Trust: An Element of Information Security

Stephen Flowerday and Rossouw von Solms

The Centre for Information Security Studies, P. O. Box 77000, Nelson Mandela
Metropolitan University, Port Elizabeth, 6031, South Africa
sflowerday@telkomsa.net, rossouw.vonsolms@nmmu.ac.za

Abstract. Information security is no longer restricted to technical issues but incorporates all facets of securing systems that produce the company's information. Some of the most important information systems are those that produce the financial data and information. Besides securing the technical aspects of these systems, one needs to consider the human aspects of those that may 'corrupt' this information for personal gain. Opportunistic behaviour has added to the recent corporate scandals such as Enron, WorldCom, and Parmalat. However, trust and controls help curtail opportunistic behaviour, therefore, confidence in information security management can be achieved. Trust and security-based mechanisms are classified as safeguard protective measures and together allow the stakeholders to have confidence in the company's published financial statements. This paper discusses the concept of trust and predictability as an element of information security and of restoring stakeholder confidence. It also argues that assurances build trust and that controls safeguard trust.

1 Introduction

Trust and controls help curtail opportunistic behaviour, therefore confidence in information security management can be achieved. Besides the technical aspect of information security and IT that should be implemented using best practices, one needs trust to help curb 'cheating' and dishonesty. This paper focuses on the information found within the financial statements of a company. Stakeholder, especially investor, confidence needs to be restored in the board of directors in the domain of financial reporting. The avalanche of corporate governance scandals such as Enron, WorldCom, Tyco, and Parmalat has caused many to be suspicious of the information found within financial statements.

It has been necessary to draw from the work in other research disciplines to extend the study of trust and risk to this domain. This fragile, yet important concept, *trust*, greases the wheels of industry. Trust allows the various users of information, found within information systems, confidence when making decisions.

An important aspect of corporate governance is the management of risk. Companies today use a system of controls in their efforts to manage their risk. Often these controls focus on the company's various financial processes and systems. The reason for this is that these important processes and systems are often the target of security breaches. It has therefore become imperative that the security for these

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

systems is comprehensive. Both opportunistic behaviour, which involves a human element, and the conventional technical IT security threats, need to be addressed.

It is stressed that [1], *"security is not a separable element of trust"*. This statement collaborates that both trust and security-based mechanisms are classified as safeguard protective measures [2]. Together these provide technological, organisational and relationship benefits to the various company stakeholders.

This paper introduces the concept of trust and uncertainty reduction followed by what constitutes trustworthiness. Self-centred opportunism, 'cheating' and dishonesty are classified as unfavourable behaviour, consequently behaviour is addressed using game theory to illustrate possible outcomes. The very close relationship that trust and risk have, is discussed with assurances being emphasised as an element to help build trust. Finally, a trust strategy is emphasised as a way to avoid unfavourable behaviour and to build and safeguard the concept of trust.

2 The Theory of Trust

Trust should not be left in the domain of philosophers, sociologists, and psychologist but also needs to be addressed by all attempting good governance. Can there be any doubt that fairness, accountability, responsibility, and transparency [3] are facets that contribute to the building and safeguarding of trust? Trust is not something that simply happens. It is fragile and not easily measured or identified [4].

2.1 Uncertainty Reduction Theory and Trust

In general, trust is defined as a psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behaviour of another [5]. Trust also refers to the notion of the degree one risks: this risk is predicated on the belief that the other party is beneficent and dependable [6]. The notion of trust is that it involves the willingness of a trustee [7] *(the recipient of trust or the party to be trusted, i.e. board of directors)* who will perform a particular action important to the trustor *(the party that trusts the target party or the trusting party, i.e. investors)*.

If no uncertainty exists between the two parties, it indicates that no risk or threat is found in future interaction between the parties [8]. Noting that we do not live in a perfect world and we don't have perfect competition it is therefore impossible to have absolute uncertainty free interaction *(in other words, a degree of uncertainty always exists)*. One needs to make an effort to reduce uncertainty and to increase predictability about how the other party will act. Both the board of directors and the various company stakeholders should consider this.

