Issues in Information Systems
Volume 14, Issue 1, pp.286-299, 2013

ASSESSING THE IMPACT OF GOVERNMENTAL REGULATIONS ON ORGANIZATIONAL COMPETITIVENESS : AN ANALYSIS USING NEO INSTITUIONAL THEORY

Amita Goyal Chin, Virginia Commonwealth University, amita@saturn.vcu.edu
Sushma Mishra, Robert Morris University, mishra@rmu.edu

ABSTRACT

Given monumental events including the September 11th attack on the World Trade Center and the Pentagon as well as the Enron and MCI Worldcom debacles, people have witnessed, and more readily accepted, a significant increase in governmental authority, leading to a dramatic upsurge in the number of governmental regulations imposed on business organizations and society. This manuscript presents an analysis for understanding the implications -- both technical and managerial -- of such regulations on the IT industry. Using neo institutional theory as a theoretical basis, this manuscript examines the repercussions of governmental regulations, which have become strong institutional forces, on the IT industry. The analysis suggests that such significant institutional forces may gravitate an otherwise highly disparate IT industry towards industry wide homogenization. Three examples of published case studies are used to demonstrate the impact of the regulations on the IT industry.

Keywords: Neo Institutional theory, Organizational change management, regulatory environment, governmental regulations, SOX, HIPAA and GLB

INTRODUCTION

IT infrastructure, processes, and security have been thrust to the forefront due to catastrophes such as the September 11th attack on the World Trade Center and the Pentagon, illegal corporate activities, identity theft, and cyber crime. A plethora of governmental regulations have successfully been passed to tighten organizational processes and security. Regulatory mandates such as Sarbanes-Oxley Act (SOX), USA Patriot Act, Gramm-Leach-Bliley Act (GLB), and Health Insurance Portability and Accountability Act (HIPPA) act as catalysts for applying due diligence in the organizational use of information technology (IT). As a process and as a product, IT has to be used within the confines of the regulations shaping the industry. These regulations hold business organizations unmistakably accountable, with serious consequences, including fines and imprisonment, for noncompliance. While all such legislation may not directly be aimed at corporate IT, the pervasive presence of information technology along with the indisputable gravity of these governmental regulations has forced most business organizations to revisit and subsequently revamp their IT infrastructure and processes in order to achieve legislative compliance.

Historically, the IT infrastructure within IT-oriented as well as non-IT-oriented organizations has been largely disparate. Perhaps this is a consequence of the unprecedented rapid advancement of the industry and the inability of the legal, social, and cultural forces to maintain pace. The IT industry altogether has significantly suffered due to the lack of both an orthodox organizational infrastructure and a robust methodology of processes. The introduction of the multiple, industry-wide governmental regulations and the necessary subsequent corporate restructuring may gravitate the IT industry as a whole toward a standardization and homogeneity which has traditionally been sorely lacking. Neo institutional theory [18] provides a theoretical basis using which we are able to analyze and comprehend the behavior of particular organizations with respect to the industry of which they are a component. Today's IT-oriented organizations in particular are exposed to various institutional forces, a prominent one of which is governmental regulations. Using the neo institutional theory perspective, we suggest that IT organizations, which traditionally are not standardized in structure, form, or method of operation will, in the face of the institutional forces to which they are exposed, begin showing considerable similarity and standardization industry wide. Furthermore, the specific choice of information technology implemented for infrastructural organizational support will be impacted more by the mandates of these governmental regulations than by the hype of the proprietary technology products or processes used.

Setting the stage to investigate the impact of regulatory forces on the information technology industry, we present a brief discussion of three very significant governmental regulations that have been mandated of the IT industry and their considerable impact and implications on information technology, both from a technical and from a managerial

perspective. Employing neo institutional theory as the underlying theoretical basis, we analyze the impact of the abundance of governmental regulations being imposed on the information technology industry. The conceptual analysis suggests that these regulations are migrating organizations in the IT industry to uniformly conform and implement standardized infrastructures, processes, and practices

The remainder of this manuscript is organized as follows: Section two presents three major regulations that are currently influencing the IT industry and discusses some plausible impacts of these regulations on the IT domain. Section three presents the neo institutional theory, including its basic tenets as well as a review of previous research that has applied the neo institutional theory specifically to the information systems discipline. In Section four, an analysis is presented in which the neo institutional theory is used to explain the similar, industry-wide organizational and technological repercussions resulting from the governmental regulations on the IT industry. To further validate the claims, an example of three case studies in the context of each of the legislation is presented. Finally, Section five summarizes the contributions of this work and suggests future research directions.

GOVERNMENTAL REGULATIONS

The past decade has witnessed the injection of an abundance of governmental regulations into the business world. This manuscript discusses the details of three such regulations – SOX, HIPAA, and GLB. These legislations were specifically chosen because of their significant impact on organizational resources and the considerable implementation challenges that they present for the IT industry.

Sarbanes-Oxley Act (SOX)

In the aftermath of the Enron and MCI WorldCom fiascos, the Sarbanes-Oxley Act (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, was enacted in response to public anger with accounting fraud and corporate governance and reporting failures, and protects investors from fraudulent reporting by corporations [39]. SOX, applicable only to public traded companies, mandates that companies employ stringent policies and procedures for reporting financial information accurately.

SOX includes eleven titles, each of which contains multiple "Sections," which itemize the mandatory requirements [49]. Several of these sections have grave implications for key corporate executives, including the CEO, CFO, and CIO. Perhaps the most serious of the SOX sections are Sections 302 and 906, which require signatures from the CEO and the CFO attesting that the information provided in the company's quarterly and annual reports is authentic and accurate [52]. Furthermore, these key company executives bear the responsibility for any inaccurate representation of the reports, whether or not they possessed a priori knowledge of such errors. Section 906 holds CEOs, CFOs, and corporate directors both accountable and liable for the accuracy of financial disclosures. Unlike Section 302, Section 906 penalizes officers only if they know of a possible problem or error when certifying a report [30]. Sections 103 and 802 specify audit record retention and security requirements [30].

Section 401 requires the company to disclose not only balance sheet transactions, but also additional transactions that are not normally shown on the balance sheet. All arrangements, obligations (including contingent obligations) and other relationships that might have a material current or future effect on the financial health of the company [30] must be divulged. Section 401 restricts the use of pro forma information and directs companies to represent financial information in a manner consistent with generally accepted accounting principles (GAAP).

