# A MODEL AND IMPLEMENTATION GUIDELINES FOR INFORMATION SECURITY STRATEGIES IN WEB ENVIRONMENTS

C. MARGARITIS[1], N. KOLOKOTRONIS[1], P. PAPADOPOULOU[1], P. KANELLIS[2], D. MARTAKOS[1]

*[1]h_margar@cc.uoa.gr, {nkolok,peggy,martakos@di.uoa.gr}*
*Department of Informatics and Telecommunications,*
*National and Kapodistrian University of Athens,*
*University Campus, 157 71 Athens, Greece*
*Tel: +3017275225*
*Fax: +3017275214*
*[2]panagiotis.kanellis@gr. arthurandersen. com*
*Arthur Andersen*
*Syngrou Ave. 377, 175 64 Athens, Greece*
*Tel: +3019470275*
*Fax: +3019425681*

Keywords: Information Security Strategy, Security Semantics, Web, Systems Development

Abstract: The decentralised nature of web-based information systems demands a careful evaluation of the pantheon of security issues in order to avoid the potential occurrence of business risks that could not be easily mitigated. Understanding that information security is not merely a technical solution implemented at each one of the endpoints of the inter-organizational application, this paper presents an integrated approach based on a rigorous multi-level and multi-dimensional model. Through synthesis and aiming to contribute towards implementing the most effective security strategy possible, the approach has as a starting point the overall business goals and objectives. Based on those it aids the development of a strategy from the lower levels of securing data in storage and transition to the higher levels of business processes. Its use and applicability is demonstrated over 'Billing Mall' – a system for Electronic Bill Presentment and Payment.

# 1. INTRODUCTION

As organisations are rushing to revamp business models and align operations around e-commerce initiatives, information systems (IS) play a central role in the definition of the new value adding activities. It is without doubt that in the very near future, the largest percentage of a commercial activity will be taking place in a virtual world. Wanninger *et al*. (1 997) and Papadopoulou *et al*. (2000) emphasised that such systems must be thought of as 'servicescapes' – enablers of a virtual realm where products and services exist as digital information and can be delivered through information-based channels.

The achievement of strategic goals such as increasing market share, are directly related to the reliability of the technological infrastructure of organisations. It follows that the occurrence of business risks is now more eminent as the corporate network, processes, and critical business data are vulnerable to attacks by anyone having Internet access (Abela and Sacconaghi, 1997; Derivion Corp., 1999; Segev *et al*., 1998; Walker and Cavanaugh, 1998). What it has been observed however is that most organisations treat the Internet simply as a transport medium. The result as Segev *et al*. (1998) noted is that "...Internet security remains a relatively technical, local and distinct issue from the corporate level [IS] design and management". We advocate that, as security is the dependent variable for the success of web-based IS, the formation of any information security strategy should begin by taking into account the business vision, goals and objectives. Furthermore, it should not be approached as an afterthought, but rather it has to be designed and evolve concurrently with the development of the system, Any other way to approach this issue could result to a badly designed IS where purposive failure "...quickly leads to massive fraud, system failure, and acrimonious lawsuits" (Hughes, 1997). In summary, the definition of any effective information security strategy should thus be a well planned and concentrated effort initiated at the corporate level, and not be seen only as a local technology issue, or as an ad hoc mix of particular technical solutions to specific problems.

Taking into consideration the above issues, this paper offers an integrated approach to the development and implementation of an information security strategy for IS operating in web environments. Based on a comprehensive multi-level and multi-dimensional model, it defines the issues and sets the guidelines for infusing security both at a low and higher level. The section that follows presents the model and its building blocks for aiding the implementation of an effective security strategy. Its application is demonstrated in section 3 over a web-based Electronic Bill Presentment and Payment (EBPP) system developed for the Hellenic Telecommunications

Organisation (OTE), and currently in its deployment phase. A concluding discussion closes the article.

## 2. AN INFORMATION SECURITY STRATEGY MODEL

The use of security models and frameworks has been very much of a specialty area. The assumption that security is largely a technological issue and an afterthought that has to be addressed during a system's implementation phase, may explain the fact that relevant works are absent from the IS literature. However, as Baskerville (1993) notes "...a developmental duality of information systems security exists, that results because the information system and its security are treated as separate developments. This duality may cause conflict and tension between a system and its security". The model that is presented in this article was developed taking the above issue under consideration. It acquired an added importance as it was developed during our attempt to define an information security strategy for 'Billing Mall' – a system for on-line bill presentment and payment whose intended users range from corporate customers to households. Taking into account that the majority of current and potential Internet users are alert to the security issue through media over-exposure, it was clearly understood that security was a dependent variable for the level of adoption, and subsequently the future success of the system. The model which is depicted in figure 1, portrays a cyclic iterative process for designing and deploying an information security strategy depicting the different stages and successive steps that have to be taken. The stages identified, namely business needs analysis, risk analysis, security strategy implementation, and monitoring, research & analysis, are described in the rest of this section.

