مقاله درس زبان تخصصی استاد جناب آقای دکتر حاجی رمضانعلی

سیامک اسمعیلی طارمسری
بابک آشفته یزدی

E-banking security: A communication perspective

This research focuses on the communication of security risk messages among organizations and particularly on communication between IT employees and managers within a bank in Greece. An important aspect of any information systems (IS) security activity is about ensuring the security of its infrastructure, and in doing so, communication is a key necessity for present e-banking security managers. Two questions motivated this research. First, what is the experience of organizations following e-banking security measures and controls as part of security management procedures? Second, what are the communication standards and procedures that play an important role in the success of e-banking security adoption? The research findings aim to shed some light into new communication practices that can be of use to IS security risk management. A case study research approach was used to investigate security communication in e-banking adoption. The issues of communication found to play an important role in e-banking security included: organizational flexibility, availability of resources, e-banking project alignment, support from top management, information transparency and security knowledge and awareness. The article concludes that banks may need to eradicate security communication problems through the successful appliance and establishment of the previously mentioned communication issues in e-banking security adoption.

Keywords:

e-banking; organizational change; security risk communication; case study

امنیت بانکداری الکترونیک :چشمانداز ارتباطات

تمرکز این تحقیق بر روی ریسک امنیتی پیام های ارتباطی در سازمانها به ویژه ارتباط بین کارکنان بخش IT و مدیران درون بانکی در یونان انجام گرفته است.یک جنبه مهم از امنیت هر سیستم اطلاعاتی تضمینی از طراحی زیر ساخت و عملکرد آن میباشد ، با توجه به اینکه امنیت مدیریت بانکداری الکترونیک یک ضرورت کلیدی میباشد. دو سئوال انگیزه ای این تحقیق بوده است اول:تجربه سازمانها در مورد روش های اندازه گیری و کنترل امنیت بانکداری الکترونیک چه بوده است؟ دوم:استانداردهای ارتباطی و شیوه هایی که نقش مهمی در موفقیت امنیت بانکداری الکترونیک اتخاذ شده اند چه هستند.؟یافته های تحقیق افقهای جدیدی برای تمرین ارتباطهای بروز میباشند و میتوانند در جهت تشخیص ریسک امنیتی سیستمهای اطلاعاتی به کار گرفته شوند.این روش تحقیق بر اساس سرمایه گزاری و داده کاوی در امنیت ارتباطی اتخاذ گردیده است.پیامدهای ارتباطی نقش های مهمی را امنیت بانکداری الکترونیک در بر میگیرند که عبارتند از:انعطاف سازمانی ،دسترسی به منابع ، پروژه صف بندی بانکداری الکترونیک که توسط مدیران بالا دست ،شفافیت اطلاعات ، امنیت دانش و آگاهی سازمانی.این مقاله بانک هایی را شامل میگردد که ممکن است نیاز به حذف مشکلات امنیتی فعلی دارند و از طریق تمهیدات موفق اشاره شده ارتباطی بدنبال اتخاذ امنیت بانکداری الکترونیک میباشند.

Introduction

As the society and its economic patterns have evolved from the heavy-industrial era to that of information, in terms of providing new products and services to satisfy people's needs, organizational strategies have changed too. In effect, corporations have altered their organizational and managerial structures, as well as work patterns, in order to leverage technology to its greatest advantage such as e-banking services. Economic and technology phenomenasuch as downsizing, outsourcing, distributed architecture, client/server and e-banking, all include the goal of making organizations leaner and more efficient. However, information systems (IS) are deeply exposed to security threats as organizations push their technological resources to the limit in order to meet organizationalneeds (Dhillon, 2001; Dhillon andTorkzadeh,2006).

مقدمه

همانند جوامع و الگوهای اقتصادی آنها که دوران صنعتی شدن وعصر اطلاعات نکامل پیدا کردند تا محصولات و خدمات جدید در جهت ارضاء نیازهای افراد فراهم نمایند ، استراتژیهای سازمانی نیز تغییر یافتند.بر اساس همین تاثیر شرکتها با تغییر سازمان و ساختار مدیریتی به همراه الگوی کار با عث پیشرفت تکنولوژی به بالا ترین مزیت خود همچون خدمات بانکداری الکترونیک شدند.اقتصاد و تکنولوژی و پدیده هایی همانند کوچک گرایی،برون سپاری،معماری توزیع شده ،سرویس گیرنده/سرویس دهنده و بانکداری الکترونیک همه باعث شدن تا سازمانها خطی (در مدیریت) و موثر تر شوند. به هر حال سیستمهای اطلاعاتی بصورت گسترده ای در معرض تهدیدات امنیتی قرار گرفتند ،بطور خاص سازمان هایی که منابع تکنولوژیکی داشتند با محدودیت نیاز سازمانی موجه گشتند.(دیلن سال ۲۰۰۱ و دیلن ترک زاده سال ۲۰۰۶)

Although the area of e-banking has only appeared in IS literature since the mid-1990s, there is a lack of research into e-banking security adoption and associated organizational issues, especially in the Greece context. There is also a lack of case studies reporting the actual experience of organizations in implementing e-banking security, particularly. As e-banking is an IT product for development, this gap in the research poses some problems for banks, especially those that currently develop e-banking security because the limitations in relation to this area usually mean difficulties in planning and developing e-banking security measures and controls.

اگرچه بحث بانکداری الکترونیک از اواسط سال ۱۹۹۰ در حوزه سیستمهای اطلاعاتی آغاز گردید ، فقدان تحقیق در انخاذ امنیت بانکداری الکترونیک و پیامدهای مرتبط سازمانی با آن بخصوص در یونان وجود داشت. همچنین عدم بررسی مطالعاتی گزارشات واقعی بویژه از تجربیات برقراری امنیت بانکداری الکترونیک نیز وجود ندارد.همانطور که بانکداری الکترونیک محصول توسعه یافته فناوری اطلاعات میباشد این شکاف در تحقیقات مشکلاتی برای بانک ها بخصوص آنهایی که در حال توسعه امنیت امنیت بانکداری الکترونیک هستند ایجاد میکند به این دلیل که محدودیت برقراری ارتباط با چنین جاهایی مشکلاتی در طراحی و توسعه اندازه گیری و کنترل امنیت بانکداری الکترونیک به همراه دارد.

The use of new distribution channels such as the internet increases the importance of e-banking security because it becomes sensitive to the environment and may leave organizations more vulnerable to system attacks. Although there are many approaches to security as a whole (for

example, checklists, risk analysis, formal methods and soft approaches – Backhouse and Dhillon, 1996; Siponen, 2001) whose value is evident – there is a belief that security can be more efficiently managed if the focus goes beyond technical-oriented solutions (James, 1996; Siponen, 2001; Dhillon and Torkzadeh, 2006).

استفاده از کانالهای نوین توزیع اعم از اینترنت اهمیت امنیت بانکداری الکترونیک را افزایش میدهد، زیرا حساسیتی که این محیط ایجاد میکند سازمانها را جهت حملات سیستمی آسیب پذیر تر مینماید.اگر چه شیو های کنترل امنیتی وجود دارند (بطور مثال: چک لیستها،آنالیز ریسک،متدهای رسمی {تفضیلی} و شیوه های نرم(بکهاوس و دیلن ۱۹۹۶ :سایپونن ۲۰۰۱) که ارزشی{اندازه گیری} راآشکار میکنند (باوری بدین مضمون وجود دارد که امنیت میتواند موثرتر مدیریت شود اگر تمرکز بر روی راه حل هایی فراتر از مباحث مرتبط تکنیکی انجام پذیرد) (جیمزوسایپونن ۱۹۹۶ و دیلن و ترک زاده ۲۰۰۶).

E-banking can not only provide enormous benefits to consumers in terms of ease and cost of transactions, but it also poses new challenges for banks in supervising their financial systems and in designing and implementing necessary security measures and controls. In doing so, understanding security communication in e-banking issues is important for senior management because it would help them improve their approach to security e-banking security. This article addresses this issue by reporting an exploratory case study of a Greek bank, which is from the first banks in Greece to develop and implement e-banking. Specifically, this research aims to explore how communication of e-banking security measures and controls takes place within the bank, what are the communication standards and procedures that play an important role to the success of e-banking security and what key lessons come out of their experience which could be generalized.