Section 404 requires that executives attest not only to the company's financial statements, but also to the control processes for the collection of the data supporting the financial statements [25]. Section 409 requires real time disclosure of financial and operating events, requiring companies to disclose any events that may have material impacts on their financial condition or operations on a rapid and current basis [52]. Technological progress may soon define "rapid and current basis" to be within 48 hours following the occurrence of an event. Compliance with Sections 404 and 409 requires that each step in a business transaction -- order, payment, storage of data, aggregation into financial reports, etc. -- must be audited, verified, and monitored.

Section 802 requires the retention and protection of corporate records and audit documents and expressly includes e-records in the mandate [28]. This Section institutes criminal penalties for unauthorized document alteration or destruction.

Impact on the Information Systems Domain

Complying with SOX has proven to be both complex and expensive for organizations. "In an annual survey of compliance, in IT by businesses, the estimated cost of compliance for year 2006 is more than $6.0 B, almost equal to the amount spent in 2005 which is $6.1 B [27]." SOX significantly depletes organizational resources [7] and forces organizations to reevaluate IT governance practices [23], since both managerial and technical commitment is required to create the organizational infrastructure necessary for compliance. This means that management must establish and exercise considerable internal control assessment measures -- quarterly reporting, security policies, cost management, and external audits -- in order to be prepared to cope with the demands of SOX.

Table 1: Impact of Legislations on the Information Systems Domain

Legislation	Impact on Information Systems Domain	
	Technical	**Managerial**
Sarbanes-Oxley Act (SOX)	▪ Database Systems (data integrity, data quality, database architecture) ▪ Software development methodologies ▪ Security ▪ Versioning and auditing of electronic record retention ▪ Extensive documentation	▪ IT Governance (effective internal control) ▪ Systems Audit ▪ Quarterly reporting ▪ Cost management ▪ Policy evaluation
Health Insurance Portability and Accountability Act (HIPPA)	▪ Data Security ▪ Data integrity ▪ Transaction processing ▪ Disaster recovery ▪ Real-time data access ▪ Encryptions and authentication ▪ Network communications	▪ Privacy policy for health information access ▪ Audit control planning ▪ Privacy policy implementation at all information collection points
Gramm-Leach-Bliley Act (GLB)	▪ Web privacy ▪ Significant security safeguards	▪ Ensure no information leak to third parties ▪ Detailed privacy notice to customers and opt out plans

Some technical issues that must be revisited and subsequently modified due to the enactment of this regulation include: data management ([52],[53],[22]), including data and systems security [8]; software development methodologies, which must now incorporate compliance issues as a component of the development lifecycle [37]; and documentation and record keeping, which must now be strengthened to include versioning and audit capability [41], [52].

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA safeguards the privacy of medical records of patients by preventing unauthorized disclosure and improper use of patients' Protected Health Information (PHI). With a significant emphasis and monetary investment in the 1990s on the computerization of health services operations, the possibility of data manipulation and nonconsensual secondary use of personally identifiable records has tremendously increased [5]. HIPAA declares PHI "privileged," protecting individuals from losses resulting from the fabrication of their personal data. Businesses subjected to

HIPAA are directed to protect the integrity, confidentiality, and availability of the electronic PHI they collect, maintain, use, and transmit.

Three major components of HIPAA are:

- Privacy: the privacy of individuals' health information in written, oral and electronic form must be protected. Health information includes medical records, claims, and payment information, and almost all additional information related to patient health care.

- Security: private information of individuals must be kept safe from damage of any kind. The purpose of this clause is to protect electronic patient information from alteration, destruction, loss, and accidental or intentional disclosure to unauthorized persons.

- Transaction: various participants in the healthcare industries must effectively and electronically communicate patient information. Successfully meeting this requirement necessitates that privacy and security covenants also be met.

Impact on the Information Systems Domain

The cost of compliance with HIPAA to healthcare organizations, just for 2002, was $270 million [40]. Compliance with HIPAA is not just a matter of technical products ensuring safe and secure data collection, transaction, and storage; rather, compliance is an issue of "organizational change management." It requires instituting new structures and patterns for health care companies to coordinate efficiently, trust other's intentions, and responsibly maintain and protect sensitive data [28]. Success depends on how well each organization develops a "management infrastructure with well defined roles that will address administrative, physical, and technical safeguards [34]" HIPAA compliance requires companies to constantly evaluate and test their internal controls over all business units and functional areas [22]. Additionally, organizations must provide audit trails which are subject to external evaluation [41], implement proper planning, institute privacy policies [34], and ensure controls in all data access points [34].

HIPPA impacts healthcare organizations at the basic infrastructure level, thus demanding reevaluation at all levels, including the creation and implementation of technical solutions. Employing and adapting to technical solutions requires not only proper planning but also an overhaul in organizational processes. Data integrity [34], data security ([28], [38]), transaction processing ([28]; [41]), real time accessibility [41], encryption and authentication techniques [33], network communications [28], and disaster recovery techniques must all be investigated and modified in order to guarantee private patient data storage and interchange.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley (GLB) Act, or the Financial Services Modernization Act of 1999, proposes regulations regarding the scope and interrelationships, particularly with respect to consumer privacy, of key financial industries -- insurance, securities, and banking. (Prior to GLB enactment, the Glass-Steagall Act guided these industries.) Given the increased and tremendously heavy dependence on information technology to store, manipulate, and use data, maintaining the sanctity of consumer data and customer relationships has become of paramount importance. GLB requires that companies which engage in financial activity must respect the privacy of customer data and undertake such measures as are necessary to protect the data while in organizational care, custody, and control.

GLB authorizes eight federal agencies and all States to enforce three major rules regarding financial privacy, the safeguarding of personal information, and pretexting:

- Financial Privacy: The Privacy Rule requires that organizations that engage in financial activity provide customers copies of their privacy policy and explain their practices on sharing customer information.
- Safeguarding of Personal Information: The Safeguards Rule requires organizations protect the confidentiality and integrity of personal consumer information, and design, implement, and maintain the necessary security processes. This rule applies not only to the financial institutions which are primarily responsible for collecting this information from customers but also to all secondary users of this information, including credit rating agencies which receive this information from financial institutions.

