Author(s): Kala Sethupathy, D.S.; Preston, D.; Imafidon, C.O.
Title: Impact of corporate governance on information security practices in (UK) financial industry
Year of publication: 2010
Citation: Kala Sethupathy, D.S., Preston, D. and Imafidon, C.O. (2010) 'Impact of corporate governance on information security practices in (UK) financial industry.', Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 5th Annual Conference, University of East London, pp.135-142.

IMPACT OF CORPORATE GOVERNANCE ON INFORMATION SECURITY PRACTICES IN (UK) FINANCIAL INDUSTRY

Kala Sethupathy D. S, Preston D, Imafidon C. O
University of East London
ksdevsenapathy@yahoo.com, d.preston@uel.ac.uk,c.o.imafidon@uel.ac.uk

Abstract: The empirical study of this paper focuses particularly on the UK financial industry for trends in the framework of policies in order to manage information security as operational risk and how corporate governance plays a vital role in framing policies within the company (Poole and CISM, 2006). The increasing dependency of UK financial industries on IT solutions and services to manage their business processes has indirectly coupled the financial IT systems to the economic well being of a country. This means that risks associated with such financial IT systems would have an impact on the economic elements of a nation. As more and more UK financial industries relies on IT solutions to manage their businesses, Information security (IS) trails are increasingly becoming a part of general audit practices within these UK financial industries. IS and IT audit trails for risk assessment includes a number of risk elements like data security, firewall, server, network, application, etc. Corporate governance policies are mostly excluded from IS audits as there is no regulated roadmap for assessment. However some companies adopted industry wide standards like COBIT and ISO but still unregulated by government authorities. Hence this research investigates the significance of corporate governance policies towards the development of a robust IS framework in the financial industry. It also looks at the government authority's role as a watchdog.

1. Introduction

Productivity and economic growth are deeply tied down by policies framed, adopted and implemented by corporate governance and government authorities. Over a period of time, steady and increased productivity act as a key driver for sustained economic growth (Camus, 2007). One of the ways of measuring Productivity in UK is by measuring GDP through the income approach. According to ONS (Office for National Statistics) GDP through income approach is calculated by the sum of gross operating surplus, compensation of employees and taxes on production and products. However, the gross operating surplus is calculated by the sum of the following excluding holding gains (Camus, 2007):

- Self-employment income (mixed income and quasi-corporations)
- Gross trading profits of private financial corporations
- Gross trading profits of private non-financial corporations
- Gross trading surplus of public corporations (financial and non-financial)
- Rental income
- Non-market consumption of fixed capital
- FISIM

Consequently financial sector including public and private financial corporations is one of the biggest contributors to the UK economic growth and businesses across non financial sectors. The recent global financial crisis started in 2008 elucidates the deep penetration of financial market practices and its effect on businesses and economies across the world (Bullock, 2008) (Shiller, 2008). The 1980 US banking crisis which led to the 1990's US recession; Wall Street crash of 1929 which led to the great depression in 1930; and Asian Financial crisis of 1997 are some of the black days in the global economic diary caused by the failure of regulatory mechanism and poor policies adopted (Kindleberger and Aliber, 2009). Monitoring and regulation of market practices, operations and systems of UK financial industry is currently handled through policies, regulations and frameworks. Financial policies are framed and implemented by corporate governance, government regulatory authorities and monitory organisations. Subsequently, regulations are mainly implemented by government authorities and frameworks are adopted based on the unremitting changes in the market trends. Within the scope of this paper corporate governance in UK financial sector is subjected to investigation. This is to study the impact on the information security policies governing the risks associated with IT operations and systems maintained or developed through outsourcing business process.

2. Productivity, Economic Growth and Policies

Historically productivity across different sectors in a country depends mainly on the labour time, labour contribution and the quality of the work force. However when more and more IT systems and operations replaced the labour intensive work of the traditional business processes it is evident that the productivity factor which contributes to the growth of economy is slowly shifting towards the effective governance of IT systems and operations. However, effective governance of corporate systems and operations is installed by corporate governance policies and framework.