بانکداری الکترونیک نه تنها میتواند مزیتهای شگرفی در زمینه سادگی و هزینه تبادلات اطلاعات داشته باشد ، بلکه عرصه (رقابتی) جدیدی برای بانکها در ارتباط با نظارت بر سیستمهای مالی و کنترل و اندازه گیری در طراحی و پیاده سازی امنیت ایجاد می نماید.برای انجام چنین کاری فهم امنیت ارتباطات و پیامد های آن برای مدیران ارشد مهم میباشد، زیرا به آنها در بهبود روشهای امنیت بانکداری الکترونیک کمک میکند. این مقاله این پیامدها که از گزارشات مورد مطالعه کسب شده ازیک بانک یونانی (اولین بانک یونان که توسعه و پیاده سازی بانکداری الکترونیک انجام شده) نشات گرفته است. بطور مشخص هدف این تحقیق ردیابی چگونگی کنترل و اندازه گیری امنیتی بانکداری الکترونیک و محل وقوع (رخ دادن)آن در بانک میباشد ،که استانداردهای ارتباطی و شیوه هایی که نقش مهمی در موفقیت امنیت بانکداری الکترونیک بازی میکنند و منجر به موضوع کلیدی میگرددکه از این تجربیات بدست می آیدکه میتواند عمومی گردد.

Hence, e-banking security should support the mission of the financial institutions, it must be cost effective and must be in sync with employees' e-banking security understanding seamlessly, that is integrate technology, processes and people through an efficient communication process. Communication can be described as an attempt by one or more persons to send and receive messages with a clear object to provide understanding of the security context in which they apply providing an opportunity for some feedback.

از این رو امنیت بانکداری الکترونیک باید از ماموریت موسسات مالی پشتیبانی کند ، آن باید مقرون به صرفه باشد و قابل فهم برای کارمندان (امنیت بانکداری الکترونیک باید بدون نقص فهمیده شود که شامل تجمیع تکنولوژی ، فرایندها و اشخاص میباشد که در حیطه فرایند موثر ارتباط

قرار میگیرد .ارتباط میتواند همچون کوشش یک یا چند شخص برای ارسال یا دریافت پیام با هدف واضح توصیف شود تا منجر به فهمیدن مفاد امنیتی که بکار گرفته میشود و دریافت بازخورد آن فراهم میگردد.

Background to e-Banking and Security

The e-banking issue

E-banking has been around for some time in the form of automatic teller machines and telephone transactions. More recently, it has been transformed by the internet, a delivery channel for banking services that benefits both customers and banks. Access is fast, convenient and available around the clock, whatever the customer's location. In addition, banks can provide services more efficiently and at substantially lower costs.

سابقه بانکداری الکترونیک

پیامدهای بانکداری الکترونیک

بانکداری الکترونیک بصورت دستگا ههای خود پرداز و بانکداری تلفنی از مدت ها قبل پیرامون ما وجود داشته است.در این اواخر بصورت اینترنتی نیز تغییر شکل داده است (ارائه کانل سرویس بانکی که مزیتهایی برای مشتریان و بانک به همراه داشته است). دسترسی سریع ، متعارف و در هر زمان و در محل مشتری.بعلاوه بانک میتواند سرویس موثرتر و و متعاقبا با هزینه پایینتر ارائه دهد.

Although e-banking can provide a number of benefits for customers and new business opportunities for banks, it exacerbates traditional banking risk that is, operational risks, reputational risks, legal risks, to mention only some of them. Even though considerable work has been done in some banks in adopting e-banking security measures and regulations, continuous vigilance and management will be essential as the scope of e-banking increases. There is still a need to establish greater harmonization and coordination with the banks' business objectives. The next section summarizes some of the research done in the area of organizational information security approaches.

اگرچه بانکداری الکترونیک میتواند مزیتهای زیادی برای مشتریان و فرصتهای جدید کسب و کار برای بانکها به همراه داشته باشد،ریسکهای ستنی بانکی را نیز تشدید مینماید (ریسکهای عملیاتی، ریسکهای اعتبار،ریسکهای قانونی)که برخی از آنها اشاره گردید. با این اوصاف با در نظر گرفتن اتخاذ دستورالعملها و اندازگیری های امنیتی بانکداری الکترونیکی ، استمرار در مراقبت (نظارت) و مدیریت در حوزه بانکداری الکترونیک افزایش می یابد، هنوز نیاز به برقراری هم آهنگ سازی و هماهنگی بیشتر با اهداف کسب و کار بانک وجود دارد.بخش بعدی خلاصه ای از تحقیقات انجام گرفته وشیوه های آن در امنیت اطلاعاتی سازمانی ذکر شده است.

Interpretative information security behavior within organizations

Although a number of IS security approaches have been developed over the years whose value is evident such as checklists, risk analysis and evaluation methods, they ignore the wider organizational context and take into account the technical issues. In this context, Dhillon and Backhouse (2001) argued that these approaches represent the functionalist paradigm. However,

there is still an alternative interest to study the social and organizational context in which information security is developed and managed. For example, Dobson (1991) used social theory to investigate security in terms of human roles, actions, goals and policies. Willcocks and Margetts (1994) emphasized the importance of the social and qualitative characteristics of information security. Kokolakis *et al* (2000) combined risk analysis with organizational analysis on the basis of a structure consisting of agents, activities, resources, information, assets and roles.

تقسیر امنیت اطلاعات و رفتار آن در سازمانها

با اینکه تعدادی از روشهای امنیت سیسمهای اطلاعاتی در طول سال ها توسعه پیدا کرده اند که شامل سنجشهایی از قبیل چک لیست،آنالیز ریسک و متدهای ارزیابی میگردند ، این سنجشها در سازمانهای بزرگ در نظر گرفته نمیشوند و به محاسبه پیامد تکنیکی تغییر می یابند.در همین زمینهدیلن در سال ۲۰۰۱ استدلال نمود این شیوه ها بیانگر تناقض کنش های عملیاتی میباشد.با این حال هنوز مطاعه جایگزین مورد علاقه در جامعه و سازمانها در ارتباط با توسعه و مدیریت امنیت اطلاعات جود دارد.بطور مثال دابسون در سال ۱۹۹۱ از تئوری اجتماعی در تحقیقات امنیتی با مضامین (نقش های افراد،عملکردها، اهداف و خط مشی)استفاده نمود.ویل کلاک و مارگارت در سال ۱۹۹۴ بر اهمیت جوامع و خصوصیات کیفیتی امنیت اطلاعات تاکید نمودند.کوکولاکیس در سال ۲۰۰۰ آنالیز ریسک را باآنالیز سازمانی بر پایه پایداری ساختار بنگاه ها ، فعالیت ها ، منابع ، اطلاعات ، دارایی ها و نقش ها ترکیب کردند.

Similarly, Orlikowski and Gash (1994) emphasized the importance of understanding the assumptions and values of different stakeholders to successful IS implementation. Such values have also been considered important in organizational change (Simpson and Wilson, 1999), in security planning (Straub and Welke, 1998) and in identifying the values of internet commerce to customers (Keeney, 1999). Dhillon and Torkzadeh (2006) have also used the value-focused thinking approach to identify fundamental and mean objectives, as opposed to goals, that would be a basis for developing IS security measures. These value-focused objectives were more of the organizational and contextual type.

مشابه همین ، اورلیکاوسکی و گراش در سال ۱۹۹۴ بر اهمیت فهم مفروضات و ارزشهای متفاوت ذینفعان جهت پیاده سازی موفق سیستم اطلاعاتی تاکید کردند.این چنین ارزش گزاری در تغیرات سازمانی مهم در نظر گرفته میشود(سامسون و ویلسون در سال ۱۹۹۹) در طراحی امنیت (استراب و ولک در سال ۱۹۹۸)و در هویت ارزشها ی بازرگانی اینترنتی مشتریان (کنی در سال ۱۹۹۹ودیلون و ترک زاده در سال ۲۰۰۶)،ارزش تمرکز و شیوه تفکر برای شالوده هویت و تجسم اهداف در مقابل اهداف به صرف توسعه اندازه گیری امنیت اطلاعات به کارگرفته شده است.