- Pretexting: This provision of the GLB Act protects consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."

Impact on the Information Systems Domain

GLB requires organizations to engage in financial activities such as preparing tax plans, providing customers the company privacy policy, and explaining corporate practices in sharing customer information [9]. The implications for IT from a technical perspective are manifold. Under GLB, compliance requires state-of-the-art expertise in hacking, malware, and social engineering [9]. This law has implications for upper management including the CIO, making him/her personally responsible for any oversight of compliance. Furthermore, under GLB, issues such as the absence of risk assessment, the absence of safeguards to control risks and failure, and the absence of service contracts for security standards would hold management accountable. That is, the CIO is required to be personally responsible for any compromise to the privacy of customer information.

There are multiple implications of the GLB for the CIO and the company IT department. Under GLB, companies need to have expertise in dealing with hacking, malware, and social engineering. These are not skills over which the typical CIO has knowledge or mastery [9]. Therefore, a distribution of authority for administration and enforcement becomes necessary in order to comply with this law. With the GLB, organizational obligations to protect consumer privacy and the requirement to completely and accurately disclose the organization's policies become mandatory. GLB holds the CEO, the CIO, and the IT management responsible for safeguarding the public's interest.

NEO INSTITUTIONAL THEORY

We use the concepts of the neo institutional theory to understand the impact of institutional forces on the IT industry. In this section, we present first a brief introduction to neo institutional theory, and then, a review of research that specifically applies the neo institutional theory to the field of information systems.

Background

Researchers ([35]; [18]) of neo institutional theory focus primarily on the cause and implications of the observation that organizations in the same line of business, or industry, appear similar in their form and structure. Neo institutional theory provides a means by which to understand deeper and resilient aspects of social structure. It considers the processes by which structures, including schemas, rules, norms, and routines, become established as authoritative guidelines for social behavior [45]. It inquires into how these elements are created, diffused, adopted, and adapted over time. Scott (2004) argues that this theory also provides insights into conflict and change within social structures.

According to neo institutional theory, organizational decision-making always occurs in the context of social political institutions. Meyer and Rowan (1977) claim that organizations do not rationally structure and organize their processes in response to environmental pressures; rather, they tend to respond in a similar manner to the same social forces to which they are exposed, thus developing similarity in both structure and form. This process of homogenization is called isomorphism [18]. "[I]somorphism is a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions ([18], pp.66). Institutional isomorphism may be categorized in the following ways:

Coercive isomorphism: Results from both the formal and informal pressure that is exerted upon a business enterprise from organizations upon which this business enterprise is dependent. Coercive isomorphism also refers to pressures from the society in which the business enterprise functions, particularly in the form of political expectations (e.g., governmental regulations). DiMaggio and Powell (1991) argue that the existence of a common legal environment does affect the behavior and structure of organizations, for it forces them to behave and operate in a manner that adapts to such legal requirements. Thus, the presence of overarching regulations tends to provide a common structure and conformity industry wide. As organizations grow in size and dominance in different areas of social life, coercive isomorphism reflects structures that are legitimated and institutionalized by government ([35], [18]). This results in the homogenization of organizations in a given domain.

Mimetic isomorphism**:** DiMaggio and Powell (1991) argue that not all intra-institutional isomorphism occurs as a result of coercive forces. Uncertainty in task as well as the institutional environment promotes the imitation of

actions within organizations. When their own goals are even somewhat ambiguous, organizations tend to model themselves after similar organizations within their own industry that they perceive to be more socially accepted and successful in economic terms, and that have successfully dealt with such uncertainties. Benchmarking or role modeling responses based on other organizations not only provides a concrete model for an organization to imitate, but also provides the organization a way to respond to uncertainty in a seemingly less risky way. Therefore a level of homogeneity results within organizations with similar business uncertainties and institutional complexities.

Normative isomorphism: The origin of normative isomorphism lies in the concept of professionalization, which is defined as "the collective struggle of the members of an occupation to define the condition and methods of their work [18]" so that there is a clear, established cognitive base and legitimization for occupational autonomy. The established norms and behavior for a profession tend to shape all of the professionals entering that profession in a similar way, thus creating an isomorphic pattern for the professionals. Two sources of normative isomorphism are generally identified: formal education and professional networks. In has been observed [47] that "schools, colleges and universities are among society's major agents of socialization," providing legitimization in a cognitive base, which is produced by university specialists. Professional and trade associations are also important vehicles for creating and enforcing normative rules and laws.

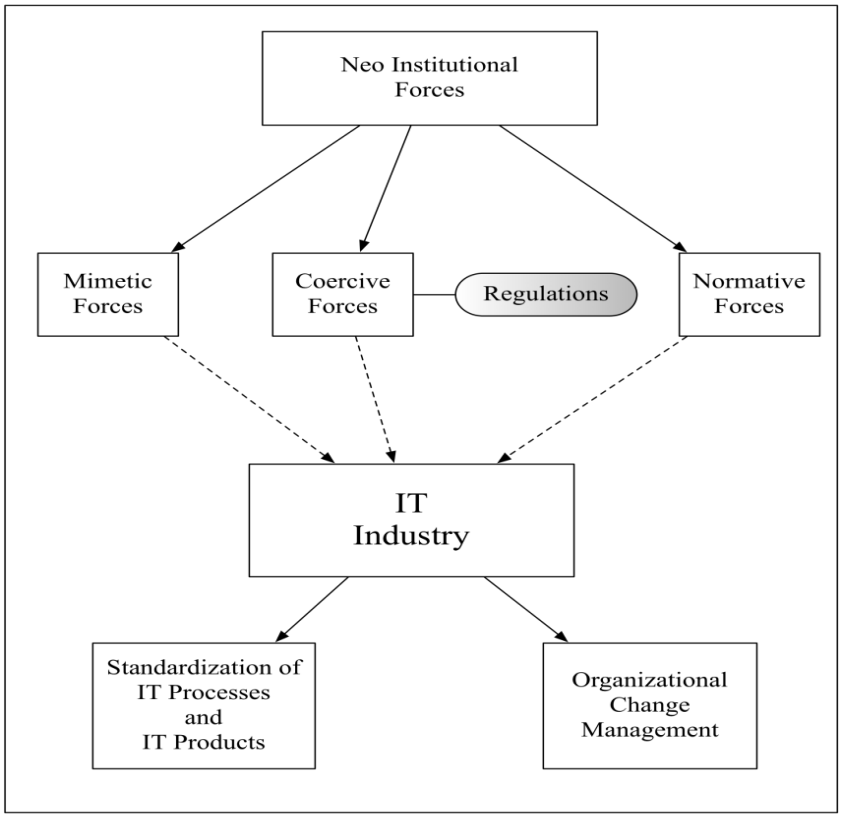

Figure 1: Impact of regulation on IT Industry

In any institutional system, the above factors are altogether present, interacting and promoting orderly behavior across an industry (see Figure 1). However, the research in this area tends to emphasize one factor over another, depending on the problem that is being addressed and the particular perspective of the researcher(s). As Scott (2005) observes, "economists stress regulatory factors, political scientists and early sociologists [stress] normative factors, while recent sociologists, anthropologists, and cognitive psychologists emphasize cultural-cognitive factors (pp. 135)."

