value d_i of a data item D_i can indeed be one of the following:

1. Correct, defined as BP
2. Correct but delayed, defined in this research as $D4(D_i)$ or $D8(D_i)$
3. Wrong, defined as $Wd(D_i)$ or $Wh(D_i)$.

A set of experiments was run with MICSS to simulate failures in information exchange and analyze the potential consequences of failures on the performance of the company. First, a Baseline Policy was built for the company. The values in the purchasing policy, marketing policy, etc… were chosen so that the company performs well. Then, information assurance failures such as Delayed information or Wrong information were introduced in the Baseline Policy to assess the consequences of low-level information assurance on the performance of the company.

The following parameters were used to simulate the information failure scenarios:

1. Information failure type,
    a. Correct
    b. Correct but delayed
    c. Wrong
2. Data item (type of data affected by information failure),
    a. D_1 = Price
    b. D_2 = QLT (Quoted Lead Time)
    c. D_3 = Batch Size
    d. D_4 = Order Level
3. Length of delay,
    a. 4 months
    b. 8 months
4. Error size (ratio between the wrong value of data item and the correct value),
    a. Double
    b. Half.

As a consequence, 17 scenarios were simulated.

For each scenario, ten runs were simulated. During a run, the functioning of the company was simulated for one year, and the performance of the company (Profits π, and Due Date Performance DDP) was recorded after each period p of two months. The detailed statistical analysis is described by Bellocci et al. (2001).

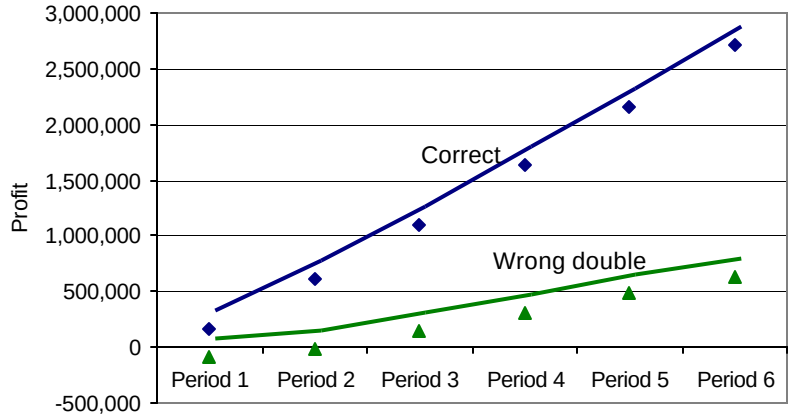
The design of experiment is presented below (Table 2). The objective of these experiments was to answer the research problem introduced in Section 1: Are there specific information failures in ERP systems that have a larger impact on the profits π and the due-date-performance DDP of a company than others?

An example of the graphs and results obtained with the MICSS lab experiments is presented in Figure 2.

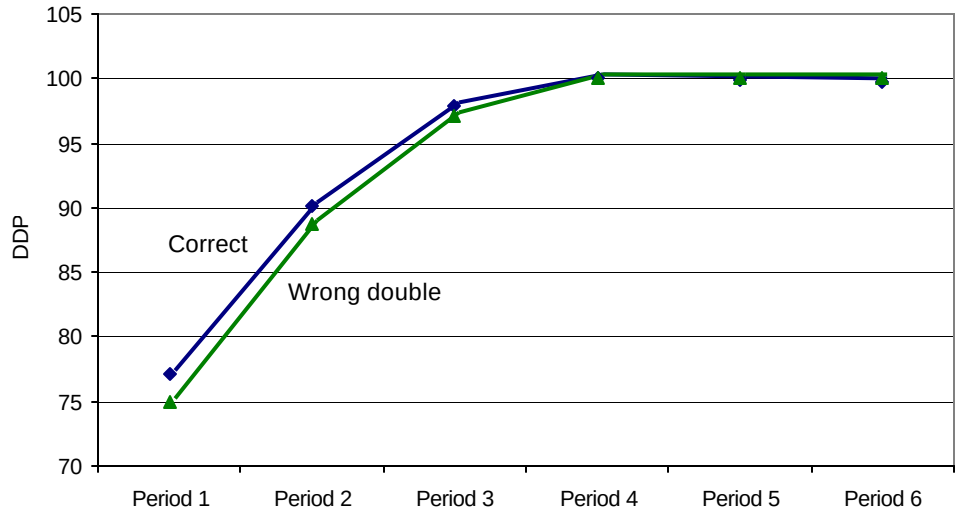
Table 2. Design of information assurance failures experiments