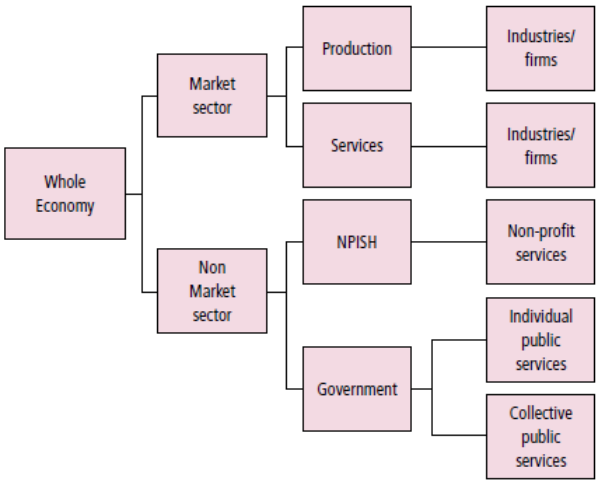

Figure 28: Disaggregation of productivity data by activity (Camus, 2007)

According to Campus (Camus, 2007) when UK economy is disaggregated in to activity of market and non market sectors it is evident that products and services offered by the financial companies holds the major share of the industries and firms in terms of productivity, profitability and economic contribution. On the other hand government, non profit sectors hold the major share of individual, collective and non-profit public services. Subsequently this research focuses on the activity of financial companies and its impact on the productivity and economic growth factors. Furthermore the research investigation studied the corporate governance policies of the financial companies as an activity, which drives the productivity and controls the level of impact

over the economic growth factors. The relation between corporate governance policies and the productivity could be categorised under multi factor productivity (MFP). If a productive labour hour is replaced by the efficiency, output and security of an IT system then the Domar aggregation equation (Domar, 1961) could be derived as,

Growth of GDP per hour worked = [Capital deepening (2)] + [Effective IT system's contribution (which replaced Labour quality contribution)] + [MFP growth]

Where,

Capital deepening = [Capital's share times growth of capital input per hour worked]

Effective IT system contribution = [IT system's share times growth of IT system input per hour maintained efficiently and securely]

Rearranging (1) and (2), MFP can be seen as:

Growth of MFP = [Growth of GDP (3)] – [Capital's share times growth of capital input] – [IT system's share times growth of IT system input per hour maintained efficiently]

Growth of MFP (4) per hour worked = [Growth of GDP per hour worked] – [Capital deepening] – [effective IT system's contribution]

Though the above equation was solely built on the primary industrial data it is necessary to consider the intermediate inputs when trying to define the growth of MFP for a particular industry (i). Hence,

Growth of MFP in industry (i) = Growth of total output in industry (i) (7) – cost-share-weighted growth of capital services, IT systems and intermediate input

Hence the aggregation of Domar's equation is, Aggregate MFP growth rate = [Domar-weighted sum of industry MFP growth rates]

Where, the Domar weight for industry (i) = [Nominal total output of industry (i)] / [Nominal GDP]

The real and nominal value has been calculated based on the accounted inflation rate. Domar's equation applied for the IT system's productivity (by replacing labour quality contribution), evaluates the relationship between productivity and economic factors considering the modern financial industrial activities run by massive IT systems and services. This research will now try to address the factors that have a major impact on financial IT systems and services. It will also try to study the governance and its impact on risks associated with information security.

3. IT Systems, Services and Information Security in UK Financial Industry

Financial businesses in UK are now crossing a new era of IT systems and associated services. This mainly includes independent software applications, application maintenance services, web based applications, additional services for IT systems (e.g., database management, content management, network routing service, etc.), networking, hosting services, outsourced IT development, maintenance, operations and ITES services. A study by ENISA concludes that the growth of business dependency on

IT systems is exponential compared to the developments in regulating security issues of IT systems and services. According to ENISA's statistics only one in every six small companies in UK could survive without IT (PriceWaterHouseCoopers, 2006). The trend in today's industry to compact business needs without compromising quality is a consequence of businesses fighting against competition, resources and cost amidst globalisation and socio-economical turmoil. One of the major practises adopted by the industry to cut cost, avail cheaper and swift resources in less time is to outsource business needs. Business needs varies based on the nature of business itself. When it comes to IT development and operations more than 53% of the companies outsource their IT operations (PriceWaterHouseCoopers, 2006).