Neo institutional theory by no means suggests that organizations would not vary in their responses to institutional forces or would not attempt to shape such forces according to their own needs. Research in the healthcare industry has used the neo institutional framework extensively to study the impact of various regulations in shaping the management of hospitals. As Alexander and D'Aunno (2000) observed, "this interplay between broader context and inter-organizational dynamics explains the variation in which corporatization expresses itself within the health care sector (pp. 51)." Neo institutional theory argues that over a period of time, the presence of strong institutional forces homogenizes the overall response of the collection of organizations that operate within a similar industry.

Previous Research

The information systems (IS) discipline lacks good theories [42], and therefore, routinely borrows theories from other disciplines. While the neo institutional theory has previously been used in information systems, the applications have been limited to only the organizational level. Research within the IT industry has focused primarily on the micro level analysis of inter-organizational conflicts.

Applications of neo-institutional theory have been seen in a range of situations. Research in healthcare has used the institutional framework extensively to study the impact of various regulations in shaping hospital management such as impact of HIPAA on information security [3]. Bj¨orck (2004) suggests that neo institutional theory will prove to be a valuable tool for analyzing IT problems, for this theory teaches us about the management of IT security in organizations. The theory helps to understand and explain the discrepancy between formal security structures and actual security behavior. Also, neo institutional theory sheds light on why organizations often create and maintain formal security structures without trying to implement them fully [10]. Abraham and Chengalur-Smith (2011) used neo institutional theory to understand how multiplicity of views impacts the design and implementation of security policies. Benders, Batenberg and Blonk (2006), using the neo institutional theory framework, argue that the use of ERP systems may lead to a standardization within and between organizations and that institutional pressures play a significant role in ERP adoption. They call it "technical isomorphism." Using a framework from DiMaggio and Powell's (1983) article on structural isomorphism, Chiravuri and Ambrose (2002) analyze organizational downsizing and its effects on certain aspects of competence in the IT departments. Chiravuri and Ambrose (2002) reason that organizational downsizing occurs because of coercive forces, i.e., there is a pressure on organizations to act in a particular way. There could also be mimetic forces acting on organizations such that they can remain competitive. Finally, organizations may face normative pressure to downsize as key persons in important managerial positions believe in downsizing.

Software development is a highly uncertain, highly interdependent, and highly complex task. Adler (2005), studying the Software Engineering Institute's Capability Maturity Model (CMM®) for software development, uses institutional theory to focus on the symbolic dimensions of the created object. He concludes that adherence to the CMM is a symbolic conformance to established standards. The task organization process is not merely technical in nature but also symbolic, i.e., to ensure the legitimacy of its operations in the eyes of the stakeholders [2]. Thus when software development organizations adopt the CMM, this adoption signals a step towards conformance of CMM standards and hence gains legitimacy.

Jones, Orlikowski, and Munir (2004) argue that the broader institutional influences -- such as political, industrial, economic and global -- that shape IT phenomenon have largely been ignored in IT research. There is some awareness to have industry wide common benchmarks and practices that could lead to the standardization of the industry; however, this is primarily done by practitioners rather than by academicians. The creation of maturity models [24], governance standards such as the Control Objectives for Information and related Technology (COBIT), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO), are all examples of these endeavors [30]. But academic researchers are lagging behind in undertaking such institutional level research and creating a research agenda in this area. King et. al. (1994) argue that the lack of a coherent protocol for the creation of government policy for IT innovation signals a shortfall in the understanding of the vital role of government institutions in the IT innovation process. Governmental regulations in developing nations are geared towards the acceleration of IT innovation within their national boundaries. Robey and Holmstrom (2001) studied the implementation of a governance support system in a government organization in Sweden and analyzed the implications of the use of this technology at the organizational as well as at the institutional level. Their study

concluded that by focusing on both the organizational and institutional levels simultaneously, a comprehensive understanding of the global forces shaping the organizational and societal changes is achieved.
Many organizations have acquired IT products just to be a part of IT "fashion" (Akhlaghpour et al., 2010 in Safadi and Faraj, 2011). Even though there is no higher performance associated with acquiring latest IT solutions however sich IT fashionable companies tend to have better reputation and higher executive compensation in the short term [54]. "Health IT fashion" is quite common in healthcare organizations. Indeed, institutional change in healthcare is sometimes induced by legal requirements, economic incentives and competition. While it is understood that organizations seek to attain legitimacy by adopting new practices and norms [18], it can be problematic particularly in the context of health IT because mindless implementation of technology will limit and even inhibit its promised advantages (Safadi and Faraj, 2011). Institutional settings can create a conducive (or restrictive) atmosphere that determines an organization's behavior in its market. Wickramasinghe et al (2012) argue that understanding the interactions and the institutional context is important, particularly in complex knowledge intensive settings, such as healthcare and e-health as it can help deepen current understanding concerning ensuing strategic behaviors of stakeholders. The researchers conclude that the development of pervasive e-health solutions may be better understood with a full examination of the institutional setting where organizations interact in attempts to achieve their objectives.

While research in information systems has used the neo institutional theory to study a variety of problems, the level of analyses is organizational in nature. In spite of the impact of the various institutional forces on IT related tasks, and the attempts of organizations to mimic certain practices in the IT industry, there exists a scarcity of IS research which examines the IT industry as the unit of analysis.