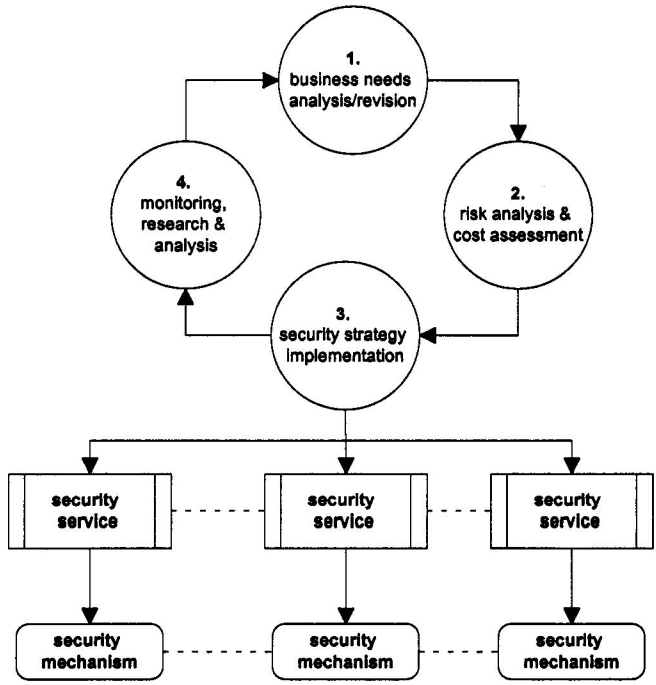


*Figure I: The life cycle of a system's security strategy*

## 2.1 Business Needs Analysis

As already mentioned, security should be examined as an integral part of the overall strategic plan. Thus, any approach to security should start with an analysis of the business needs in order to provide a solid foundation for setting a strategy. Business Needs Analysis is the task of creating and maintaining an IS strategy that correctly reflects the overall mission and goals of the organisation. Understanding business objectives and organizational as well as inter-organizational requirements is fundamental for identifying the security requirements for a web-based IS. Since such a system may surpass the organisation's boundaries and extend across multiple organizational entities (Yang and Papazoglou, 2000), a deep understanding of business goals at strategic level is deemed necessary to enable a clear estimation of the demanded security. Some techniques that can be used for performing this task are Critical Success Factors (CSF) analysis and Strengths-Weaknesses-Opportunity-Threats (SWOT) analysis.

## 2.2 Risk Analysis and Cost Assessment

Since the information owned by an organisation is of critical importance, the information resources that are to be protected in terms of their value to the business goals, together with their owners and physical location should be identified. In addition, it has to be specified from whom the previously defined organizational assets should be protected from. All these issues have to be considered in conjunction with the cost of deploying the security strategy. Cost assessment will also ensure the provision of management support, an essential part for developing the strategy and a prerequisite for its future application success (Segev *et al*., 1998). The distributed nature of web-based systems implies the existence of a multitude of vulnerabilities and threats which have to be thoroughly examined to guarantee a secure environment for commercial transactions. Potential risks should be identified at all levels of the corporate IS, including vulnerabilities and threats associated with network services, architecture, operating systems and applications.

Amongst others, typical business risks include the theft and alteration of data, unauthorised access to sensitive information, inability to meet customer needs quickly and the loss of business. Hence, the purpose of risk analysis is to facilitate decision-making about the desired level of security as well as the methods that should be adopted for preventing risks. Risk analysis can be used before the deployment of an IS to define in advance the acceptable level of risk that may be associated with it. A similar process can then be followed after deployment to re-evaluate the level of risk according to 'live' operating conditions. The difference between the acceptable risk level and the current risk level is then used as an evaluation metric. The results of the new risk analysis process can then be utilised to identify areas that require additional attention.

Risk quantification should be undertaken including a cost assessment of the possible damage associated with each threat against the cost of preventing the threat in terms of time, expenses and resources. The identified risks should then be categorised according to their probability and the severity of their impacts (see figure 2), and prioritised with respect to the cost needed for their elimination. Certainly one needs to consider first those threats resulting in greater losses (classes D and C), but still not to ignore threats of less probable financial impact, occurring more frequently (class B). Following the above steps, a complete analysis of risks is produced that can be used proactively to mitigate the number of potential threats compromising the security of an organisation's web-based IS.

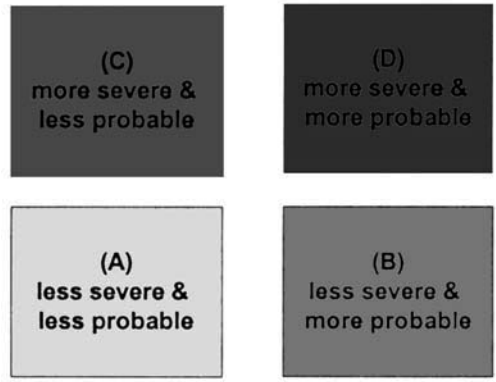


*Figure 2: Risk classification*

## 2.3 Security Strategy Implementation

When risk analysis is completed, the next step is to implement the organisation's information security strategy. The strategy should aim to ensure the most effective use of resources, and will, where appropriate constitute a consistent approach to security across a range of different systems. How the strategy is to be implemented should be described in detail in a Corporate Information Security Policy (CISP) document. Strategic objectives should be outlined. These are general security objectives, which may be defined, for instance, in terms of the levels of confidentiality, integrity, availability and accountability that the enterprise wishes to attain. The creation of the CISP is thus based upon the process of risk analysis conducted during the previous step.

### 2.3.1 Identifying Security Services

Undoubtedly, this is the most difficult part of the security strategy development plan, since this step involves the identification of the security services needed to be offered in order to protect the organisation's information assets from known and unknown threats (see figure 1). Not all security services are used for the protection of all kinds of information resources, since different classes of data require different levels of security. Classes of security services include integrity, confidentiality, authentication, accountability and auditing, authorisation, availability, and non-repudiation. In order to provide these security services to a web-based IS, we have to consider (a) the security mechanisms offered for data in transit, and (b) the security mechanisms offered for data in storage. These are illustrated in tables 1 and 2 respectively.