No.	Experiment	Independent variable	Levels	Performance Measures
1	Delayed 4 months information	Information failure type	a. BP b. D4(D_i)	a. π b. DDP
	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company between the correct policy BP and the policy D4(D_i).			
2	Delayed 8 months information	Information failure type	a. BP b. D8(D_i)	a. π b. DDP
	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company between the correct policy BP and the policy D8(D_i).			
3	Wrong half information	Information failure type	a. BP b. Wh(D_i)	a. π b. DDP

	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company between the correct policy BP and the policy $Wh(D_i)$.			
4	Wrong double information	Information failure type	a. BP b. $Wd(D_i)$	a. π b. DDP
	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company between the correct policy BP and the policy $Wd(D_i)$.			
5	Length of Delay	Length of Delay	a. $D4(D_i)$ b. $D8(D_i)$	a. π b. DDP
	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company if the correct value of data item D_i is delayed 4 months or delayed 8 months.			
6	Error Size	Error Size	a. $Wh(D_i)$ b. $Wd(D_i)$	a. π b. DDP
	Research Hypothesis: Given a data item D_i and a period of the year p_t, there is no significant difference in the performance of the company if the value of data item D_i is wrong half or wrong double.			

	Baseline policy (10 runs)					
QLT Wrong double (10 runs)	**Metric: Profit**					
	Period 1	**Period 2**	**Period 3**	**Period 4**	**Period 5**	**Period 6**
	D -	D -	D -	D -	D -	D -
						
	Metric: DDP					

	Period 1	**Period 2**	**Period 3**	**Period 4**	**Period 5**	**Period 6**
	D -	D -	D -	S	S	S



Legend:
S = similar
D = significantly different
D- = significantly different and metric's value smaller than with Baseline Policy
D+ = significantly different and metric's value bigger than with Baseline Policy

Figure 2. Wd(QLT) versus BP (for Profit and Due Date Performance)