A number of studies investigated inter-organizational trust in a technical context. Some of them have studied the impacts of trust in an e-commerce context (McKnight *et al*, 2002; Gefen *et al*, 2003; Gefen and Straub, 2004) and others in virtual teams (Ridings *et al*, 2002; Sarker *et al*, 2003). Workman (2007) studied trust as a factor in social engineering threat success and found that people who were trusting were more likely to fall victims to social engineering than those who were distrusting. Koskosas (2008) used trust and goal setting theories to understand security

management procedures and found that higher levels of trust among employees in organizations lead to more efficient goal security mechanisms and procedures.

تعدادی از تحقیقات مطالعاتی درون سازمانی بر اساس مفاد تکنیکی میباشد .برخی دیگر برپایه تاثیرات درونی مفاد بازرگانی الکترونیکی (مک نایت ۲۰۰۲،جفن ۲۰۰۳ ، و جفن استراب ۲۰۰۴)استوار است و برخی دیگر در تیمهای مجازی (ریدینگ ۲۰۰۲ ، سارکر ۲۰۰۳، ورکمن ۲۰۰۷)با مطالعه اعتماد به فاکتور مهندسی اجتماعی، تهدید و موفقیت بنا شده است که بر همین اساس افرادی که به این موضوع اعتقاد داشتند بیشتر در معرض اینگونه مخاطرات قرار گرفته بودن تا دیگر افراد که اعتقادی به این موضوع نداشتند.(کسکوساس در سال ۲۰۰۸) ار تئوری اعتماد و هدف استفاده نمود و متوجه گردید شیوه های مدیریتی که بر اساس اعتماد بالای بین کارکنان در سازمان ها پایه ریزی شده اند به سمت اهداف و شیوه ها و مکانیزم های امنیتی موثرتر رهنمون گردیده اند.

However, in terms of information security behavior within organizations, security behavior can be seen as part of the organizational culture and may define how employees see the organization. Similarly, organizational culture is a system of learned behavior, which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process. Albrechtsen (2007) found that users considered a user-involving approach to be much more effective for influencing user awareness and behavior in information security. Leach (2003) studied influences that affect a user's security behavior and suggested that by strengthening security culture organizations may have significant security gains. Debar and Viinikka (2006) investigated security information management as an outsourced service and suggested augmenting security procedures as a solution.

به هر حال با عنایت به رفتار امنیت اطلاعات درون سازمان ها ، رفتار امنیتی میتواند همچون بخش از فرهنگ سازمانی نگریسته شود و نگرش کارمندان به سازمان را تعریف مینماید.متشابها فرهنگ سازمانی یک سیستم یاد گیری رفتار است که بازتابی از درجه آگاهی کاربران میباشد و میتواند بر روی موفقیت یا شکست فرآیند امنیت اطلاعات موثر باشد.آلبرتسن در سال ۲۰۰۷ متوجه گردید که نگرشهای کاربران در شیوه های کاربر محور، بر روی تنویر آگاهی های کاربران و رفتار امنیت اطلاعات آنان میتواند بسیار موثر باشد. لیچ در سال ۲۰۰۳ بر روی نفوذ(تاثیر) جنبه های رفتاری امنیت کاربران مطالعه نمود و اظهار نمود که قوی نمودن فرهنگ امنیت در سازمان ها میتواند مزیت شگرفی در امنیت به همراه داشته باشد. دبر و ویکینا در سال ۲۰۰۶باتحقیق بر برون سپاری خدمات مدیریت امنیت اطلاعات آنرا بعنوان را ه حلی جهت تقویت شیوه های امنیتی پیشنهاد کردند.

In the context of information security, behavior can be considered as the perception of organizational norms and values associated with information security and so it exists within the organizations, not in the individual. To this end, individuals with different backgrounds or at different levels in the organization may tend to describe the organization in similar way. Security culture is used to describe how members perceive security within the organization. According to Beatson (1991), security is part of corporate culture and should be taken into consideration, as well as other elements of corporate culture such as the successful communication of security policies and procedures to the people involved. As security and risk minimization are embedded into the organizational culture all employees, managers and end-users must be concerned of security issues in their planning, managing and operational activities. In order to ensure effective and proactive information security, all staff must be active participants rather than passive observers of information security. In doing so, staff must strongly hold and widely communicate the norms and values of the organizational culture in terms of information security behavior,

understanding and perception through efficient communication procedures. *To this end, this research suggests that an effective communication process through which security messages are embedded and circulated positively among employees, will play an important role in e-banking security planning and development.*

پیرو موضوع امنیت اطلاعات رفتار میتواند همچون درک استاندارد سازمانی در نظر گرفته شود و ارزشها مرتبط با امنیت اطلاعات که میتوند در درون سازمان وجود داشته باشد نه در فرد.در ارتباط با نکته آخر افراد با زمینه های مختلف یا قدرت متفاوت در سازمان ممکن است گرایش به توصیف سازمان از را ه مشابه باشند.فرهنگ امنیت در صدد توصیف چگونگی درک امنیت درون سازمان است.مطابق با تعریف بیتسون در سال ۱۹۹۱ امنیت بخشی از فرهنگ شرکت است و باید به همراه دیگر المان های امنیت شرکت در نظر گرفته شود ، همچون خط مشی ها و شیوه های امنیتی ارتباطی که افراد را در بر می گیرد.همانطور که امنیت و کوچک کردن ریسک در درون فرهنگ سازمانی نهادینه میشوند همه کارمندان ، مدیران و کاربران باید دلواپس پیامدهای امنیتی در طراحی هایشان ، مدیریتشان و دیگر فعالیتهای عملیاتیشان باشند.همه کارکنان باید مشارکت فعال بجای مشاهده امنیتی اطلاعاتی غیر فعال داشته باشند.جهت انجام این مهم همه کارکنان باید قدرتمندانه و گسترده در چهارچوب و ارزش های فرهنگی سازمان با عنوان رفتار امنیتی سازمان و فهم و درک شیوه های موثر ارتباطی حضور داشته باشند.*در پایان این تحقیق اظهار مینماید که یک فرایند ارتباطی موثر بر اساس پیامهای(تبادلات) امنیتی نهادینه شده اند که گردش مثبتی درون کارمندان سازمان دارند(نگرش مثبت به کار درون سازمانی بین کارکنان) و نقش مهمی را در طراحی و توسعه امنیت بانکداری الکترونیک بازی می کنند.*

Information security risk communication

Communication can be mainly distinguished into formal and informal communication whereas a single message is communicated securely through the interplay of these two types of communication (Rogers and Kincaid, 1981). However, it is believed that formal communication, as opposed to informal, is not very interactive and does not support the establishment of new ideas with quick feedback from specialized people who can uniquely address the question and who have pre-defined a common ground (Mikhailov *et al*, 1984).

ریسک ارتباط امنیت اطلاعات

ارتباط میتواند در اصل بین ارتباط رسمی و غیر رسمی تمیز داده شود.در حالیکه در اثر متقابل این دو یک پیام بصورت ایمن ارتباط داده میشود .(روژر و کینکید سال ۱۹۸۱) . به هر حال این باور وجود دارد که ارتباط رسمی در مقابل ارتباط غیر رسمی قرار دارد ، و این موضوع خیلی فعل و انفعالی نیست و از برقراری یک ایده جدید با باز خورد سریع افراد متخصصی که میتوانند منفردا سوالی را طرح نمایند و کسانی که از پیش مشخص همین تفکر را دارند پشتیبانی نمیکند .(مایک هایلو ۱۹۸۴)

In a similar vein, risk communication could accurately be described as a subset of communications science. Though there are numerous definitions for the term communication, in this research, communication itself could be described as the attempt by one or more persons to send and receive messages with a clear object to provide an understanding of the context in which they apply providing an opportunity for some feedback.