It is emphasised that through communication and the exchange of information about each party, a decrease in uncertainty occurs [9]. According to Berger [10] uncertainty about the other party is the *"(in)ability to predict and explain actions"*. Thus the basic premise of Uncertainty Reduction Theory, if one applies the principles to the various company stakeholders, is that it attempts to reduce uncertainty and to increase predictability about each party's behaviour. This confirms that uncertainty can only be reduced by the information shared and a knowledge as to the condition of this information, which will affect the (un)certainty level [10].

Without a certain degree of predictability, a party has no basic assumption of how the other party will or will not utilise their trusting behaviour [8]. When one party is able to predict a degree of the other party's future actions this leads to a decrease in one's perceived vulnerability *(risk is perceived to be reduced)*. Therefore uncertainty reduction is a necessary condition for the development of trust. One's predictability about the other should be increased, thus reducing uncertainty via communicating (producing financial statements for the various stakeholders) with the other party. As a result: when more uncertainty is reduced, perceived predictability should be increased and vulnerability will be minimised (based upon prior experience). This highlights the paramount importance that the information found within the company financial statements has its integrity intact. If not, a trust problem will occur.

2.2 Trustworthiness

Fig. 1 is a proposed model of trust of one party for another which highlights the elements of trustworthiness [7]. This model illustrates that the level of trust and the level of perceived risk in a situation will lead to risk-taking in a relationship. It also touches on a trustor's propensity, which is said to be influenced by how much trust one has for a trustee prior to information on that particular party being available. Propensity will differ in a party's inherent willingness to trust others [7].

In this model, the three elements that help to create and define a trustworthy party are discussed. These elements are: *Integrity, Benevolence,* and *Ability*. This perception of trust can be applied to corporate governance in the following way:

- Integrity-based trust refers to whether the directors are honest and fair and not *'fudging the numbers'*. Some scholars in their research have used the words *reliability* or *predictability* in place of integrity [2, 11].
- Benevolence-based trust implies that the directors would be loyal, keep the best interests of the various company stakeholders at heart, and not seek to be self-serving and opportunistic. Some scholars have used the words *goodwill* or *openness* in place of benevolence [2, 11].
- Ability-based trust relates to the director's *skill level,* for example, their technical competence and understanding of information systems and security. Some researchers favour the word *competence* rather than *ability*, however, little difference is found in the meanings of these words [2, 11, 12].

Perceived trustworthiness requires honesty and integrity. These are attributes that a party needs to demonstrate so that when opportunities to *'cheat'* arise, they will be turned down. As stated [7], *"... if the trustee had something to gain by lying, he or she would be seen as less trustworthy"*. In addition, the more perceived benevolence and integrity found in a party, the more likely it will be to predict a favourable future outcome for a relationship with that party [13].

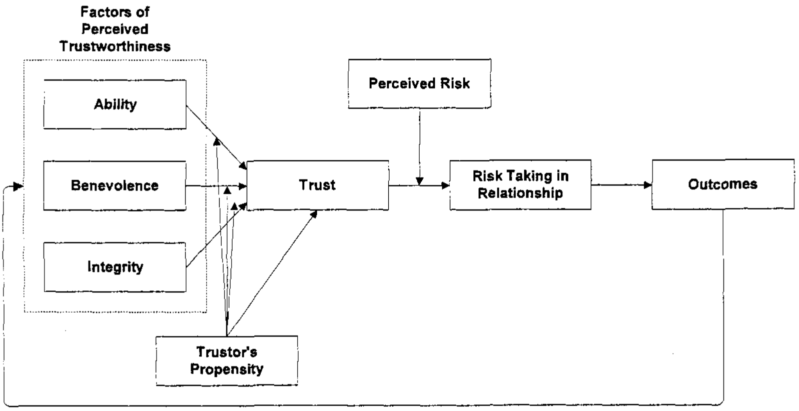

Fig. 1. Proposed Model of Trust [7].

2.3 Trust, Behaviour and Game Theory

Perceived risk and trust affect behaviour and this varies at different stages of a relationship [14]. Risk is dominant in the early stages and trust, in long-term relationships. One needs to consider the *cause and effect* relationship between *trust and risk,* which have an effect on *behaviour.* This view of trust is important because in order to build trust, the perceived risks by the various company stakeholders, especially investors, need to be catered for to avoid unfavourable behaviour.