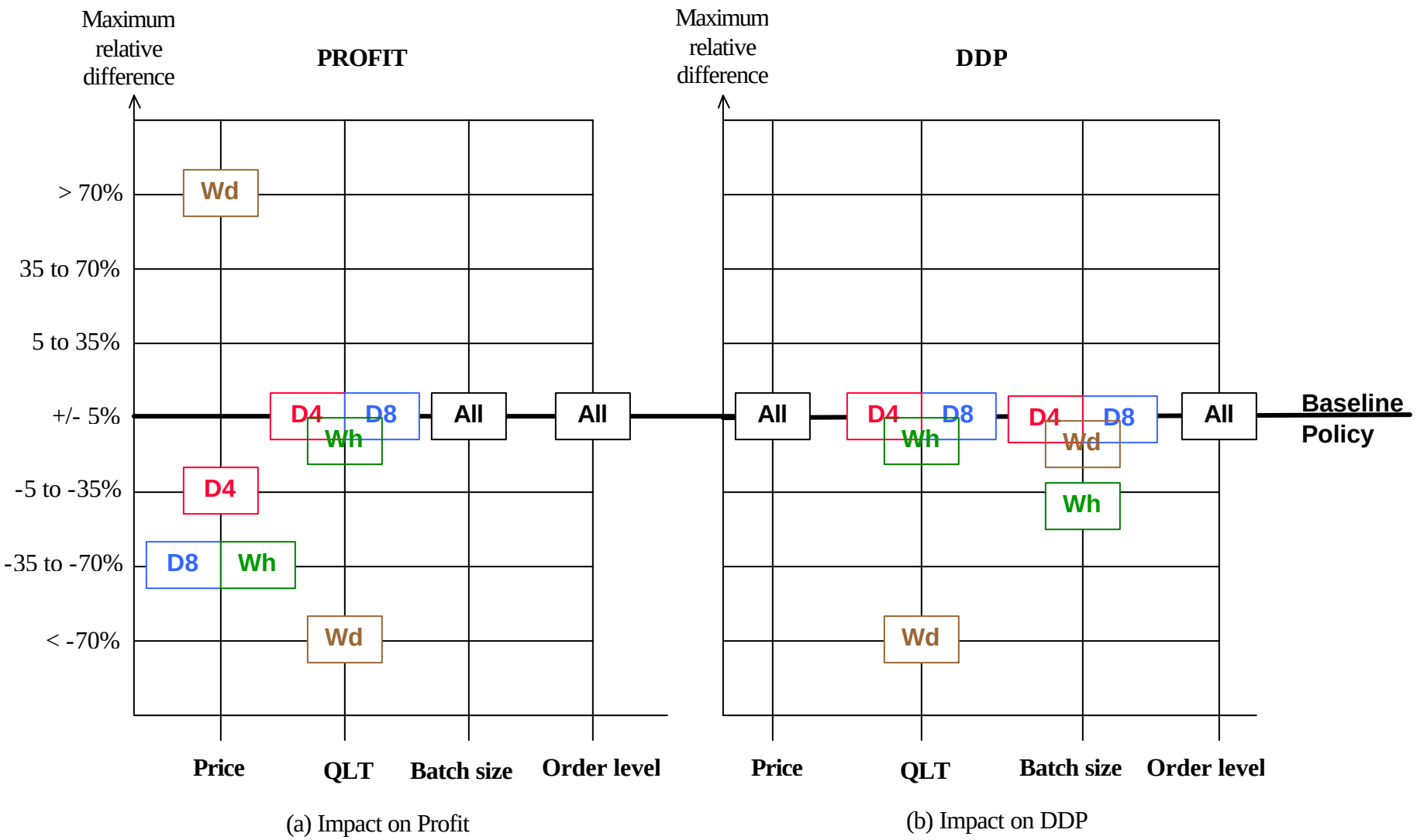
Conclusions from the lab experiments:

1) The experiments show that information failures have significant impact on the performance of a company only under specific conditions.
2) Profit is very sensitive to information failures. Due Date Performance reacts more slowly and is impacted significantly only after long lasting and large errors.
3) The impact of information failure depends greatly on the Data item that is concerned by the failure. For instance, the consequences of a problem concerning Price are usually much more serious and long lasting than when the error concerns Batch Size.
4) Data items have different characteristics that make them more sensitive to a specific type of failure. For instance, a delay of 8 months has a large impact on Profit when it concerns Price, but no real impact when it concerns Batch Size.

5) A difference in the length of delay influences the performance of the company only when Price is concerned by the error.
6) The impact of an information failure depends on the error size, except when the error concerns Order Level.
7) The impact of each type of information failure on each data item is presented in Figure 3 using the maximum relative difference to the BP's performance reached in a one-year period. The specificities of each Data item are summarized in Table 3. It appears that each Data item has strong particularities regarding the performance metrics of the company that it affects, and the type of failures that it is most affected by.

Table 3. Summary of information failures' impact on Data items

Error in Data item	Impact on	Critical Failures	Length of delay	Error size
Price	Profit	Wd (positive impact) Wh, D8, D4	Important	Important
QLT	Profit	Wd	Not important	Important
	DDP	Wd	Not important	Important
Batch Size	DDP	Wh	Not important	Important
Order Level	None	None	Not important	Not important



(a) Impact on Profit

(b) Impact on DDP

Figure 3. Impact of information failure on company's performance (based on MICSS lab experiments)

2.5. Industry survey

On the basis of the lab experiments, an industry survey was designed to assess the information assurance requirements of the corporate world. Two questionnaires were developed. One was sent to the information system manager of a given company, and the other one to the department managers of the same company (e.g., production manager, marketing manager…). The objective of the first survey questionnaire was to understand the general approach of companies regarding information security and assurance. The second survey questionnaire was designed to study the actual information assurance problems encountered by users of the company's information system.