در حالت مشابه،ریسک ارتباط بشکل صحیحی به زیر مجموعه ای از علم ارتباطات توصیف میگردد.اگرچه تعاریف زیادی برای واژه ارتباط وجود دارد، در این تحقیق ارتباط به خودی خود میتواند به کوششی توصیف گردد که توسط یک یا چند شخص جهت ارسال و دریافت پیام ها با هدف مشخص و درک زمینه پیام ، همراه باا فرصتی برای بکار بستن برخی از بازخوردها فراهم میگردد.

Risk communication is more complicated and difficult as it might appear. In particular, risk communication becomes difficult not only because the exchange of information among the involved parties is complicated, but also because the risk messages have to be formulated, embedded and circulated within the wider organizational and, more specifically, cultural contexts to which they apply. The evolution of practice in risk communication comes from an understanding that communication is more than just the transfer of knowledge. It can only be termed communication if the message has been transferred and understood.

ریسک ارتباط پیچیده تر و غامض تر از آن چیزی است که به نظر میرسد. به ویژه ریسک ارتباط غامض تر میشود نه فقط به خاطر تبادل اطلاعات در پیچیدگی فعالیت ارتباطی که در برخواهد داشت ، بلکه به خاطر ریسک پیام هایی که مجبورند تنظیم گردند،جاسازی شوند و در گستره سازمان به چرخش درآیند و به طور خاص تر زمینه فرهنگی که باید به کار گرفته شود.تکامل تمرین در ریسک ارتباط ، از درک این که ارتباط بیش از انتقال دانش است می آید.و آن فقط موقعی میتواند ارتباط نامیده شود که پیام انتقال پیدا کرده و درک نیز گردد.

The US National Research Council distinguishes between two types of major problems in risk communication: those deriving from institutional and political systems and those between risk communicators and receivers. In the first case, various kinds of legal considerations such as liability and informed consent affect the content of risk messages by influencing the available options for risk managers. Similarly, the problems between risk communicators and receivers arrive in case of difficulty to establish and recognize credibility, being alert in case of emergency, make messages understandable, capture and focus public's attention, and receive information (NRC, 1999).

انجمن بین المللی تحقیقات آمریکا بین دو نوع اصلی مشکلات ریسک ارتباط تفاوت قائل میشود:یکی آنهایی که مشتق از موسسات و سیستم های سیاسی هستند و دیگری ریسکی که فی مابین ارتباط دهندگان و دریافت کنندگان وجود دارد.در حالت اول انواع مختلفی از ملاحظات قانونی از قبیل مسئولیت و تجویز آگاهانه بر روی محتوی ریسک پیام ها از طریق تحت نفوذ قرار دادن اختیارات مدیریتی تاثیر گذار خواهد بود.متشابها مابین ریسک ارتباطهاو مخاطبین آنها ازقبیل مشکلات برقراری ارتباط و تشخیص اعتبار سنجی ،زنگ خطر حالت اضطراری ،درک صحیح از تولید پیامها،گرفتن و تمرکز بر موضوعات مهم عمومی و دریافت اطلاعات وجود دارد (NRC۱۹۹۹).

Research Method

In order to identify appropriate research methods for this research, a taxonomy of IS research methods proposed by Galliers (1992) was used. The ontology of this research with regard to e-banking security is that security should not only be treated as something tangible and concrete, but also as a communication issue. To this end, a qualitative research approach having philosophical foundations mainly in interpretivism was deemed appropriate for this study. Data were collected over a period of 6 months. Access to Omega bank was gained through a personal

contact at senior management level. Omega bank consisted of more than 5500 employees within its organizational structure inside and outside of Greece with 410 employees of them in the IS/IT unit of the bank.

روش تحقیق

پیرو تشخیص روش تحقیق مناسب برای این تحقیق، روش پیشنهادی طبقه بندی علمی سیستم های اطلاعاتی توسط گالیرز در سال ۱۹۹۲مورد استفاده قرارگرفت.هستی شناسی این تحقیق با ملاحظه امنیت بانکداری بدین نحو است که امنیت باید نه تنها محسوس و واقعی باشد بلکه همانند رخداد ارتباطی نگریسته شود.در پایان یک تحقیق کیفی باید ماهیت فلسفی داشته باشد و حالت تفسیری برای مطالعه این تحقیق خاص فرض گردیده است.اطلاعات در بازه زمانی ۶ ماهه جمع آوری شده اند.دسترسی به بانک امگا مزیت ارتباط با مدیران ارشد را به همراه داشته است.بانک امگا متشکل از ۵۵۰۰ پرسنل در ساختار سازمانی داخلی و خارج از یونان با ۴۱۰ نفر از پرسنل در بخش سیستمهای اطلاعاتی-فناوری اطلاعات بانک می باشد.

For the purpose of this research, it was decided that the advantage offered by a single case study – investigating a phenomenon within its real life context – made this method the most appropriate (Yin, 1994; Cavaye, 1996). A phenomenon is investigated in depth and a rich description and understanding are required when a single case study is used (Walsham, 1995). As no previous research has studied e-banking security through a communication perspective in Greece, this research study represents an innovative and original contribution to the field. However, the method of selection could bias the results because of (a) the specific market sector studied, that is, bank; (b) the investigation followed through within a specific culture, which may not be applicable to different cultures; and (c) the collection and analysis of results from one particular organization.

جهت دستیابی به هدف این تحقیق ،تصمیم گرفته شد که مزیت یک روش تحقیق واحد(با تحقیق بر روی مفاد حقیقی و واقعی زندگی) این روش را به بیشترین(بهترین) شکل اختصاصی سازد.(ین درسال ۱۹۹۴ و کاویه در سال ۱۹۹۶). یک پدیده زمانی بصورت کامل سرمایه گزاری میگردد و بشکل جامع توصیف و درک میگردد که یک روش تحقیق مجزا و منفرد خاص آن استفاده شود (والشام ۱۹۹۵). همانطور که هیچگونه تحقیقی از قبل بر روی امنیت بانکداری الکترونیک با چشم انداز ارتباط در یونان انجام نشده بود،مطالعه این تحقیق بیانگر یک انگیزه و شراکت ریشه ای در این زمینه میباشد.به هر حال روش انتخابی میتواند بیانگر این نتایج و بدین علل باشد (a) بخش مشخصی از بازار مورد مطالعه که بانک میباشد (b) تحقیق بر روی فرهنگ خاصی پیگیری گردیده که ممکن در فرهنگهای مختلف دیگر کاربردی نباشد.(c) جمع آوری اطلاعت و آنالیز نتایج درمورد سازمانی مشخص.

Data for this case study were collected using a number of data gathering tools such as interviews, archival records, documents (data triangulation) and observations. These tools and their applications in this research are described in the following.

داده های این روش تحقیق با ابزارهای مختلفی از قبیل مصاحبه، ثبت های آرشیو شده ، مستندات (اطلاعات سه وجهی) و مشاهدات جمع آوری شده اند.

Interviews

Rubin and Rubin (1995) defined interviews as, any verbal confirmation or dis-confirmation of observation or any formal, informal or casual answers to questions. Interviews took place as a primary tool for data collection, as they provide in-depth information about a particular research issue or question. The number of people interviewed was approximately 155. Most interviewees were interviewed approximately 6–10 times during the 6-month period. The interviewees ranged from IT managers, deputy managers, auditors, technicians, mathematicians, software programmers, IT analysts and so on. The interviews were conducted face-to-face, and when necessary, follow-up telephone interviews were scheduled to discuss unclear data. Table 1 presents the type of interviews and other related details. When the interviews were of the formal type, they were focused only upon the research and recorded. Informal interviews were conducted in informal settings such as lounge room, corridors, outside the building and were not tape-recorded but were based on the researcher's personal interpretation.