As the dependency of industry on IT systems increased scholars were more sceptical regarding the security of fast developing systems. "Many UK businesses are a long way from having a security-aware culture. Their expenditure on security is either low or not targeted at the important risks (PriceWaterHouseCoopers, 2006)". Roughly two-fifths of businesses spend less than 1% of their IT budget on information security (PriceWaterHouseCoopers, 2006). Businesses tend to restrict their concern and expenditure to basic rules of security framed by the government representatives. However, research conclusions demonstrates the need for businesses to extend their security concern towards best practices in industry; models employed in building services or systems; models employed in information exchange and outsourcing. Such practices in the industry would contribute towards consistency in openness, transparency of systems and business processes, socio-economic progression, safeguarding community and globalisation.

Standards for information security practices in industry set by the government failed to make a strong influence on the current practices among companies. A study by ENISA concluded that only 44% of companies have carried out any security risk assessment in the last year. This is a small increase on six years ago (PriceWaterHouseCoopers, 2006). There is still a shortage of security qualified staff; only one in eight companies has any (PriceWaterHouseCoopers, 2006). Revolution in internet forced companies to go online. On the other hand, Internet facilitated the growth of companies while reducing the cost and resources. Though Internet serves as a global medium of information exchange, it is still an unsecured system including its design and operation (Ofcom, 2006). Findings from the British Crime Survey of 2003/2004 concluded that an average of more than £ 238 millions is lost every year on fraud. It also concludes that the percentage of internet and technology contributions towards the overall fraud is increasing every year (Wilson, et. al, 2006).

4. Corporate Governance and its impact on operational and system risks

Corporate Governance plays a vital role in the internal control and management of the organisation. Policies framed and decisions made as a part of corporate governance spirals down the line from the senior management till the operational end. This demonstrates the major influence it has on the organisation's day to day operations, practices followed and path taken in the market.

The major milestone of a secured industry would be to attain the highest standards through design and adoption of desired policies and practices. Three-fifths of UK businesses are still without an overall security policy, though a third of these have defined an acceptable usage policy for the Internet (PriceWaterHouseCoopers, 2006). Researches conclude that information security standards and policies in businesses should not be restricted to IT, ICT, ITES, Business models and outsourcing models. However, research conclusions pay much emphasis on HR recruitment process, Learning and Development and Disaster Recovery Systems. "Recruitment processes at a quarter of companies do not include any background checks; 19% of companies that believe security is a very high priority fail to check the background of their staff. One in eight organisations does nothing to educate their staff about their security responsibilities. Only a quarter of UK companies have tested their disaster recovery plans in the last year." (PriceWaterHouseCoopers, 2006). Survey conducted by ENISA and PWHC states that only 40% of UK companies have a formally documented and defined information security policy. E Business and E Commerce are emerging as the industry's next giant step towards attaining business compactness and independency in a global perspective. Discussing the E Business practices and its evolution would help government authorities to frame models and policies to adopt the best practice in safeguarding the potential industry-community framework.

5. IT Outsourcing Market and UK Financial Industries

According to a survey conducted by European Information Technology Observatory (EITO), UK IT services market value grows every year with out regulatory implications (Figure 2).

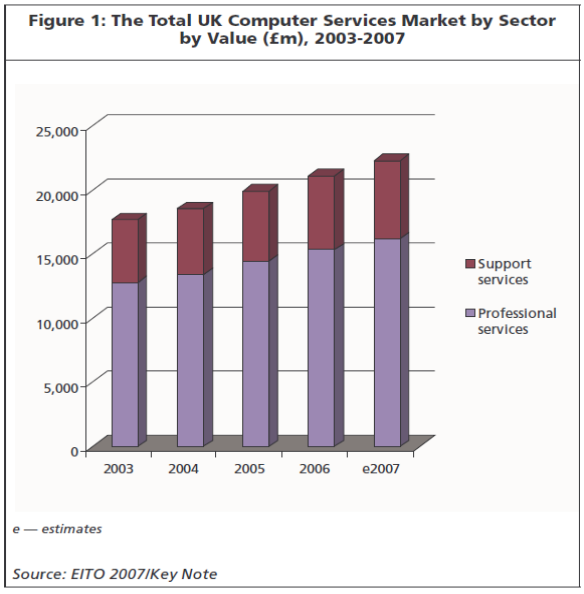

Figure 29 (Baxter, 2008)