AN ANALYTICAL DISCUSSION

While mimetic and normative forces also play an important role in shaping industries, the main emphasis of this manuscript is to understand the impact of regulatory forces, a prominent coercive force, on the IT industry (see Figure 2).

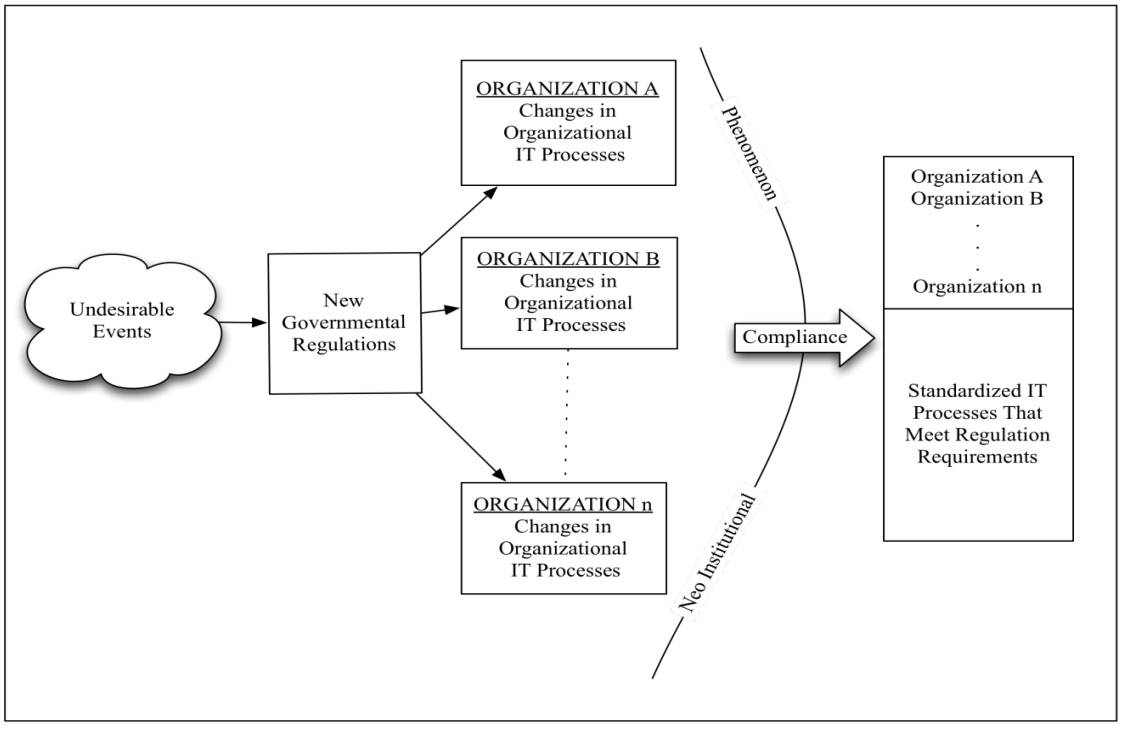

Figure 2: Regulatory environment and standardization of IT

Institutional forces on the IT industry

Neo institutional theorists have provided evidence that many modern organizational characteristics have their origins in public policy. The legal environment has become more pervasive, especially for the IT industry. Edelman and Suchman (1997) describe the regulatory environment for organizations as a world where "law appears as a system of substantive edicts, invoking societal authority over various aspects of organizational life (pp. 483)." The legal system, on behalf of society, takes the initiative to control organizational behavior. Some researchers, on the other hand argue that, a regulatory environment often merely institutionalizes the indigenous practice of the regulated population [19]. According to neo institutional theory, regulations are one of the many institutional agents that influence the broader environment of an industry. Depending on the seriousness of such institutional forces, organizations have to either initiate or follow other organizations to institute changes.

DiMaggio and Powell (1988) assert that "bureaucratization and other forms of homogenization are affected largely by the state and the profession, which have become the great rationalizers of the second half of the twentieth century (pp. 147)". The state exerts coercive pressure on the organizations to adapt their structures to institutionalized forms. The IT industry is facing strong institutional forces, in the form of an ever-changing regulatory environment, which will impact future years. Institutional forces on the IT industry thus far have primarily been limited to governmental regulations, but as organizations begin adopting the changes required by these regulations and begin internalizing such changes, an incremental impact of additional institutional forces -- mimetic and normative -- will occur (see Figure 1).

The Standardization and Commoditization of IT

The IT industry may be conceptualized as an organizational field since it comprises a heterogeneous network of parties with a variety of tangible and intangible interests [14]. Information Technology as an industry is immature, highly fragmented, and non-standardized. Most organizational tasks, ranging from the simple to the highly complex, may be accomplished using a wide variety of solutions. Each organization chooses different solutions to solve the same tasks, oftentimes even developing hybrid solutions, all resulting in inconsistent and incompatible systems. This disparity is further heightened with the vastly varying methods of securing informational assets that are employed by organizations, the diverse systems development practices followed, the different underlying data models implemented in databases, etc. Such behavior has rendered any collaboration efforts as arduous, often unachievable endeavors and resulted in an industry plagued with ad hoc, band-aid solutions to many common problems. Clearly, a necessity for the standardization of IT practices across the industry has emerged.

Organizations view compliance with regulations as an opportunity to improve their business processes and start new ways of enhancing business. For instance, according to an Ernst and Young survey, compliance with regulations is the most influential driver that has significantly affected or will affect organizations' information security practices [21]. Many organizations believe that standards in IT industry such as in security related matters are beneficial as such standards allow these organizations to convince their clients of their commitment [21].

The regulatory forces are driving IT organizations towards a direction that ensures the standardization of processes, products and practices. The pressure from the institutional environment could lead to the standardization of operating procedures in order to gain legitimacy [57]. Institutional statements that neither demand nor prohibit a particular behavior promote heterogeneity of action [13]. In sociology, institutions are perceived as models, schemas or scripts for behavior and are understood as models that provide substantive guides for practical action [13].

In order to show conformity, IT organizations can gradually achieve similar standards across the industry, resulting in an unprecedented homogeneity of this industry. From the perspective of neo institutional theory, society exerts pressure on business environment to follow certain broad guidelines, and regulations are an attempt to standardize the environment and show conformity to societal rules.