رابین در سال ۱۹۹۵ مصاحبه را بصورت هر تایید یا عدم تایید شفاهی یا هر جواب معمولی رسمی یا غیر رسمی به ستوالات تعریف نمود.مصاحبه بعنوان ایزار اصلی برای جمع آوری اطلاعات با جزئیات برای تحقیق خاص یا رخداد یا سئوال مصاحبه در نظر گرفته میشود.تعداد افراد مورد محاسبه حدود ۱۵۰ نفر بودند.بیشترین حوزه مصاحبه شوندگان از مدیران فناوری اطلاعات ، جانشین مدیران ،حسابرسان ،تکنیسینها ، ریاضی دان ها ، بر نامه نویسان نرم افزار،تحلیل گران فناوری اطلاعات و غیره بودند.مصاحبه ها بصورت نزدیک و روبروی هم بودند و درصورت نیازبرای داده های مبهم بصورت تلفنی زمان بندی میگردید.جدول ۱ بیانگر نوع مصاحبه ها و جزئیات آن میباشد.برای مصاحبه های رسمی برپایه ثبت و تحقیق تمرکز میگردید.و مصاحبات غیر رسمی در محل هایی همچون اتاق استراحت ، راهرو و خارج از ساختمان و جاهایی که دستگاه ثبت وجود نداشت ولی بر پایه تفسیر و پژوهش شخصی انجام میگردید.

Table 1 - An example of the interviews conducted at the Omega bank.

Table 1. An example of the interviews conducted at the Omega bank

Figures and tables index | Next table

Type of interview	*Respondent position in organization*	*Respondent position in the e-banking security management*	*Number of formal interviews*	*Number of informal interviews*
Face to face	Head of IS/IT unit	Leading e-banking projects	2	2
Face to face	IS/IT deputy manager	Active action in all IS/IT projects	3	4
Face to face	Support analyst	Technical planning	2	1
Face to face	Programmer	Programming	1	1
Face to face	Risk evaluator	Risk evaluation	4	–
Face to face	Mathematician	Risk analyst	2	–
Face to face	e-commerce marketing coordinator	e-banking interface and liable for new e-products/services	2	4
Face to face	IS/IT employees	General e-banking activities	55	20
Face to face	Investments manager	Participation to project activities	3	2
Face to face	Other bank employees	Part of the organization's general activities	35	0

Figures and tables index | Next table

Observations

An observation is the act of being part of a phenomenon, often with instruments and trying to record it for scientific reasons or otherwise. Data gathered from observations are used for the purpose of description of settings, activities, people and the meanings of what is observed from the perspective of the participants (Patton, 1990). Observation was particularly useful during this research period as it provided useful insights into e-banking security and communication among the organizational employees.

مشاهدات

مشاهده بخشی از واقعیت وجودی یک پدیده است، اغلب با ابزارها و کوششی جهت ضبط آن بدلایل علمی یا غیر آن.داده ها از طریق مشاهدات که به منظور توصیف چیزها یا فعالیتها ، اشخاص و به معنی هر چیز مشاهده شده از منظر شرکت کنندگان جمع آوری میگردد(پاتون ۱۹۹۰).مشاهده در طول این دوره تحقیق بصورت ویژه ای مهم بوده است ، همانطور که مشاهدات فراهم میگردیده است، به علت روشن نمودن امنیت بانکداری الکترونیک و ارتباط در بین کارمندان سازمان مهم بوده است.

Examination of organizational documents

Another issue to be resolved with the research approach used here concerns data collection. This study employed multiple data-collection methods, as this is important in case research studies (Benbasat *et al*, 1987). In all cases, data were collected through a variety of methods and secondary data, including documents, reports, white papers, organizational records and physical artefacts as shown in Table 2. The use of multiple data collection methods makes triangulation possible, and this provides for stronger substantiation of theory (Eisenhardt, 1989). Triangulation is not a tool or strategy but rather an alternative to validation (Denzin, 1989; Flick, 1992). Thus, any finding or conclusion made from the case is likely to be more convincing and accurate if it based on several different sources of information (Yin, 1994). Five types of triangulation have been identified in the literature (Janesick, 2000): data, investigator, theory, methodological and interdisciplinary. The present study used data, theory (IS security and communication), methodological (case study) and interdisciplinary (IS and social sciences) triangulation.

آزمایش مستندات سازمانی

دیگر رخداد مقرر شده در این شیوه تحقیق ملاحظات مربوط به جمع آوری داده میباشد.این مطالعه چندین روش جمع آوری داده را به کار گرفته است، کمااینکه در مطاللعه موضوع تحقیق مهم میباشد (بن باسات سال ۱۹۸۷). در همه حالات داده با روش های متنوع و جانبی داده : شامل گزارشات ،دست نویس های کاربردی، ثبت های سازمانی ومصنوعات فیزیکی، همانطور که در جدول ۲ نشان داده شده است جمع آوری شده اند .استفاده از چندین روش جمع آوری داده، محاسبات سه وجهی(چندین نوع محاسبه همزمان) را ممکن میسازد و اثبات محکم فرضیه را موجب میگردد(ایسنهارت ۱۹۸۹). محاسبات چند سطحی یک ابزار یا استراتژی نیست بلکه یک بدیلی برای اعتبار میباشد (دنزن ۱۹۸۹:فلیک ۱۹۹۲). بنابراین هر یافته یا استنتاجی از یک موضوع احتمالا متعارف تر و دقیقتر خواهد بود اگر اگر مبتنی بر چندین اطلاعات منبع باشد (بین سال ۱۹۹۴). پنج نوع محاسبه چند وجهی در متون مشخص گردیده اند (جانیسیک سال ۲۰۰۰) : داده ، محقق ، فرضیه ، روش شناسی، و تحقیق در چندین رشته علمی. ره آورد (دستاورد) مطالعه شامل داده ، فرضیه (امنیت سیستمهای اطلاعاتی و ارتباط)، روش شناسی (موضوع تحقیق) و تحقیق چند وجهی (سیستمهای اطلاعاتی و علوم اجتماعی) خواهد بود.

Table 2 - Sources of secondary data used in this research.

FROM:
E-banking security: A communication perspective
Ioannis Koskosas

Table 2. Sources of secondary data used in this research

Previous table

• Organizational annual reports
• Omega bank's organizational chart
• Archival records
• Leaflets informing customers about e-banking products and services
• IS/IT investment reports
• E-banking security development reports on past projects
• White papers
• Organizational records
• Financial investments on previous technologies relative to e-banking security
• Background information documents about the organization's history
• Observation of physical artefacts

Analysis of data

The analysis begins with the identification of themes emerging from the raw data and was focused over issues found to be critical. This technique provided a reflection in the understanding of communication from different perspectives. The result findings were presented in the form of a report that was sent to all participants within Omega bank. Thereafter, having discussed the findings with the research participants at Omega bank and after some amendments on the research results, in part of the bank senior executives and IT employees, it was agreed that the results were inside focus.

Top of page

تجزیه و تحلیل داده

تجزیه و تحلیل با شناسایی تمهای پدیدار شده ازمیان داده های خام و تمرکز بر روی مهم ترینشان آغاز می گردد .این تکنیک برای فهم ارتباط از دیدگاه های مختلف است . نتایج یافته شده در قالب یک گزارش که به همه شرکت کنندگان در بانک امگا ارسال شد . پس از آن، درباره یافته ها با شرکت کنندگان در تحقیق در بانک امگا بحث و گفتگو شد و بعد از آن اصلاحاتی در نتایج تحقیقات به عمل آمد سپس نتایج حاصله را با مدیدران ارشد بانک و کارمندان بخش IT در میان گذاشته شد .توافق گردید تا تمرکز در درون سازمان باشد.

The Omega Bank – Background

The Omega bank (Omega bank's real name has been substituted because of confidentiality reasons) is one of Greece's leading providers of personal financial services and products with more than 5500 employees internationally and assets of 35 billion in year 2009–2010. Omega bank has more than 650 branches around the world, including Greece, and is a very innovative organization with large investments on new technologies that put Omega bank at the forefront of providing financial services through its electronic channels in the country.

امگا بانک – سابقه

بانک امگا (بانک امگا یک بانک واقعی می باشد که به دلایل امنیتی با این نام خوانده می شود) یکی از بانکهای پیشرو در زمینه تامیین منابع مالی و محصولات گوناگون در یونان می باشد .این بانک بیش از 5500 کارمند بین المللی و دارای دارایی معادل 35 میلیارد در سال 2009-2010 می باشد. بانک امگا دارای 650 شعبه در سراسر دنیا و از جمله یونان است .این بانک با سرمایه گذاری فراوان یکی از سازمانهای بزرگ در ارایه خدمات جدید و نوآورانه می باشد که در خط مقدم ارایه خدمات مالی از طریق بسترهای الکترونیکی در این کشور قرار گرفته است .