When data in transit is considered (table 1), protocols offering security services are divided into three main categories depending on the International Standards Organisation's (www.iso.ch) Open Systems Interconnection (OSI) layer they operate, namely the network, transport and the application layer. Furthermore, the application layer security mechanisms can be subdivided according to the specific structure and nature of the data they are targeting, differentiating sensitive (financial) from non-sensitive data.

*Table 1: Mechanisms used to enforce the security policy for data in transit*

| Layer | Protection | Mechanism |
|---|---|---|
| network/ Internet | host-to-host | IP Security (IPSEC), IP Authentication header (AH), IP encapsulating security payload (ESP), network layer security protocol (NLSP), point-to-point tunnelling protocol (PPTP) |
| transport/ session | process-to-process | secure sockets layer (SSL), transport layer security (TLS), open financial exchange (OFX) |
| application | data structure-specific | secure hypertext transfer protocol (S-HTTP), pretty good privacy (PGP), privacy enhanced mail (PEM), secure multipurpose Internet mail extensions (S/MIME) |
| | data nature-specific | secure electronic transactions (SET), open financial exchange (OFX) |

In general, it is easier to protect corporate assets from third parties outside the corporate network, than from its employees who intentionally or accidentally may cause severe security incidents. Thus, it is of crucial importance to ensure that everyone inside the corporate network complies with the corporate security strategy guidelines. This means that security for data in storage does not only depend on the technology used, but also on the proper administration of systems, as well as the observance of related business procedures, physical access controls, and audit functions. Not all business requirements and objectives are identical. Consequently, security mechanisms for data in storage are not absolute - there is not one standard that will fit all businesses and industries. In table 2, we present the dominant mechanisms (hardware/software based) currently available for safeguarding critical data in storage within the organisation.

*Table 2: Mechanisms used to enforce the security policy for data in storage*

| Type | | Solutions |
|---|---|---|
| hardware | | smart cards (PVC, EMV), other tamper-proof devices, screening routers, biometric devices |
| software | operating system level | password-based authentication, password expiration and filtering, Kerberos-based distributed authentication, access control lists (ACL), security identifiers (SID) |
| | database management system level | password expiration, password standards enforcement, break-in detection and evasion, dormant user ID identification, centralised security administration, comprehensive report generation, maintenance of audit logs |
| | application level | anti-virus software, audit log analysers, firewalls, backup utilities |

### 2.3.2 Defining Security Requirements at Business Process Level

Our discussion thus far has focused on the implementation of a security strategy mainly at the lower infrastructure level. We agree with Baskerville (1993) that a security strategy should evolve concurrently with the design of the system and not be approached as an afterthought. As such, any integrated approach should address how security could be possibly implemented at a higher level, i.e. the business process level. IS that support business transactions are developed based upon well-defined business process models. A business process is defined by an executive or middle manager – usually with the help of an outside consultant - and contains the following components: information flows between organizational units involved (e.g. business units, departments, agents, etc.), tasks to be performed, information sources and their usage and structure, and behaviour of all the components involved.

In order to arrive at a complete understanding of the security requirements at the business process level, Röhm *et al.* (1998) suggested examining a business transaction from at least five different perspectives/views, each one extended accordingly in order to capture the security semantics:

- The *business process view* representing the flow of work in terms of activities and participating entities from the viewpoint of the whole business process. It is used both as a means to communicate the

architecture of the system to the stakeholders and to guide the modelling efforts for the other four viewss.

- The *informational view* representing the information entities, their structure and any relationships between them.
- The *behavioural view* showing what tasks and activities are associated with the various objects, the events that trigger these activities and the message exchanging that occurs between them.
- The *dynamic view* representing for each information entity all possible states and any transitions that may occur within the life cycle of the information entity.
- The *structural view* showing where and by whom tasks and activities are performed.

The above can guide the analyst towards acquiring a holistic view of any business process – from the highest to the lowest level. We adopt those views – placing them within the 'security strategy implementation' stage of our model and defining a hierarchy and thus the order with which they must be performed. Their practical application is demonstrated in the next section of the paper.

Most existing research in the engineering of secure information systems has used formal methods in the context of a conventional process model (Boehm, 1988). In general, a waterfall process works well for systems where requirements and design issues are well understood from the outset (Kemmerer; 1990). In the past many security critical systems exhibited these characteristics. In these environments, conventional formal methods were generally adequate. However, they are much less useful in an environment where security and other design goals may be in conflict (Baskerville, 1993). Pressures to compete against smaller or more flexible firms in global marketplaces are mounting. In response, organisations are attempting to achieve new forms that foster rapid adaptation to change. These competitive trends are forcing organisations to develop new forms of IS that are more open and adaptable to changes.

In such an environment, a multi-dimensional approach integrating security semantics with business transaction models offers significant advantages such as the following:

- The security ramifications of different design alternatives can be explored before the decision is made to commit to any single one.

- Basic verification strategy can be laid out early in the process in order to avoid the unpleasant possibility that a workable design is impossible to verify.
- Decisions to bypass security in order to meet other goals are made consciously early in the process, avoiding thus the possibility to be discovered as a result of a security incident much later.

## 2.4 Monitoring, Research and Analysis

The monitoring, research and analysis step of our model can be performed using both internal and/or external auditors. A plethora of solutions that are available widely by software vendors, such as audit log analysers and intrusion detection mechanisms can provide valuable information regarding potential implementation flaws. Their value rests on the provision of information to the administrators about the status of the systems. This information indicates possible weaknesses of the currently deployed security strategy, and may in turn constitute the starting point for radical changes in the organisation's strategic security plans and needs.