Regulations are serving as the impetus for the standardization of the IT industry. Any such standardization effort would require technical as well as managerial support in order to institute changes. The commoditization of IT would result in providing a standard usage of similar IT products and processes. In situation of uncertainty, organizations may be able to achieve legitimacy by following the collective action of other organizations and the "best practices" adopted by other similar organizations [18].

Organizational Change Management

From the neo institutional theory perspective, the current state of the IT industry, with increasing regulatory interventions, is an unmistakable signal for organizations to become prepared to change their current IS practices. Institutional forces, such as regulations, are becoming stronger over time and are gradually standardizing the industry by compelling organizations to change in a uniform manner. In the process of complying with new laws, IT organizations are streamlining their processes with better security measures, following standard development methodologies, adopting similar governance frameworks, welcoming audit practices, emphasizing internal controls, and are migrating towards similar forms and similar structures.

Even though technical needs of the organization seem to be the main driver of various changes instituted in business process, within a given institutional filed, the symbolic needs tends to overcome the technical needs and lead the organizational change process [2]. IS plans do not compensate for weak or disputed organizational change orientation [4]. Change management as an initiative has to be performed simultaneously to reap the maximum benefits of the exercise. When organizational change management is not well planned, all the improvised efforts to harness IT for organizational change are likely to be erratic. Yet, IT innovation tends to intensify rather than being held accountable for organization transformation results [4]. Institutionalization helps in adopting and maintaining a change because of its acquired legitimacy, irrespective of whether or not it produces its promised technical value [4]. Changes brought into business processes (see Table 1) due to various regulatory forces would be gradually adopted into organizations. As belief systems and norms vary over time and place, institutional concepts provide a means to study organizational emergence and change.

Organizational responses to institutional forces depend on several factors that are internal to an organization, such as the political environment, the culture [26], the resources available, etc. Organizational responses to external environmental pressures may be drastic, abetting the organization in adopting radical changes, or such responses may be gradual, leading to the adoption of small changes. The mode of response of organizations may be different, however, the stringent and pervasive nature of such regulations is forcing organizations to revisit their IT management techniques and prepare their functions for adaptive behavior.

CASE STUDIES

Many strategies have been used by organizations for successful compliance, such as frequent internal audit and security monitoring, investing around 30% of the time in IT compliance and spending 10 % of the IT budget on security efforts [49]. This section presents a brief description of three organizations that successfully been making many fundamental changes to comply with regulations. The lessons learned from these cases are discussed.

Case 1: HIPPA Compliance

Lake Forest hospital, a small hospital in Illinois, had a poor network infrastructure and tracking patient information was open for everyone. The responsibility of ensuring unauthorized disclosure was placed on the clinicians. HIPPA compliance regulations forced the organization to secure their networks and to prevent unauthorized access to patient data. The hospital's decision to move to a single network was among the most valuable decision it made in terms of compliance. The hospital network developed the capability of logging data from within its firewalls, servers and other network devices. Having logging features in place positioned it to meet HIPAA's logging requirements. The hospital deployed Microsoft's Active Directory to make applications available only to authorized users.

HIPPA regulations necessitated new capital expenditures in the storage facility of digital information. HIPAA mandated that the hospital "devise a policy on how to handle and store everything from fetal heart strips to mammograms." The hospital implemented a solution of EMC's Clariion CX500 and Cisco System's Storage 9216i switches. In the future, the hospital plans to virtualize its servers and to create a redundant data center at a second campus with the ultimate goal being the protection of data in the event of an outage and providing the tracking and backup that HIPAA requires. Audit capability is also being built into the information systems as reviewers from the Joint Commission for the Accreditation of Healthcare Organizations (JCAHO) routinely audit the hospital's HIPAA compliance efforts.

Case 2: SOX Compliance

HP managed the challenge of SOX compliance by applying the principles of open standards for processes, risks and controls. Management at HP felt that the SOX challenge was best approached with the right combination of people, processes and technology. The organization applied the principles of open standards reference models, including its own HP ITSM Reference Model, in a step-by-step manner, to provide a common platform organization wide. The HP compliance team relied on a series of IT frameworks to help assist with the formulation of its methodology. It used the model based on: People (Core team of cross disciplinary people was built to implement the compliance program), Process (framework that guides the team through infrastructure assessments and evaluation of datacenters and overall system security) and Technology (helped in faster IT services management with reduced effort providing management with process-level business risks).

An organization's IT process maturity has a direct relation to their SOX readiness. HP created solutions that automated the IT Controls that were required for SOX. The challenge with SOX compliance is not just going through the compliance one time but rather continuing to achieve compliance every year.

Case 3: GLB Compliance
Allied Home Mortgage Capital Corporation is one of the largest privately held mortgage bankers. It has offices in 49 states and over 700 investors with several thousand programs and innovative partnerships. The organization has experienced a double digit growth rate since 1991. As a financial services provider, Allied had to comply with GLB and address administrative, physical and technical security requirements. The platforms used by the organization did not provide a common central means for authenticating all of its users. Policy management and technical controls processes also suffered from a lack of centralization. The company had no common data repository to hold all of the key data in one place, making the Application of stringent security measures in the current infrastructure a significant challenge.

Allied commissioned the consulting company, DYONOX, to provide solutions and help with the compliance process. DYONOX provided service solutions that included process optimization, process automation via custom applications development, secure active directory migration design, and policy management solutions through a Premier status partnership with NetIQ. DYONOX mapped and optimized these processes and created a central repository of data using custom scripts. The entire process of hiring was streamlined and automated.

The new systems reduced the overall time required to complete the hiring process and increased the efficiency. This resulted in lower costs to the organization. Optimizing the process with technology provided significant time and cost savings for everyone. Security management became more efficient and easier. The benefits from streamlining the processes occurred because of a requirement to be GLB compliant. The regulatory constraint provided an impetus to restructure the business process.

Discussions
Regulatory requirements are forcing organizations to make similar changes in order to be compliant, leading to a standardization initiative in the industry. HIPPA has made significant changes in the healthcare industry by forcing organizations to adopt electronic medical records (EMR), to provide more secure data storage facilities, and to incorporate stringent security standards. SOX provided an impetus to increase agility, minimize risk and improve performance. Compliance with this act forced organizations to have a better IT governance structure, a sound internal control assessment program, and strong data management techniques, auditability and security. Organizations complying with SOX broadly use similar techniques to meet the compliance requirements and make similar changes in their IT infrastructure. GLB compliance results in similar infrastructural change management challenges.