Gefen et al. [14], from their research, found that the risk perception is more than a mere "*moderating influence*" affecting behaviour. They claim that the perceived risk "*mediates*" the affect trust has on behaviour. This, again, highlights the importance of information security in reducing the *'threats'* (both human and technical) that financial information systems are exposed to.

Economists and mathematicians have used game theory in their study of trust since 1944 [15]. These formal trust models consider how *'players'* discover trust and can quantify how trust or mistrust can occur [16, 17]. This paper discusses the principles of two games and the mathematical route will not be pursued.

Game theory involves the behaviour of rational decision makers *(players),* whose decisions affect each other. These players could be the company investors and managers, or any of the company stakeholders that may have conflicting interests. As emphasised [17, 18], an essential element of game theory involves the amount of information known about each other by the various players. The information the various players have will determine their behaviour. Also to be noted are the *'rules'* of the game (codes, regulations, policies, etc. that the company needs to comply to).

A classic example of game theory is known as the Prisoner's Dilemma. There are two prisoners in separate cells, faced with the dilemma of whether or not to be police informants. Without further communication, the two players need to trust each other to have integrity and to be benevolent. The following are possible outcomes.

If neither become informants and defect, the police have insufficient or only circumstantial evidence to convict them and therefore both players receive light sentences. If trust is lacking and both turn and become informants for the police, through their defection, both players receive heavy sentences. If one player defects and becomes a police informant, that player is set free and the player that did not defect is convicted and receives a very heavy sentence due to the testimony of the player that defected. The dilemma of the scenario highlights the issue of trusting the other player without continuous communication. Applied to a corporate governance setting the 'communication' could be affected by both the *accuracy* (fraud) and *reliability* (confidentiality, integrity and availability) of the information found within the company financial statements.

As observed [19], if the police were to tell the prisoners (players) that the interrogation is ongoing and without a foreseeable end, a pattern emerges and cooperation can become stable. This is the discovery of trust as the players learn to trust each other over time and the perceived risk element is reduced. If one applies this model of trust to corporate governance it can be assumed that, over time, trust will be established between the various stakeholders, including the CEO, the board of directors and investors.

Axelrod [20] suggests that, with time, a pattern of cooperative behaviour develops trust as in game theory. However, one could trust the director's ability (technical and information security capabilities) but not the integrity of the person behind the systems that may act opportunistically. This highlights that trust is more specific than '*I trust the board of directors*'. One should clarify what it is that I trust the board of directors to do.

To explain this concept another way an everyday example will be used. Note that trust is not transitive and is rather domain specific [21]. Example: one might entrust their colleague with $100 loan, but not entrust the same resource to that colleague's friend whom you do not know. Trust therefore weakens as it goes through intermediaries. Furthermore, to re-emphasise a related aspect, one might trust their colleague by loaning them $100 but not allow them access to your bank account to withdraw the $100 themselves. The second example highlights the domain specificity of trust. One does not blindly trust, but one trusts a party in a specific area or domain.

To continue with the prisoner's dilemma, the interests of the players are generally in conflict. If one chooses the high-risk option and the other chooses the low, the former receives a maximised positive outcome and the latter a maximised negative outcome. There are cases of opportunistic behaviour, such as the directors of the over-valued telecommunications companies who cashed in and sold their shares totalling more than US$6 billion in the year 2000, yet they touted the sector's growth potential just as it was about to collapse [22]. The investors chose the high risk option and remained committed while many directors 'defected' choosing the low risk option and short term financial gains.

Kydd [23] stresses a different point of the Prisoner's Dilemma by pointing out that, strictly speaking, there is no uncertainty about motivations, or behaviour and the dominant strategy would be to defect. As a result, uncertainty is smuggled in through the back door. He emphasises that *"...trust is fundamentally concerned with this kind of uncertainty"*. Kydd's research discusses trust and mistrust, and, claims that there is no uncertainty in the prisoner's dilemma about whether the other side prefers to sustain the relationship. He questions whether future payoffs are valued highly enough to make sustained cooperation worthwhile, or whether they are not and the parties will defect. He states that trust is therefore perfect or nonexistent. To model trust in the prisoner's dilemma one must introduce some uncertainty, either about preferences or about how much the parties value future interactions [23]. Applying Kydd's argument to the various company stakeholders illustrates that there needs to be a *win win* situation for all. The information one party has, needs to be had by the other parties as well. Conflicts of interest need to be avoided so that the benefits of opportunistic behaviour are minimised.