In this section we provided a comprehensive model for aiding the definition and deployment of an information security strategy from a multi-level and multi-dimensional perspective. What follows is a description of how this model was used to define and implement the security strategy of 'Billing Mall' – an EBPP system developed for the Hellenic Telecommunications Organisation (OTE).

# 3. INFORMATION SECURITY STRATEGY IMPLEMENTATION

The initial response of the market to various commercial applications regarding EBPP systems is indicative of their future potential in becoming contenders for a permanent place in the worldwide Internet infrastructure. According to industry analysis, within 3-5 years the majority of bills will be presented and paid electronically (Just in Time Solutions Corp., 1999). In the United States alone it is projected that by taking the 'paper' out of the billing process, EBPP could save billers, customers and other constituents over $2 billion annually by 2002 (Ouren *et al*., 1998). 'Billing Mall' (http://alexandra.di.uoa.gr) is such a system, offering facilities for bill presentment and payment, customer application processing and personalised marketing (see figure 3). The system provides electronic delivery of bills to customers through the presentment of bill information in both summarised and detailed form, and secure electronic payment of a single or multiple bills

upon customer request. Customer Application Processing (CAP) provides the means to customers who wish to order a new product or service that are available by OTE to do so. Finally, Personalised Marketing (PM) offers the necessary functionality and support needed for the effective promotion of products and services based on a customer's identified needs and characteristics.

The architectural model of the system is based on the Open Internet Billing (OIB) (Just in Time, 1999) model. According to OIB, a central service provider, the Consolidator, collects and stores electronic summary bills from registered billers. While offering a single point of access for viewing and paying bills, it provides the customer with the option to have access to the biller's web site for detailed bill information. When the customer visits the web site requesting to see a detailed bill, the Biller presents him with informative messages regarding products and services available. The customer is also provided with a facility for placing orders for the advertised products and/or services.

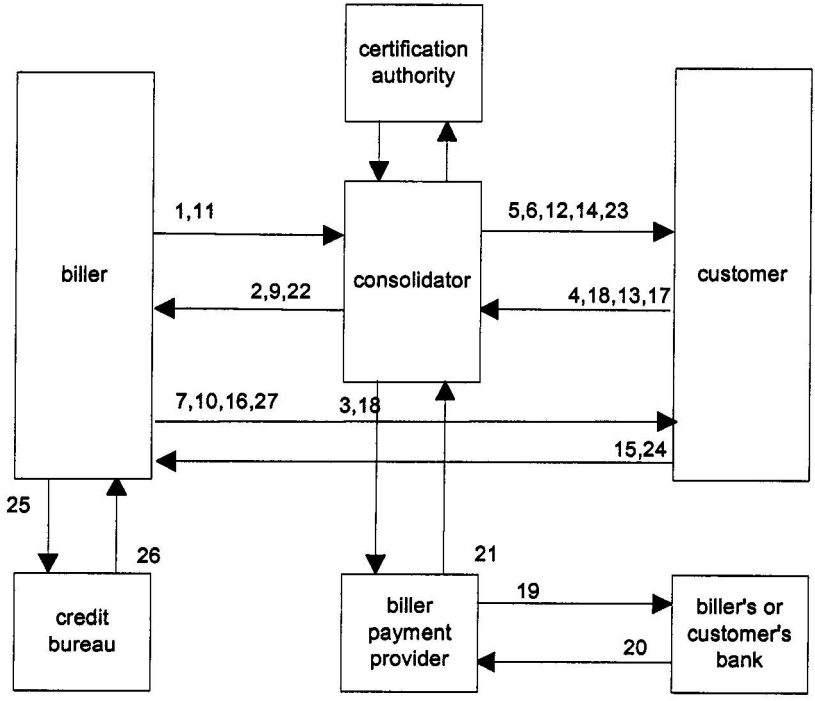


*Figure 3: The 'Billing Mall' Internet Bill Presentment and Payment System*

*1*. Biller enrols to consolidator to offer services, *2*. Biller's certificate from Certification Authority (CA), *3*. Biller Payment Provider (BPP) receives certificate from CA, *4*. Customer

enrols to consolidator and selects billers, *5.* Customer's certificate from CA and login account, *6.* Announcement of new biller participating in EBPP service, *7.* New biller providing EBPP service, *8.* Request for receiving and paying bills from the new biller, *9.* Request for including the new biller in EBPP service is forwarded to biller, *10.* Notification of EBPP service becoming active for customer, *11.* Bill summary is made available to consolidator, *12.* Notification of a new bill made available for viewing and paying, *13.* Customer logs in, *14.* Bill summary is accessed by customer, *15.* Request for accessing detailed bill information, *16.* Detailed bill information and personalised marketing, *17.* Customer initiates bill payment, *18.* Payment request is forwarded to BPP, *19.* Payment execution is originated, *20.* Payment execution is completed, *21.* Notification for completion of payment, *22.* Notification for bill payment execution and remittance information, *23.* Notification for successful execution of bill payment, *24.* Order submission for biller's products and/or services, *25.* Request for information about risk of crediting customer for purchase of ordered products and services, *26.* Information about credit risk associated with customer, *27.* Notification about acceptance or rejection of submitted order.

An evaluation of the critical factors for the successful deployment and consequent adoption of the system imposed the need for the parallel development of a comprehensive security strategy. Aiming to guarantee an integrated approach to the multilateral issue of security, the model described in the previous section has served as the basis for the design and implementation of the security strategy.