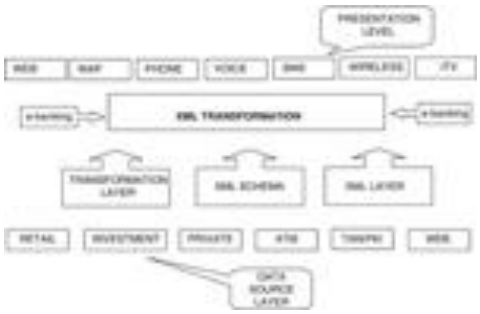
Communication at Omega bank

Communication among different units within Omega bank was efficiently processed through a variety of channels including fax, telephone, e-mails, digital televisions and wireless application protocol (WAP) phones (see Figure 1). This meant that all employees and executives have all-time access to the files in which they are liable to during specific time frames only.

Figure 1.

ارتباطات در امگا بانک

ارتباط میان واحدهای مختلف در بانک امگا از طریق بسترهای ارتباطی مختلف نظیر فکس ، تلفن ، ایمیل ، تلویزیون دیجیتال (ویدئو کنفرانس) و استفاده از پروتکل بیسیم می باشد .(تصویر 1) این بدان معنی است که کلیه کارکنان و مدیران در هر زمان به فایلها و اطلاعات مورد نظرشان با توجه به حدود اختیاراتشان دسترسی دارند.



Levels of multi-channel applications with XML use.

Full figure and legend (61K)

By doing so, bank employees had access to the files depending on their position and line of execution within their units and only during office hours from 08:00 hours to 19:00 hours the latest, that is in order to avoid any possible suspicious activities. In turn, the employees' units were part of three main levels of hierarchy: (1) the execution level, in which units were responsible for daily routine activities such as transactions, payments, debit decisions, sales and so on, (2) the managerial level, in which units were responsible for surveillance, control and decision-making activities of the middle management executives, and (3) the strategic level, in

which units were responsible for strategic issues with regard to bank long-term investments and competition from the external environment.

In all these three levels of hierarchy, there was a vertical line of communication among these different units depending on the functionality each unit was capable of, for example, marketing and sales, finance and accounting, human resources, IS/IT systems backup unit and so on. Therefore, each unit depending on what level of the hierarchy it belonged to, and on its functionality, had access to specific files and documents of the bank. An example of the general communication process through hierarchy levels within Omega bank is illustrated in Figure 2.

ارتباطات در امگا بانک

با انجام این کار با توجه به موقعیت شغلی و میزان دسترسی هر یک از پرسنل آنها تنها در ساعت اداری 8:00 الی 19:00 به اطلاعات دسترسی دارند .همچنین به منظور جلوگیری از هر گونه تخلف در هر بخش سه سطح دسرسی دیده شد.

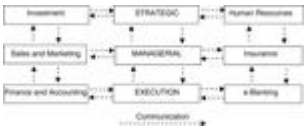
سطح 1 : سطح اجرایی .که در این سطح فعالیتهای روزانه مانند معاملات ، دریافت و پرداخت ها ، فروش و غیره اننجام می گردد .

سطح 2 :سطح مدیران میانی : در این سطح مسولیت نظارت و کنترل بر فعالیتهای صورت گرفته دیده شده است.

سطح 3 : سطح استراتژیک (مدیران ارشد) : در این سطح با توجه به سرمایه گذاریهای بلند مدت بانک و همچنین رقابت با رقبای بیرونی برانامه استراتژیک بانک تعیین می گردد .

با توجه به قابلتهای هر یک از این سه سطح یک ارتباط به صورت از عمودی (سلسله مراتبی) وجود دارد .به عنوان مثال بازاریابی و فروش، مالی و حسابداری، منابع انسانی، آی تی ، واحد سیستم های پشتیبان و غیره

و (**Figure 2.**



Communication flow through hierarchy levels at Omega bank.

روند ارتباط از طریق سطوح سلسله مراتب در بانک امگا

Full figure and legend (51K)

However, communication within Omega bank was most of the times efficient, which in turn allowed for continued e-banking setting and activities plan that had an ultimate effect on the e-banking security development and management. *The experience of the bank following e-banking security measures and controls as part of security management procedures was a positive and*

complex one since the communication within the organization was almost flawless and without any serious drawbacks while it was complex due to the new changes the organization went through with an ultimate effect on the procedures of security design.

با این حال، درون بانک امگا اغلب اوقات ارتباطات موثر بودند، و در عوض به ادامه فعالیت برنامه طرح و تنظیم بانکداری الکترونیکی که یک تاثیر نهایی در توسعه امنیت و مدیریتی بانکداری الکترونیکی دارد، اجازه داد. اقدامات امنیتی بانکداری الکترونیکی و کنترل به عنوان بخشی از روش های مدیریت امنیت قسمت مثبت و پیچیده تجربه از بانک بود، زیرا ارتباطات درون سازمانی تقریبا بی عیب و نقص و بدون هیچ گونه اشکالات جدی بودند، در عین حالیکه با توجه به تغییرات جدید سازمان با اثر نهایی در مراحل طراحی امنیتی، پیچیده بود.

Similarly, communication had an ultimate effect on security management in the long term. Having an IT security program consistent with the overall business goals ensures that problems can be manipulated efficiently during the support of e-banking products and services to the customers. That said, the security measures and policies with regard to e-banking development and management, implies that part of them should consider the overall business goals of the bank strategic scheme. Such business goals mainly include cost reduction, service quality and systems efficiency. An IT executive officer stated: *The main idea behind the development and use of e-banking services offered to our customers was initially to improve the quality of our financial services while minimizing production costs. In doing so, we had to plan considerable amounts of money and effort to ensure that security threats will not dampen the bank's overall business goals and in doing so, communication is vital.*

به طور مشابه، ارتباطات دارای یک اثر نهایی در مدیریت امنیتی در دراز مدت هستند. داشتن یک برنامه امنیتی فناوری اطلاعات سازگار با اهداف کلی کسب و کار تضمین می کند که با حمایت محصولات و خدمات بانکداری الکترونیکی، مشکلات مشتریان می توانند به طور دقیق برطرف گردد. گفته می شود، اقدامات و سیاستهای امنیتی در رابطه با توسعه بانکداری الکترونیکی و مدیریت نشان می دهد که، بخشی از این طرح استراتژیک باید به عنوان اهداف کلی کسب و کار بانک در نظر گرفته شوند. این اهداف کسب و کار به طور عمده شامل کاهش هزینه، کیفیت خدمات و بهره وری سیستم می شوند. یک کاربر ارشد اجرایی فناوری اطلاعات اظهار داشت: در ابتدا، بهبود کیفیت خدمات مالی در حین به حداقل رساندن هزینه های تولید، در پشت ایده اصلی توسعه و استفاده از خدمات بانکداری الکترونیکی ارائه شده به مشتریان بود. در انجام این کار، ما باید پول و تلاش قابل توجهی را به گونه ای برنامه ریزی میکردیم تا اطمینان حاصل شود که تهدیدات امنیتی، اهداف کلی کسب و کار این بانک را کاهش نداده و در انجام این کار، ارتباطات حیاتی هستند.

The security of e-banking channels, for Omega bank, was a key enabler for minimizing consumers' fears about such type of transactions, as security is one of the main obstacles for e-commerce growth (Regan and Macaluso, 2000; Turban *et al*, 2000). In doing so, Omega bank used the highest levels of encryption standards to secure e-banking services. The Omega bank IT deputy manager claimed *we use the finest encryption techniques in all areas of our front end and back end systems. In particular, we use secure layer technology which encrypts all information, from a customer logging in or filling in an application form to storage and feedback to the customer.*

از آنجایی که امنیت یکی از موانع اصلی برای رشد تجارت الکترونیک است، امنیت کانال های بانکداری الکترونیکی بانک امگا، فعال سازی یک کلید برای به حداقل رساندن ترس مصرف کنندگان در مورد این نوع از تراکنش ها بود (Regan and Macaluso, 2000; Turban et al, 2000) . در انجام این کار، بانک امگا از بالاترین سطح از استانداردهای رمزگذاری برای تامین امنیت خدمات بانکداری الکترونیکی استفاده کرد. معاون مدیر بانک امگا ادعا کرد: ما از بهترین تکنیک های رمزنگاری در تمام زمینه های قابل دسترس و غیر قابل دسترس مصرف کننده استفاده می کنیم. ما به طور خاص از تکنولوژی لایه امن که تمام اطلاعات مشتری از مرحله ورود به سیستم یا پر کردن یک فرم درخواست تا ذخیره سازی و بازخورد به مشتری را رمز گذاری می کند، استفاده می نماییم.