Currently there are more than 85,030 VAT-based IT enterprises providing IT service to financial companies in UK apart from a large source of overseas IT enterprises competing in the market. This massively growing industry in terms of both value and technology is highly unregulated and unorganised in terms of development and adoption of industry wide approved standards for providing IT services (Baxter, 2008). However, when looked at the IT services market trend it is evident that the market is mainly driven by IT technological innovation, people's skill and the service time. Though this market trend pushed Information Security governance and regulations to the bottom of the list it is still

continuing to help major companies to drive down their operation cost despite increasing employment opportunity in IT services. Hence, IT services industry grows towards facilitating an unsecured information society despite its current contributions to the major economic drivers. According to the market report of keynote (Baxter, 2008), Financial companies including banks, insurance companies, investments, financial services are the largest consumers of the IT services compared to retail, communication and manufacturing sectors. However, more than two third of the IT services contracts fail due to trust related issues between the customer and the service provider. This trust is currently centred more on the cost, time and quality than information security, privacy and other factors. Current financial market considers cost, time and quality as core factors affecting its business processes directly compared to information security and privacy. However experts believe that increase in the number of businesses affected by information security and privacy issues during the outsourcing process will soon include them as a major factor deciding the trust and relation between customer and service providers.

Software development is another key sub sector in the UK IT market which has equal contribution towards the development, maintenance and operation of IT infrastructure in UK financial companies compared to the IT services sector. Investment in software systems by financial companies are increasingly considered as assets of IT infrastructure (Fenn, 2008). Software sector is currently wide, innovative and fast growing than the service sector. Constant innovation, technological breakthrough, cost and efficiency are some of the major factors which drive the growth of this sector. Just like IT service sector the software sector also grows exponentially without a comprehensive regulatory compliance in place. "Based on figures from the European Information Technology Observatory (EITO), Key Note estimates that software accounted for around 11.3% of UK expenditure on information and communication technology (ICT) in 2007. This proportion has remained fairly stable since 2003 (Fenn, 2008)".

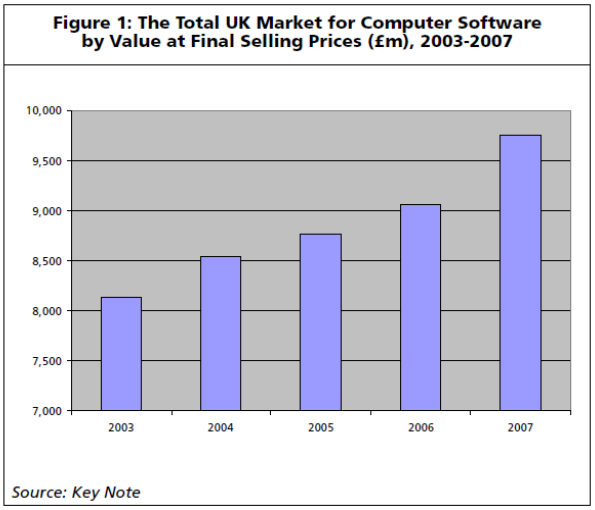

Figure 30 (Fenn, 2008)

Market analysts predicted that any breach in the IT infrastructure could cost more to the economy than the percent of expenditure spent on developing it. This is solely because of the increasing dependency of core services like finance, health, governance, security, etc, on the IT infrastructure of UK. However, when financial sector is analysed in particular it is becoming evident that this dependency on IT systems poses some new challenges to both government authorities and the financial company in terms of addressing the gaps while building and maintaining such IT systems through outsourcing. They are:

- Financial customers loosing track of outsourced project in terms of its management and development process due to the increasing complexity of IT

projects and the change in technologies adopted for the development.

- Non availability of expertise and complexity in developing comprehensive regulatory framework in a market where there is a swift phase of change in technology and consumer behaviour
- Globalisation through outsourcing market trend and incapacity of existing national infrastructure to monitor and regulate the flow of data, IT systems and IT services across the borders.
- The fast changing market, consumer, vendor and social behaviour due to the adoption of Internet as a common medium