Following the stages prescribed by the model, a business needs analysis has been conducted first, providing the foundation for the strategy. In this context, business goals were clearly defined, indicating the need for a system guaranteeing secure electronic transactions associated with all types of offered services. A rigorous examination of this issue denoted the security requirements that had to be satisfied in order for the system to be trusted and adopted by the intended customer base. To this end, the resources that were to be protected were identified at both organizational and inter-organizational levels, in terms of the information stored, the applications and the hardware used and the underlying network infrastructure. These corporate assets were deemed necessary to be protected from internal as well as external attacks, either intentional or accidental. Finally, in order to mitigate the cost of deploying a secure communication mechanism for financial transactions between the Consolidator and the Banks, it was decided that the existing infrastructure currently in use for fund transfer between financial institutions in Greece should be leveraged. This implied the need for including an additional entity to the OIB model, the Biller Payment Provider (see figure 3), serving as an intermediary between the Consolidator and the Banks.

The next step towards the implementation of the security strategy was to conduct a risk analysis as a proactive diagnosis of the vulnerabilities and threats that could possibly hinder the proper operation of the system. A number of entity-centric and cross-organizational risks were identified. The

results of this process suggested that the potential vulnerabilities and threats should be effectively addressed by carefully selecting and applying risk prevention, detection and response methods. The analysis of revealed that the OIB model was not adequate to provide the anticipated level of security and reliability that is essential for the networked business processes. Thus, it was decided that it had to be extended in order to accommodate the establishment of a Certification Authority (CA) issuing and disseminating digital certificates to the customers (see figure 3). Furthermore, as a means for addressing the risk of insolvent customers, issuing payment transactions that could not be completed due to insufficient credit, a Credit Bureau entity was added to the architectural model of the system (see figure 3). The functional role of this entity is the provision of information related to the credit status of customers, eliminating the possibility of financial damage.

Since 'Billing Mall' requires the exchange of large amounts of financial information, the first task was to evaluate the security features of existing protocols in the field. Between Open Financial Exchange (OFX) (www.ofx.net) and Secure Electronic Transaction (SET) (www.setco.org), the former was found more appropriate mainly because (a) it is based on cryptographic protocols, (b) it supports the use of channel-level as well as application-level security, and (c) its security architecture is expandable and customisable. The SSL protocol met the requirements defined by the deliverables of the first two steps of the framework for ensuring the confidentiality and the integrity of data in transit. However, some constrains had to be put into practice concerning the cryptographic algorithms used, as well as the size of the session key. In contradiction to the OFX specification (Checkfree Corp., 1998), both server and client side certificate-based authentication is required by Billing Mall at channel-level security in order to eliminate security risks. Thus, password encryption is not required as the specification dictates for authenticating the user, who is provided with the additional capability of encrypting vital information inside the OFX message, such as credit card number and/or bank account data, with the OFX server's public key.

For this reason only one entity, satisfying the requirements imposed by the European Community's 1999/93/EC directive was decided to play the role of the certification authority. The certificates issued by the CA are based on the PKCS #6 extended-certificate syntax standard (RSA Data Security, 1993a), because of its flexibility in defining new PKCS #9 selected attribute types (RSA Data Security, 1993b) and its compatibility with applications requiring the use of X.509 certificates. In order to facilitate certificate and key management, from the customer's point of view, smart card technology was decided to be a basic part of the overall design. As far as 'Billing Mall' is concerned, a defensive policy is enforced regarding the amount for which

an issued certificate can be used. This limit, which is interpreted as the amount that the user is willing to risk per transaction, is determined by the user and may be accepted or rejected by the CA and the Credit Bureau.

Firewalls, as expected, are the first line of defence for all entities (this does not include the Customer) participating in the 'Billing Mall' system. It is suggested that important information should only be accepted from and delivered to servers with a specific IP address, which means that any network package sent by an unknown IP address is automatically rejected. Example procedures taking advantage of this feature are that (a) the Consolidator only accepts bill summary information from a small set of IP addresses in the Biller's domain, and (b) the Consolidator only forwards Customer's payment requests to the specific BPP IP address. This technique allows some degree of resistance against attacks such as the 'denial of service' attack and IP spoofing.

Our aim during the design of the 'Billing Mall' was that the objectives of the information security strategy had to be integrated in the development process. Röhm *et al.* (1998) suggests that in order for this to be achieved, a business transaction must be viewed from multiple perspectives with each view extended by the security semantics of the information security strategy. In the following section we present an example of analysing the different views of the 'BILL-PAYMENT-ORDER' business process (step 17 in figure 3) and its security requirement 'non-repudiation'. In the example we use the following notation: components of existing model or attributes, which are not affected by security requirements, are described using normal text. The attributes with relevance to non-repudiation are given in bold face.

## 3.1 Business Process View

In electronic business transactions a document has to be signed digitally as required by the European Community's 1999/93EC Directive. A digital signature 'seals' the data to be transmitted and is created by the private key of the signatory using asymmetric cryptography. In order to study what effects a digital signature has, we will first refer to the business process view in our example. Business process modelling is typically performed in order to capture the commercially important activities. This can often lead to design conflicts once the security requirements are taken into account. In order to eliminate this tension, the supporting entities and activities that are necessary to realise the system function the way it is envisioned initially, need to be captured as well. Furthermore, since the business process view is used to guide the modelling efforts from many angles, the security semantics of the business transactions are captured in a consistent and integrated manner.