The experience of Omega bank following e-banking security measures was therefore positive as the real-time perception of e-banking security risks was reflected on the overall success of e-banking security without any serious loses in the past, in terms, of operational failure, legal failure or successful attacks to systems. Although communication, in terms of how the security risk messages were circulated within the e-banking unit, was biased sometimes because of the bank's large-scale structure. In effect, there was a delay into how the messages were being circulated, transmitted and embedded, as the activities of the e-banking unit were not seen in the same positive light from other units of the bank. Thus, as the communication process entails the cooperation of different banking units, those units were sometimes in a dead end as they could not understand the exact scope and needs of the e-banking unit in the context of security development. As a consequence, there were times that the e-banking unit had to postpone security activities such as the application of new software and hardware material for the maintenance and support of e-banking. *In the following, some other communication standards and procedures which are critical to the success in e-banking security adoption are analyzed and these can be used as an example for other banks to apply*.

بنابراین، تجربه امنیتی بانکداری الکترونیکی بانک امگا مثبت بود زیرا درک واقعی از خطرات امنیتی در موفقیت کلی از امنیت بانکداری الکترونیکی، در گذشته، بدون هیچگونه شکست جدی در فرایند عملیاتی، نارسایی های قانونی و یا حملات موفقیت آمیز به سیستم، منعکس شده بود. اگر چه، بر حسب چگونگی منتشر شدن پیام های امنیتی خطر در واحد بانکداری الکترونیکی ، به دلیل ساختار بزرگ بانک گاهی اوقات مغرضانه بود. در واقع، از آنجا که فعالیت های واحد بانکداری الکترونیکی به وضوحی که واحد های دیگر از بانک دیده می شود نیست، در چگونگی انتشار، انتقال و تعبیه پیام تاخیر وجود داشت. بنابراین، از آنجا که فرایند ارتباطات در زمینه توسعه امنیت، مستلزم همکاری میان واحدهای مختلف بانکی است و گاهاً با به بن بست خوردن در یک واحد ، آنها نیازهای واحد های بانکداری الکترونیکی را نمی فهمیدند. در نتیجه، پیش می آمد که واحد بانکداری الکترونیکی باید فعالیت های امنیتی خود نظیر استفاده از نرم افزار جدید و مواد سخت افزار برای تعمیر و نگهداری و پشتیبانی را به تعویق اندازد. در زیر، برخی از استانداردهای ارتباطی دیگر و روش هایی که برای موفقیت در پذیرش امنیتی بانکداری الکترونیکی حیاتی است، تجزیه و تحلیل و ارائه گردیده که اینها را می توان به عنوان مثال برای بانک های دیگر استفاده نمود.

Organization flexibility

To provide flexible access, the Omega bank invested continuously in high technology and went through some organizational changes, the most important of which, the establishment of the e-banking unit as a separate banking unit with all the relevant resources dedicated for its purpose. In going web-enabled, the bank changed some of its business processes and departmental structures. The head of the IS/IT unit, in which e-banking was distinguished from but part of it, stated: *we first introduced e-banking and then followed the re-engineering of business processes.*

In effect, there were many processes that were totally integrated and automated such as deposit books at the customer's request, delivering cheques or transfer of money. However, that was not very effective since the re-engineering of business processes followed the introduction of e-banking rather than the other way round.

انعطاف پذیری سازمان

بانک امگا از طریق سرمایه گذاری مداوم در تکنولوژی قوی و برخی تغییرات سازمانی که از مهم ترین آن، استقرار و اختصاص تمام منابع مربوط به واحد بانکداری الکترونیکی به عنوان یک واحد بانکی جداگانه، به فراهم کردن دسترسی انعطاف پذیر پرداخت. بانک برخی از فرایندهای کسب و کار و ساختار دپارتمان را در وبسایتش تغییر داد. رئیس واحد فناوری اطلاعات، که در هر بخشی مشخصاً جدا است، اظهار داشت: ما اول بانکداری الکترونیکی را معرفی نموده و سپس به دنبال مهندسی مجدد فرآیندهای کسب و کار هستیم. در واقع، فرآیندهای بسیاری بنا به درخواست مشتری نظیر دفترچه حساب سپرده ، ارائه چک یا انتقال پول، به طور کاملا یکپارچه و خودکار درامد. اما از آنجاییکه مهندسی مجدد فرآیندهای کسب و کار بیش از همه راهها به دنبال معرفی بانکداری الکترونیکی بود، این فرایند زیاد موفق آمیز نبود.

Availability of resources

Availability of financial and human resources is critical in all types of development and maybe even more to security. In new technology development projects such as e-banking security, shortage of readily financial or human resources can be a main problem. The Omega bank got around this problem by implementing, with regard to human resources, an intensive and time frequent training program for new staff hired and with regard to financial resources, large amounts of investments on new technologies. However, problems to communication arrived often as a result of different political agendas from different banking units. In effect, project funding in the e-banking unit had been postponed for a short period of time, with a negative outcome on the co-ordination of security project activities in the context of e-banking. Different political agendas of other banking units, which required a larger 'share of the pie' led to communication break down among those units. An IT employee in particular said: *There are times where funding is not directed to the right direction since other units insist to ignore technology needs but I suppose that is because they find it difficult to adopt to changes*. As the communication process entails the cooperation of different banking units, those units were sometimes in a dead end as they could not understand the exact scope and needs of the e-banking unit.

در دسترس بودن منابع

در همه انواع توسعه در دسترس بودن منابع مالی و انسانی حتی شاید بیشتر از امنیت اهمیت دارد. . در پروژه های جدید توسعه فن آوری های مانند امنیت بانکداری الکترونیکی، کمبود منابع مالی و انسان می تواند یک مشکل اصلی باشد. بانک امگا با اجرای، طی یک برنامه فشرده و آموزش های مکرر برای کارکنان جدید الاستخدام در راستای منابع انسانی و سرمایه گذاری زیادی در فن آوری های جدید در راستای منابع مالی، اقدام به حل مشکل نموده است. . با این حال، مشکلات ارتباطات اغلب به عنوان نتیجه از برنامه های سیاسی مختلف در واحدهای مختلف بانکی نشات می گیرد. در واقع، تامین مالی پروژه در واحد بانکداری الکترونیکی با یک نتیجه منفی بر هماهنگی فعالیت های پروژه های امنیتی در زمینه بانکداری الکترونیکی برای مدت زمان محدودی به تعویق افتاده است. تفاوت برنامه های سیاسی که نیازمند توجه و تمرکز بیشتر نسبت به دیگر واحدهای بانکی است، منجر به قطع ارتباطات میان واحدها گردید. یک کارمند واحد فناوری اطلاعات به طور خاص گفت: گاهاً بودجه به مسیر درست هدایت نمیشود چرا که دیگر واحد ها اصرار به نادیده گرفتن نیازهای فن آوری دارند، اما من گمان می کنم برای آنها سخت است که تغییر را

بپذیرند. ، از آنجا که فرایند ارتباطات در زمینه توسعه امنیت، مستلزم همکاری میان واحدهای مختلف بانکی است و گاهاً با به بن بست خوردن یک واحد ، آنها محدوده دقیق و نیازهای واحد های بانکداری الکترونیکی را درک نمیکنند.

Security knowledge and awareness

In Omega bank, most of the interview participants exhibited full knowledge and awareness of e-banking security risks and it was mentioned that having held and equally shared information on security issues has a positive effect on communication and therefore on the overall success of e-banking projects. The Omega bank IT manager in particular expressed: *When the culture within the organization is strong – and consequently within the IS/IT department – the employees seem to accept the changes of activities more efficiently and in doing so, there is clarity in what we're trying overall to achieve. Certainly there are benefits of having a strong culture and these benefits are reflected in communication*. However, the Omega bank invested time and money on training seminars, which helped the employees to continuously upgrade their knowledge on security issues.