CONCLUSIONS

Institutional theory adopts an open system perspective of organizations [46] i.e. organizations are strongly influenced by their environments. The role of competition is important for organizations to shape their structure and functions but socially constructed belief and rule systems also exercise enormous control over organizations – both how they are structured and how they carry out their work [46]. Dewett and Jones (2001) imply that IT is a variable that enables better and timely decision making, thus promoting organizational performance.

Numerous governmental regulations have and are continuing to force organizations to revamp their IT infrastructures. These laws have strict demands on information technology infrastructure to establish, identify, document, test and monitor effectiveness of internal controls. These laws significantly affect an organization's business processes and information technology infrastructure preparedness. These regulations force businesses within same industry to have similar standards of compliance. Gradual standardization of the business processes in pursuit of compliance would tend to gradually commoditize "IT" as a product and as a process.

IT has become a central organizational function and thus, governmental regulations often radically impact IT and business processes, particularly in terms of the cost of compliance, preparedness for external audit, organizational restructuring, sharing of data between enterprises, enhanced technical supports and regular monitoring, and the assessment of business processes. Governmental regulations are usually proposed in reaction to growing public dissatisfaction and concerns [36]. While they may be expensive and arduous to fulfill, these regulations present an opportunity for organizations to restructure and improve their information technology operations.

This research makes multiple contributions to the existing body of research. In a discussion regarding the legitimacy of the information systems discipline, Weber (1997) argues that the information systems discipline should take theories from other disciplines and build novel theories which explain various phenomenon that are specific to the information systems discipline. This manuscript uniquely applies the neo institutional theory from the discipline of sociology and organization theory to explain the homogenization of the IT industry. This manuscript also contributes to the practitioner world by accounting for the rapidly changing regulatory environment, discussing the effects on the IT industry, and providing suggestions for organizations to deal with such changes. Finally, this manuscript provides a conceptual analysis of an industry wide phenomenon and argues for an increase in macro level research in information systems in order to further understand the implications of governmental regulations.

An empirical validation of the research model proposed in this manuscript will provide for interesting future research. Using structured equation modeling, the hypotheses presented in this manuscript may be further validated. This manuscript initiates a research effort on the impact of governmental regulations on organizations; additional studies on organizational change management in the IT environment would prove interesting.

REFERENCES

1. Abraham, Sherly and Chengalur-Smith, Indushobha, "The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective" (2011). *AMCIS 2011 Proceedings - All Submissions.* Paper 467. http://aisel.aisnet.org/amcis2011_submissions/467
2. Adler, P. S. (2005). The evolving object of software development. Organization, 12(3), 401-435.
3. Appari, A., Johnson, E. and Anthony, D. (2009). HIPAA Compliance in Home Health: A Neo-Institutional Theoretic Perspective, SPIMACS'09, November 13, 2009, Chicago, Illinois, USA
4. Avgerou, C. (2000). IT and organizational change: an institutional perspective, Information Technology & People, Vol. 13(4), pp. 234
5. Baumer, D., Earp, J. B. and Payton, F. C. (2000). Privacy of Medical Records: IT Implications of HIPAA, Computers and Society, December, 40-47.
6. Benders, J., Batenberg, R. and Blonk, H. (2006). Sticking to standards; technical and other isomorphic pressures in deploying ERP-systems. Information & Management, 43(2), 194-203.
7. Bennet, V. and Cancilla, B. (2005). IT responses to Sarbanes-Oxley. IBM, Retrieved on 09/30/05,http://www-128.ibm.com/developerworks/rational/library/sep05/cancilla-bennet/index.html
8. Bertino, E. (1998). Data Security. Data & Knowledge Engineering, 25, 199-216.
9. Berghel, H. (2005). The Two Sides of ROI: Return on Investment vs. Risk of Incarceration. Communications of the ACM, 48(4), 15-20.
10. Bj¨orck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organizations, *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*.
11. Chin, A.G. and Mishra, S. (2006). Increasing Governmental Regulations and Their Impact on IT: SOX and HIPAA, Proceedings of the International IRMA Conference, May 2006.

12. Chiravuri, A. and P. Ambrose (2002). A Theoretical Examination of Organizational Downsizing and Its Effects on IS Organizational Learning, Memory and Innovation, *Americas Conference on Information Systems, Dallas, Texas, Association for Information Systems.*
13. Clemens, E. and Cook, J. (1999). Politics and Institutionalism: Explaining Durability and Change, Annual Review of Sociology, 25:441-66.
14. Currie, W. (2004). The organizing vision of application service provision: a process-oriented analysis, Information and Organization, Vol. 14, pp. 237-267.
15. D'Aunno, T., Succi, M. and Alexander, J.A. (2000). The Role of Institutional and Market Forces in Divergent Organizational Change. Administrative Science Quarterly, 45, 679-703.
16. Demers, C. *Organizational change theories: A synthesis* Sage Publications, Inc, 2007.
17. Dewett, T. and Jones, G. (2001). The Role of information technology in the organization: a review, model, and assessment, *Journal of Management*, 27, pp. 313-346
18. DiMaggio, P.J. and Powell, W.W. (1991). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, In W. Powell and DiMaggio (Eds.). The New Institutionalism in Organizational Analysis*,* The University of Chicago Press, 63-82.
19. Edelman, L.B and Suchman, M.C. (1997). The Legal Environments of Organizations. Annual Review of Sociology, 23, 479-515.
20. Electronic Privacy Information Center (EPIC), (2001). Retrieved on 06/25/06 http://www.epic.org/privacy/terrorism/usapatriot/
21. E&Y *Global Information Security Survey 2005: Report on the Widening Gap*, Ernst & Young, 2005.
22. Farris, G. (2004). Mitigating the Ongoing Sarbanes-Oxley Compliance Process with Technical Enforcement of IT Controls. DM Direct Newsletter, DMReview.com, Retrieved on 07/17/06 http://www.dmreview.com/article_sub.cfm?articleId=1014858
23. Fox, C. (2004). Sarbanes-Oxley- Considerations for a Framework for IT Financial Reporting Controls. Information Systems Control Journal, 1
24. Fraser, M.D. and Vaishnavi, V.K. (1997). A former Specifications Maturity Model, Communications of the ACM, 40 (12), 95-103.
25. Gallagher, S. (2003). Gotcha! Complying with Financial Regulations", Baseline Magazine, Retrieved on10/02/05 http://www.baselinemag.com/article2/0,1397,1211224,00.asp/
26. Greenwood, R. and Hinings, C. R. (1996). Understanding radical organizational change: Bringing together the old and the New Institutionalism. Academy of Management, The Academy of Management Review, 21(4), 1022-1054.
27. Hagerty, J and Scott, F. (2005). SOX Spending for 2006 To Exceed $6B. AMR Research, Retrieved on 11/29/05 http://www.amrresearch.com/Content/View.asp?pmillid=18967/
28. Huston, T. (2001). Security Issues for Implementation of E-Medical Records. Communications of the ACM, 44(9), 89-94.
29. Information Systems Audit and Control Association (ISACA), (2004). CISA Review Manual, 2004 Edition. Rolling Meadows, IL: ISACA
30. Information Technology Governance Institute (ITGI). (2004). IT Control Objectives for Sarbanes-Oxley, Retrieved on 07/17/06 http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=25123
31. Jones, M., Orlikowski, W. and Munir, K. (2004). Structuration Theory and Information Systems: A Critical Reappraisal in: Social Theory and Philosophy for Information Systems, J. Mingers and L. Willcocks (eds.), John Wiley & Sons, Ltd, Chichester, England, 297-328.
32. King, J. L., Gurbaxani, V., Kraemer, K. L., McFarlan, F. W., Raman, K. S., & Yap, C. S. (1994). Institutional factors in information technology innovation. Information Systems Research, 5(2), 139-169.
33. Knorr, E. (2004). The Bitter Pill: Regulation has come to town, and IT will never be the same. CIO Magazine, Retrieved on 09/20/05 http://www.cio.com/archive/
34. Mercuri, R.T. (2004). The HIPAA-potamus in Health Care Data Security. Communications of the ACM, 47(7), 25-28.
35. Meyer, J. W. and Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology, 83 (2), 340-363.

36. Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, A. (1995). Values, Personal Information Privacy and Regulatory Approaches, Communications of the ACM, 38(12), 65-74.
37. Mishra, S. and Weistroffer, R. (2006). A Framework for Integrating Sarbanes-Oxley Compliance into the Software Development Process, Proceedings of the 9th Southern Association of Information Systems conference, Jacksonville, March 10-12.
38. Mitrano, T. (2003). Civil Privacy and National Security Legislation: A Three-Dimensional View, Educause review. November/December, 53-62
39. Moore, C. (2004). The Growing Trend of Government Involvement in IT Security, Proceedings from InfoSecCD Conference '04, October, 119-123.
40. NetWorkWorld, Retrieved on 09/29/05 http://www.networkworld.com/research/2003/0901regs.html?page=1
41. Peterson, Z. and Burns, R. (2005). Ext3cow: A Time-Shifting File System for Regulatory Compliance. ACM Transactions on Storage, 1(2), 2005, 190-212.
42. Pettigrew, K. and McKechnie, L. (2001). The Use of Theory in Information Science Research, *Journal of the American Society for Information Science and Technology,* 52(1), pp. 62–73
43. Robey, D. and Holmstrom, J. (2001). Transforming municipal governance in global context: A case study of the dialectics of social change. Journal of Global Information Technology Management, 4(4), 19-31.
44. Safadi, Hani and Faraj, Samer, (2011)"IT in Healthcare: an Integrative Study of Organizational Change" (2011). *AMCIS 2011 Proceedings - All Submissions*. Paper 21.http://aisel.aisnet.org/amcis2011_submissions/21
45. Scott, W. (2004). Institutional Theory: Contributing to a Theoretical Research Program, Chapter prepared for *Great Minds in Management: The Process of Theory Development,* Ken G. Smith and Michael A. Hitt, eds. Oxford UK: Oxford University Press.
46. Scott, W.R. (2005). Organizations: Rational, Natural and Open Systems (5th Edition). Englewood Cliffs, N.J.: Prentice-Hall.
47. Siegel, P.H., Agarwal, S. and Rigsby, J.T. (1997). Organizational and Professional Socialization: Institutional Isomorphism in an Accounting Context. The Mid-Atlantic Journal of Business, 33(1), 49-68.
48. Swire, P.P. and Steinfeld, L. (2006). Security and Privacy After September 11: The Health Care Example", *Minnesota Law Review* Forthcoming, Retrieved on 06/25/06 SSRN: http://ssrn.com/abstract=347322 or DOI: 10.2139/ssrn.347322
49. Symantec (2006), Improving IT compliance: 2006 IT Compliance Benchmark Report, retrieved on 03/06/07 http://i.i.com.com/cnwk.1d/html/itp/Symantec_2006_IT_Compliance_Report.pdf
50. TechRepublic, (2007). Case Study: Allied Home Mortgage Capital Corporation, Retrieved on 03/05/07 http://www.dyonyx.com/documents/Allied.pdf
51. U.S Securities and Exchange Commission (SEC) (2003). Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Retrieved on 06/25/06 http://www.sec.gov/rules/final/33-8238.htm
52. Volonino, L., Kermis, G., Gessner, G. (2004). Sarbanes-Oxley links IT to Corporate Compliance. Proceedings of the Tenth Americas Conference on Information Systems, New York, 2004
53. Yugay, I. and Klimchenko, V. (2004). SOX Mandate Focus on Data Quality and Integration. DM Review Magazine, Dmreview.com, Retrieved on 09/30/05 http://www.dmreview.com/article_sub.cfm?articleId=8040
54. Wang, P. "Chasing the hottest it: Effects of information technology fashion on organizations," *MIS quarterly* (34:1), 2010, pp 63-85.
55. Weber, R. (1997). Ontological foundations of information systems. Coopers & Lybrand, Australia.
56. Wickramasinghe, N., Troshani, I. and Goldberg,S. (2012). Adoption of Pervasive e-Health Solutions: The Need For an Appropriate Regulatory Framework, *AMCIS 2012 Proceedings,* http://aisel.aisnet.org/amcis2012/proceedings/ISHealthcare/4
57. Zucker, L. G. (1987). Institutional Theories of Organization. Annual Review of Sociology, 13, 443-464.