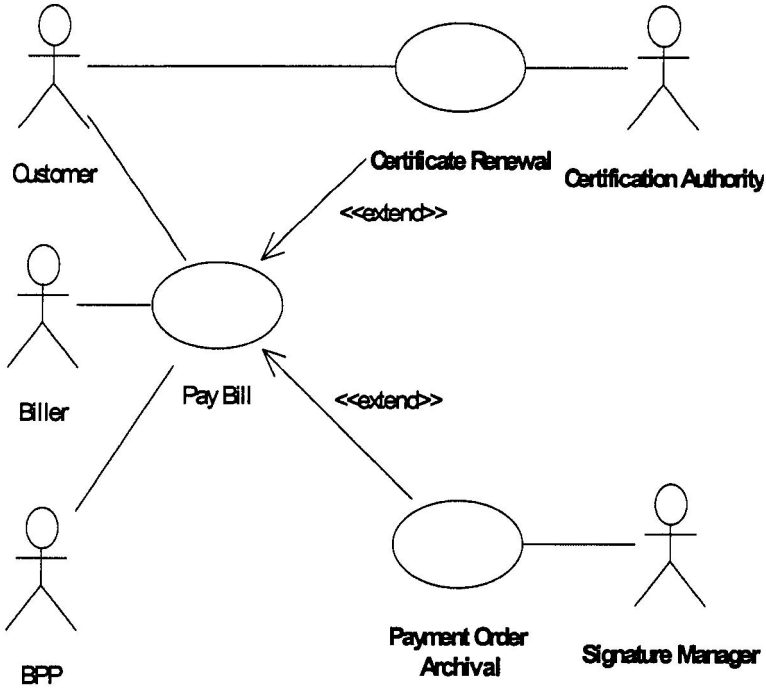


*Figure 4. Business Process View extended by security semantics*

Figures 4 and 5 depict graphically the 'BILL-PAYMENT-ORDER' process using Unified Modelling Language (UML) use case and activity diagrams. The use case diagram in figure 4 depicts the scenarios and actors involved in the business process of our example, while figure 5 shows the activities performed in completing the PayBill use case. In order to meet the "non-repudiation" requirement, our model has been extended by the appropriate actors (Certification Authority, Signature Manager), use cases (Certificate Renewal, Payment Order Archival) and activities (Verify Digital Signature, Verify Certificate Validity).

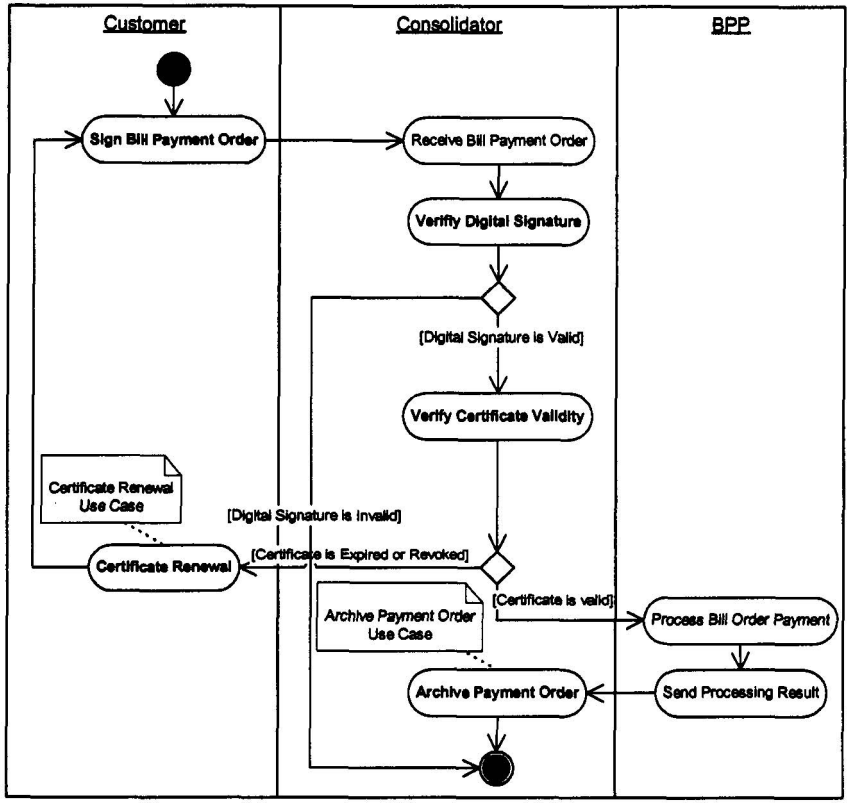


*Figure 5. Activity diagram illustrating security semantics of PayBill*

## 3.2 Informational View

According to the European Community's 1999/93/EC directive in order to sign an electronic document the 'seal' or digital signature of each signatory and the corresponding certificates are necessary. Accordingly, to effectively carry out the BILL-PAYMENT-ORDER process and to establish non-repudiation, the informational view of the transaction has to be extended by information about the signatories, the certificates used, and the trusted parties (CA) responsible for issuing the certificates. The analysis and modelling can be performed using UML class diagrams. In figure 6 we have extended the class diagram containing the customer-biller relationship of our example by appropriate classes and member fields necessary for supporting non-repudiation. These are:

- a new class CERTIFICATION AUTHORITY
- a new association class CERTIFICATE

- modification of the existing COMMITAL class by adding the appropriate fields for the digital signatures, and information about what algorithms were used for signing. The COMMITAL class is used to model any kind of document that should be signed by a customer (bill payment order), a biller (bill statement) or both (service level agreement).

In addition, customer and biller are specializations of a generic type signer, which must have a certificate relating the signer to a certification authority.