دانش امنیت و آگاهی

در بانک امگا، بسیاری از شرکت کنندگان در مصاحبه، دانش و آگاهی کاملی از خطرات امنیتی بانکداری الکترونیکی را عرضه کردند که در آن سهم تقسیم مساوی اطلاعات و اثر مثبت آن بر ارتباط و در نتیجه بر موفقیت کلی پروژه های بانکداری الکترونیکی ذکر شده بود. مدیر فناوری بانک امگا به طور خاص ابراز داشت: هنگامی که امنیت در سازمان– و به تبع آن در بخش – قوی باشد به نظر می رسد کارکنان موثر تر تغییرات را پذیرفتند و در انجام این کار و آنچه که ما در حال تلاش برای رسیدن به آن هستیم، تلاش می کنند. قطعا داشتن یک فرهنگ قوی مزایایی وجود دارد که این منافع در ارتباط منعکس هستند. با این حال، بانک امگا زمان و پول زیادی را در سمینارهای آموزشی سرمایه گذاری کرد و به کارکنان کمک کرد تا دانش خود را در مورد مسائل امنیتی بطور مداوم به روز رسانند.

Support from top management

Support and understanding either ethical or financial from top manage-ment is a basic requirement for successful completion of e-banking projects (Turban *et al*, 2000). The top bank executives from the strategic level of the hierarchy proposed a bonus motivation scheme on project completion on time. That enabled more cooperation among employees to achieve e-banking project goals within the predetermined time frames. The support analyst stated: *since the bank introduced this bonus scheme, the projects were finishing on time and were more efficiently managed*. This bonus scheme introduced in Omega bank had an ultimate effect on communication since the employees were taking more seriously project needs and requirements.

پشتیبانی از طرف مدیریت ارشد

حمایت و درک اخلاقی یا مالی از مدیریت ارشد یک نیاز اساسی برای تکمیل موفقیت آمیز پروژه های بانکداری الکترونیکی است (Turban et al, 2000) . مدیران ارشد بانک یک جایزه انگیزشی برای زمان اتمام پروژه طرح کردند که موجب گردید همکاری بیشتر میان کارکنان در جهت دستیابی به اهداف پروژه بانکداری الکترونیکی در چهارچوب جدول زمانبندی از پیش تعیین شده را به وجود آورد. یک تحلیلگر پشتیبانی اعلام

کرد: از زمانیکه که بانک این طرح پاداش را مشخص کرد ، پروژه ها به موقع و کارآمد تر اداره و تمام شدند از آنجا که کارکنان نیازها و الزامات پروژه را به طور جدی تر در نظر گرفتن بودند، این طرح پاداش معرفی شده در بانک امگا تاثیر بسزایی در ارتباطات داشت.

e-Banking project alignment

Although security is a sensitive and confidential issue, most employees in Omega bank were participating in e-banking planning and development, and in a way because of the previously mentioned bonus scheme, the coordination and clarity of specific project goals were improved. This outcome was a consequence of better communication within the banking units, which led to more efficient project alignment. The IS/IT deputy manager stated: *if you do not have good communication on security planning and development in terms of how the risk messages are formulated, transmitted and circulated, e-banking security will be misinterpreted*.

تراز پروژه بانکداری الکترونیکی

اگر چه امنیت یک مسئله حساس و محرمانه است، بیشتر کارکنان در بانک امگا در برنامه ریزی و توسعه بانکداری الکترونیکی شرکت کرده بودند، و به دلیل طرح پاداشی که قبلا ذکر شد، هماهنگی و وضوح اهداف پروژه بهبود پیدا نمود. نتیجه، توالی ارتباط بهتر در واحدهای بانکی بود که منجر به تراز دلخواه برای پروژه ای کارآمد تر شد. معاون مدیر فناوری اظهار داشت: اگر شما در برنامه ریزی امنیت و توسعه در شرایط چگونگی فرموله شدن، منتقل شدن و منتشر شدن پیام خطر، ارتباط خوب نداشته باشید، امنیت بانکداری الکترونیکی بد تعبیر خواهد شد.

Information transparency

In Omega bank a continuous effort was given to avoid different political agendas among the banking units and that there will be a continuous flow of information from higher levels of the hierarchy to lower and vice versa without any obstacles in the communication process. That was achieved to a certain degree through the intervention of top management in dead-end times and where confusion was starting to take place among different banking units. An IT employee said: *Although there are problems of communication and misunderstanding between different* peop*le among different units, the strong organizational culture of Omega bank does allow for problems to take over final project decisions. In effect, at the right time confusion is being avoided*. In addition, the culture of Omega bank enabled its employees to exchange information among each other in order to succeed as a team.

The success of risk communication is limited because of the insufficient attention it pays to social contexts within which individuals live and communicate (Otway and Wynne, 1989). In addition, it should be considered that the parties sending the messages may not always be honest, reliable, as well as responsible (Otway and Wynne, 1989).

The manner in which people and particularly employees see the risks associated with information security determines what decisions they will make regarding the actions they will take or not, in relation with whatever risk security measures their organization has put in place. This research further examines e-banking security from a communication perspective through a holistic approach, that is: integrate technology, people and processes. In doing so, this research investigates: (1) *what is the experience of organizations following e-banking security measures*

and controls as part of the security management procedures, and (2) *what are the communication standards and procedures which are critical to the success in e-banking security adoption?*

شفافیت اطلاعات

در بانک امگا تلاش های مداومی برای جلوگیری از بروز برنامه های سیاسی مختلف در میان واحد های بانکی وجود داشت و آن یک جریان پیوسته از اطلاعات را از سطوح بالاتر سلسله مراتب به پایین و بالعکس بدون وجود هر گونه مانع در فرایند ارتباطات بود. که از طریق مداخله مدیریت برتر در برابر بن بست به وجود آمده که موجب بروز هرج و مرج در میان واحد های مختلف بانکی میشود به یک نظم خاص برسد. یک کارمند فناوری گفت: اگر چه مشکلات ارتباطات و سوء تفاهم بین افراد مختلف در میان واحد های مختلف وجود دارد، لذا تصمیمات نهایی پروژه و فرهنگ قوی سازمانی بانک امگا به مشکلات اجازه می دهد که از پس آن بر آید. در واقع، در زمان مناسب از بروز سردرگمی اجتناب مینماید. علاوه بر این، فرهنگ بانک امگا به منظور موفقیت کار تیمی کارکنان خود را قادر به تبادل اطلاعات میان یکدیگر میسازد. از آنجاییکه به زمینه های اجتماعی که هر فرد در آن زندگی می کنند و ارتباط برقرار می کند توجه کافی میشود، موفقیت در ارتباطات خطرناک محدود است (Otway and Wynne, 1989) . علاوه بر این، باید در نظر گرفته شود که احزاب ارسال پیام ممکن است همیشه صادق و قابل اعتماد، و همچنین مسئول نباشند (Otway and Wynne, 1989) . شیوه ای که مردم و به ویژه کارمندان خطرات مرتبط با امنیت اطلاعات را میبینند، با توجه به اقدامات آنها تعیین میکند که چه تصمیماتی را اتخاذ نموده یا نمیکنند، در رابطه با هر خطر امنیتی جایگاه سازمان خود را اندازه گیری میکنند. این تحقیقات بیشتر به بررسی امنیت بانکداری الکترونیکی از دیدگاه ارتباط از طریق یک رویکرد جامع که: ادغام تکنولوژی، مردم و فرآیندها است می پردازد. در انجام این کار، این تحقیقات انجام پذیرفته است: (1) سازمان چه تجربه ای از اقدامات امنیتی بانکداری الکترونیکی و کنترل به عنوان بخشی از روش های مدیریت امنیت دارد و (2) استانداردهای ارتباطات و روش هایی که برای موفقیت در پذیرش امنیت بانکداری الکترونیکی حیاتی هستند چه هستند؟