The design and conclusions of the industry survey are presented by Ray, et al. (2001a). The questionnaires, and the detailed analysis of companies' answers are available in Ray, et al. (2001b). The questionnaires were sent to approximately 50 companies in the United States, Europe and Asia. The analysis was based on the 9 questionnaires returned by information system managers, and the 10 questionnaires returned by department managers.

Conclusions from the industry survey:

1) Companies think that information assurance failures have significant impact on their performance.
2) From the analysis of the survey, it is inferred that companies are more concerned by information significance than information security or integrity in their information systems. (Figure 4)
3) Further analysis showed that indeed Profit and Due Date Performance (the reputation of the company) are the parameters that are the most affected by information assurance failures. (Figure 5)
4) At present, System Authorizations, Firewalls and Antivirus are the most popular preventive measures that companies apply. This observation shows that companies are equipped to handle information security and integrity problems, but not yet to handle information significance problems.
5) Companies introduce flexibility in their information systems mainly using user groups having access to different resources using passwords.

6) The process of assuring the data is too time-consuming for information system users. In a decision-making process, information system users spend more time on acquiring the necessary information, and arguing about its accuracy than using the data.
7) Most companies disregard the information due to the fact that they maybe from unreliable sources or the information may be inaccurate.
8) If information is missing at the time of changing the policy in their ERP system, most of the companies can wait, but not for very long. If they have to wait for longer, they go ahead and change their strategies.
9) Users have difficulties to change processes because of consequential damages due to tight integration.

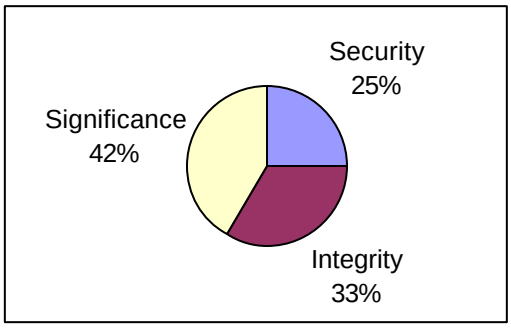


Figure 4. Sources of concern about Information Assurance
(based on 10 responses from department managers)

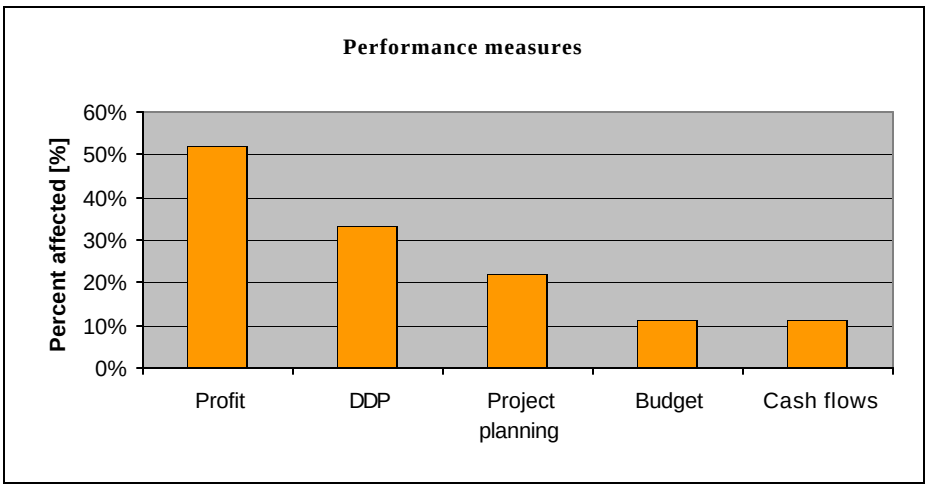


Figure 5. Performance measures most affected by information assurance failures
(based on 10 responses from department managers)

2.6. Conclusions

The conclusions of the lab experiments and industry survey were presented earlier. The general implications of these results for the research project are explained below:

1) The experiments showed differences in the impact of information failures between Data items. Thus, it is important to adjust the assurance tasks to the needs thanks to variable assurance. Each company has to investigate its own specificities to define what are the most critical information assurance failures for its activity.
2) The survey showed that companies have difficulties keeping the consistency and significance of their information. It also proved that decision-makers are willing and are able to wait to get better assured information.
3) Some examples of assurance tasks that should be automated to improve decision-making processes in a company can be formulated from the literature review, the lab experiments, and the industry survey:
   a. *Dealing with information security:*
      - access authorization
      - intrusion detection
      - virus detection
      - messages encryption
      - users and data profiles management
      - critical data monitoring and history recording
   b. *Dealing with information integrity:*
      - regular back-ups
      - data decay prevention
      - communication links quality monitoring
      - communications success monitoring (termination + mapping)
      - data safety when system crashes
      - secure restarting after system crashes
   c. *Dealing with information significance:*
      - believability check (the data stored is not obviously wrong)
      - completeness check (all of the needed characteristics of a data are stored)

- accuracy check (the value of the data is given with the required accuracy level)
- source trustworthiness (where does the data comes from?)
- timeliness (the data must be ready when needed)
- representation (the data must be displayed using the correct representation)

3. SUMMARY AND CONCLUSIONS

A broader definition of information assurance was introduced to include the data quality considerations necessary for the functioning of inter-networked enterprises. A list of information assurance requirements was developed based on literature review, lab experiments, and an industry survey. This list serves as a guideline for the design of information assurance systems, to make sure that the system meets the requirements. The lab experiments showed the large variability in the impact of information failures, depending on the failure type and the data item concerned by the failure. As a consequence, variable information assurance should be introduced in information systems. The industry survey demonstrated that information significance is the true concern of information systems users in inter-networked companies. It also helped developing a list of examples of assurance tasks that should be automated in distributed information systems. The next step of this research work is to design and evaluate agent models and variable assurance protocols to automate these assurance tasks.

4. ACKNOWLEDGEMENTS

This research was supported by the CERIAS (Center for Education and Research in Information Assurance and Security) at Purdue University.

REFERENCES

Bellocci, T., Ray, P., and Nof, S.Y., Information Assurance in Networked Enterprises: MICSS Lab Experiments, Results and Analysis, *CERIAS Technical Report 2001-35, Research Memorandum No. 01-06, School of Industrial Engineering, Purdue University,* January 2001.

Dobry, R., and Schanken, M., Security Concerns for Distributed Systems, *Annual Computer Security Applications Conference*, 1994, 12-20.

Finne, T., What are the Information Security Risks in Decision Support Systems and Data Warehousing, *Computers & Security*, v 16, n 3, 1997, 197-204.

Jelen, G., and Williams, J., A Practical Approach to Measuring Assurance, *14th Annual Computer Security Applications Conference*, Phoenix, AZ, Dec 1998.

King, C., Intranet Applications Security Checklist, *Computer Security Journal*, v 13, n 1, 1997, 47-54.

Longley, D., and Shain, M., Data & Computer Security – Dictionary of Standards Concepts and Terms, *Stockton Press*, 1986.

MICSS (Management Interactive Case Study Simulator) [http://www.mbe-simulations.com, June 2001].

Pfleeger, S.L., A Framework for Security Requirements, *Computers & Security*, v 10, 1991, 515-523.

Ray, P., Bellocci, T., and Nof, S.Y., Information Assurance in Networked Enterprises: MICSS Class Experiments and Industry Survey Conclusions, *CERIAS Technical Report 2001-37, Research Memorandum No. 01-08, School of Industrial Engineering Purdue University,* June 2001a.

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 Memorandum No. 01-09, School of Industrial Engineering Purdue University,* June 2001b.

Schwartz, A.P., and Zalewski, M.A., Assuring Data Security Integrity at Ford Motor Company, *Information Systems Security*, 1999, 18-26.

Shirey, R., Security Requirements for Network Management Data, *Computer Standards & Interfaces,* v 17 n 4, September 1995, 321-331.

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

Voas, J., Protecting Against What? The Achilles Heel of Information Assurance, *IEEE Software*, January 1999, 28-29.

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