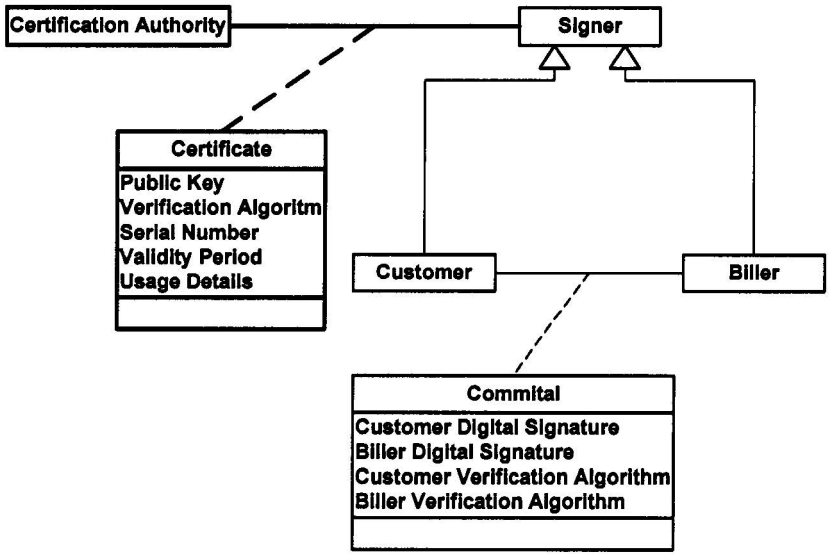


*Figure 6. Informational View extended by security semantics*

## 3.3 Behavioural View

The interactions and corresponding information flows between the entities involved in the BILL-PAYMENT-ORDER process can be analysed through the behavioural view. For the modelling of this view, UML sequence diagrams can be used. In order to assure non-repudiation, the behavioural view of the process must be modified as depicted in figure 7. The customer must digitally sign the bill payment order and the signature must be verified. In addition, because the certificate of a public key may have expired, further actions are necessary to guarantee the provability of digitally signed documents. These actions lead, for example, to extensions of the behavioural view of an object class (Verifier) responsible for validating the integrity and provability of the payment order. Again, in figure 7

necessary extensions due to security requirements are given in bold face (the sequence diagram has been enhanced by the use of scripts for accommodating complex scenarios involving conditions and iterations).

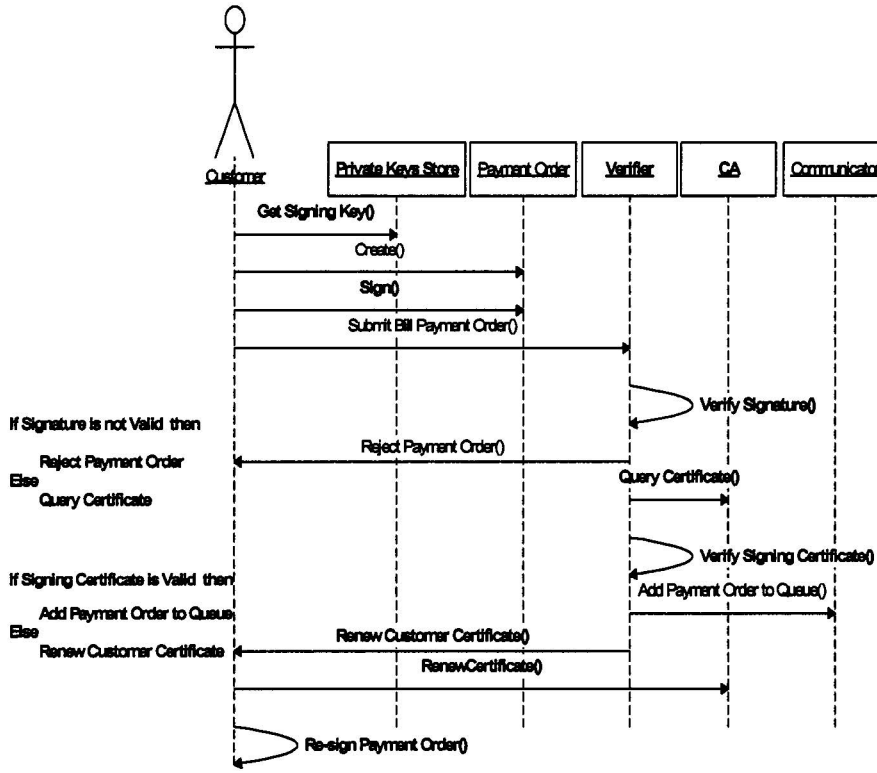


*Figure 7. Behavioural View extended by security semantics*

## 3.4 Dynamic View

The process of executing a bill payment order and establishing non-repudiation raises a number of security issues emanating from state transitions various entities undergo. These can be highlighted via an analysis and modelling of the dynamic view. In figure 8 we show the life cycle of the BILL-PAYMENT-ORDER in terms of the participating entities and their different states, using a UML state-chart diagram. As Röhm *et al.* (1998) have emphasised in a similar example, the state 'valid' is important security-wise as it represents an object of type bill payment order, which although signed, the certificate of the signatory is expired or is revoked. In this case it becomes clear that as the payment order must be re-signed.

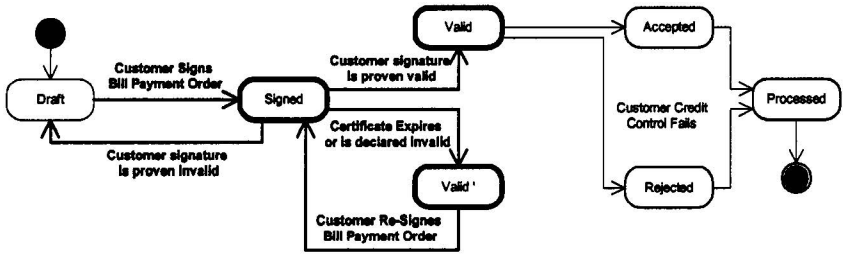


*Figure 8. Dynamic View extended by security semantics*

## 3.5 Structural View

As expected, 'non-repudiation' affects the structural view as well. Meeting critical security requirements may result in the creation and introduction of new roles with specific responsibilities. Organizational charts may need to be modified in order to mirror the new structures. In this example, a new role (Signature Manager) can be created for an employee whose main responsibility will be to check the validity of archived digital signatures, re-sign documents with certificates that are no longer valid, and monitor in general all activities in this context. Additional roles may be needed for key management (figure 9).