6. Standards for Auditing Information Security

Operational and System risks are assessed through bespoke auditing process in an organisation. Best market practices to measure financial, operational and development risks in terms of profit, legal and growth aspects are widely adopted and followed by organisations. However, best practices in terms of information security of IT systems, services and outsourcing practices are not widely adopted and regulated. ISO/IEC 17799 and COBIT are some of the effective IS standards adopted by a lot of organisations (Poole and CISM, 2006). Though these standards and framework are revised periodically according to the changing behaviour of market and the businesses, majority of organisations fail to revise their framework and standards in accordance with the change in their business and market. Cost, resources to manage the IS framework and decreasing relevance of ISO and COBIT to all business processes are some of the main reasons for organisations not to revise their framework periodically. Standards for IS auditing is arguably complex and inefficient to frame across all sectors when it comes to globalisation which involves trading, business operations, resource management, legislations and laws across the globe. Hence bespoke auditing frameworks have to be framed and adopted that are relevant to a specific industry and its business processes. Standards of ISO and COBIT which serves the purpose of some organisations to govern their IS framework could well be unsuitable for some other organisations which requires bespoke auditing solutions to govern its IS framework. Subsequently, these standards and the extent of its implementation by industries are not regulated or approved by government authorities, which again gets complicated when it involves more number of government regulatory bodies.

7. Conclusion

Though auditing and risk assessment standards like COBIT and ISO are adopted by some UK financial companies successfully to govern their IS framework it is still not monitored and regulated by dedicated UK government authorities. On the other hand UK financial companies without any bespoke IS framework or corporate governance policies to combat risks associated with the IT outsourcing process are more vulnerable to Information Security breaches than their counterparts. According to Domar's equation it is evident that the breach in the complex IT systems and processes managed by UK financial industries which moves trillions of pounds every second has a greater influence in deciding the rise or fall of economies. The number of financial crises addressed by the world from 1980 till date confirmed Domar's results. Thus a dedicated

government authority in UK working along with similar authorities around the world to monitor and regulate the IS framework, standards, market practices and corresponding corporate governance policies of UK financial sector is vital to securing the economic health of UK and shielding from any future turmoil. Eventually it would also help in overlooking the governance of best practices adopted by the UK financial organisations towards governing the outsourcing of its IT systems and operations.

8. References:

BAXTER, J. 2008. *Computer services, Key Note market report,* Key Note.

BULLOCK, N. 2008. *FT.com / In depth - Credit crunch in a century's context* [Online]. Financial Times. Available: http://www.ft.com/cms/s/0/90f513e4-64b1-11dd-af61-0000779fd18c,dwp_uuid=698e638e-e39a-11dc-8799-0000779fd2ac.html

CAMUS, D. 2007. *The ONS productivity handbook : a statistical overview and guide,* Basingstoke, Palgrave Macmillan.

DOMAR, E. 1961. On the measurement of technological change. *Economic Journal,* LXXI**,** 709–729.

FENN, D. 2007. IT security: market report 2007. 8 ed.: Key Note Publications.

FENN, D. 2008. *Computer software Key note market report,* Key Note Ltd.

KINDLEBERGER, C. P. & ALIBER, R. Z. 2009. *Manias, panics and crashes : a history of financial crises,* Basingstoke, Palgrave Macmillan.

Office of Communication Research Publication. 2006. Online Protection: A survey of consumer, industry, regulatory mechanisms and systems (21 Jun 2006), Mainsource:http://www.ofcom.org.uk/research/telecoms/reports/onlineprotection/report.pdf

WILSON, D. Patterson, A. Powell, G. Hembury, R. 2006, Fraud and Technology Crimes, *Findings from the 2003/04 British Crime Survey, the 2004 Offending,* Crime and Justice Survey and administrative Sources; Home Office ch. 2-3.

PATEL, N. S. 2009a. Financial Statistics. *In:* PATEL, N. S. (ed.) 569 ed.: palgrave macmillan.

PATEL, N. S. 2009b. *Financial statistics explanatory handbook.*

POOLE, V. & CISM 2006. Why Information Security Governance Is Critical to Wider Corporate Governance Demands—A European Perspective. *INFORMATION SYSTEMS CONTROL JOURNAL,* 1.

PriceWaterHouseCoopers. 2006, Information Security breaches survey, ENISA – European Network and Information Security Agency. http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf, updated on 20-May-08.

SHILLER, R. J. 2008. *The subprime solution : how today's global financial crisis happened and what to do about it,* Princeton, N.J. ; Woodstock, Princeton University Press.

STATISTICS, O. O. N. 2009. Profitability - UK Companies Coverage 4th quarter and year 2008. *quarterly.* 1 April 2009 ed: Office for National Statistics