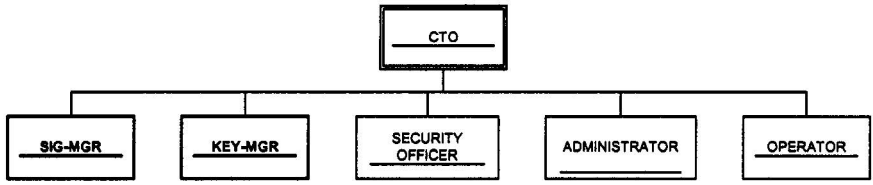


*Figure 9. Structural View extended by security semantics*

Using the five views for analysing and modelling the security semantics of business processes as proposed initially by Röhm *et al.* (1998), the preceding sections offer a summarised view of a single process and the security requirements that had to be infused and performed by the 'Billing Mall'. It becomes clear that by modelling and analysing the security semantics of the business transactions it supports, the IS and its security are not treated as separate developments. As the former becomes part of the design process, the possible duality as a cause for conflict (Baskerville, 1993) is eliminated.

# 4. CONCLUSIONS

In this article we presented an integrated approach for the development of an information security strategy based on a rigorous multi-level and multi-dimensional model. The position that any security strategy must evolve concurrently with the design of the system and not be approached as an afterthought is reflected in the model, which (a) monitors closely the development phases of an IS, and (b) addresses security at the business process level. Enabling the practitioner to evaluate and use the available security tools and techniques in a consistent manner, the structure of the model enforces the view that any security strategy must be conducted primarily at a higher level, and not be seen merely as a local technology issue. Without doubt we believe that the approach presented herein could be further refined and enhanced. We hope that its further adoption will result to any necessary enhancements or modifications, incrementing thus its value regarding its practical applicability. 'Waterproof' security of large inter-organizational systems is an issue of immense complexity, but we believe that we have at least made a few but necessary steps towards meeting this challenge.

# ACKNOWLEDGEMENTS

We gratefully acknowledge the *Greek Secretariat for Research and Technology (GSRT)* for financing the 'Billing Mall' project. We would also like to thank the partners involved in the project: Athens University of Economics and Business, Cyberce, Datamedia, Dias, Sysware, Teiresias and the University of Crete.

# REFERENCES

ABELA, A and J.R SACCONAGHI (1997). Value exchange: The secret of building customer relationships on line. *The McKinsey Quarterly* , 2, 216 –219.

BASKERVILLE, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computing Surveys,* 25(4), 375-414

BOEHM, B. (1988), A Spiral Model of Software Development, *IEEE Computer,* May, pp 61-72.

CHECKFREE Corp., INTUIT Inc. and MICROSOFT Corp. (1998) *Open Financial Exchange.* Specification 1.5.1.

DERIVION Corp. (1999). Internet Billing and the Mid-Tier Biller: Enjoying the Benefits of Electronic Bill Presentment and Payment without Operational Compromise. Available at http://www.derivion.com/index 9.html

HUGHES, E. (1997). A long-term perspective on electronic commerce. *Networker,* Nov/Dec, 38 –50.

JUST IN TIME SOLUTIONS Corp. (1999). The Value of Internet Billing. Available at http://www.justintime.com/internetbilling/index.html

KEMMERER, R. A. (1990), Integrating Formal Methods into the Development Process, *IEEE Software,* Sep, 37-50

OUREN, J., M. SINGER, J. STEPHENSON and A. L. WEINBERG (1998). Electronic bill presentment and payment. *The McKinsey Quarterly,* 4, 98 –106.

PAPADOPOULOU, P., A. TRIANTAFILLAKIS, P. KANELLIS and D. MARTAKOS (2000). A generic framework for the deployment of an Internet billing servicescape. In *Proceedings of the 1st World Congress of Electronic Commerce,* Hamilton, Ontario, Canada, January 19-21.

RÖHM, A.W., PERNUL, G. and HERRMANN, G. (1998). Modelling secure and fair electronic commerce. In *Proceedings of the 14th Annual Computer Security Applications Conference,* Scottsdale, AZ., Dec. 7-1 1, IEEE Computer Society Press.

RSA DATA SECURITY Inc. (1993). PKCS #6: *Extended –Certificate Syntax Standard,* version 1.5.

RSA DATA SECURITY Inc. (1993). *PKCS #9: Selected Attribute Types,* version 1.1.

SEGEV, A., J. PORRA and M. ROLDAN (1998). Internet security and the case of bank of America. *Communications of the ACM,* 41, Oct, 81 –87.

WALKER, K.M. and L.C. CAVANAUGH (1998). *Computer security policies and SunScreen Firewalls.* Sun Microsystems Press.

WANINGER, L., C. ANDERSON and R. HANSEN (1997). Designing Servicescapes for Electronic Commerce: An Evolutionary Approach. Available at http://www.misrc.umn.edu/wpaper/default.asp

YANG, J. and PAPAZOGLOU, M.P. (2000). Interoperation Support for Electronic Business. Communications of the ACM, 43, June, 39-47.