Another game theory game, the *Stag Hunt*, is less well known than the Prisoner's Dilemma, however, its probably more suited to this paper. Moreover, the Stag Hunt game is also known as the *Assurance Game.* Assurance being core to building trust highlights the importance of this game. An important focus is, if one-side thinks the other will cooperate, they also prefer to cooperate. This means that players with the Assurance Game preferences are trustworthy. Kydd states: *"They prefer to reciprocate cooperation rather than exploit it"*. This denotes that it makes sense to reciprocate whatever one expects the other side to do, trust or suspicion.

The Stag Hunt (assurance game) is about two hunters who can either jointly hunt a stag (an adult deer/buck, a rather large meal) or individually hunt a rabbit (tasty, but substantially less filling). Hunting a stag is quite challenging and requires mutual cooperation. If either hunts a stag alone, the chance of success is minimal. Hunting a stag is most beneficial for the group however, requires a great deal of trust among its members. Each player benefits most if both hunt stag. Thus, hunting a stag both players trust their counter-player to do the same. Conversely, a player hunting rabbit lacks trust in the counter-player. Deciding not to risk the worst possible outcome (not getting the stag) is to decide not to trust the other player. On the other hand, *"if trust exists then risk can be taken"* [16].

Cooperation is possible between trustworthy parties who know each other to be trustworthy. This can be likened to the CEO, the board of directors, and the investors. They need independent and objective assurances that the other party is trustworthy. In the Prisoner's Dilemma, cooperation can be sustainable only if the players care enough about future payoffs because they will fear that attempts to exploit the other party will be met with retaliation [24]. In the Assurance Game (Stag Hunt) the level of trust one party has for the other party is the probability that it assesses the other party as trustworthy [23].

Kydd adds that the minimum trust threshold will depend on the party's own tolerance for the risk of exploitation by the other side. To consider the situation of the CEO, board of directors and the investors, cooperation needs to be the overwhelming option to avoid cheating and mistrust. This leads back to the elements of the trustworthiness model proposed by Mayer et al. [7] that integrity, benevolence and ability are required. The best option is clearly the hunting of the stag together, as it maximises the return on effort and becomes a win win situation. Applied to a corporate setting it illustrates the need for positive cooperation and trust between the various stakeholders and the avoidance of conflicts of interest.

The development of positive uncertainty reduction should be the basis for engaging in cooperative behaviour. When a positive piece of information about the company is presented (financial statements with assurances), the uncertainty will be reduced, as a result, the chance of engaging in cooperative behaviour will be increased. In contrast, where higher uncertainty levels exist between parties, or a piece of information negatively confirms predictions, then the competitive course of action will more likely to be engaged. In a cooperative situation, both participants feel that they are perceived as benevolent. Therefore they can willingly place themselves in vulnerable positions. Under this condition, the various parties are likely to establish or perceive a relationship of mutual trust. This again highlights the point that the stakeholders need assurances to trust the information found within the financial statements (validation by auditors). This emphasises the importance of information security and that it should safeguard the *accuracy* (fraud) and *reliability* (confidentiality, integrity and availability) of information.

3 Risk, Security and Assurances

It is vital that positive predictability needs to occur for trust to increase between the various parties (stakeholders). Therefore one should ensure that through various security mechanisms, the information found within the financial statements is correct. The knowledge, via independent and objective assurances, that information security is adequate and the risks contained assist in building confidence.

3.1 The Dark-Side of Trust: Risk

Queen Elizabeth 1st in her address to Parliament in 1586 concluded with: *"In trust I have found treason"* [25]. At what stage of a relationship is one relying on trust to the point that one is overly exposed to risk? In perfect competition, Humphrey and Schmitz [26] contend, *"risk is ruled out by the assumptions of perfect information and candid rationality"*. However, they emphasise that in today's world the issue of trust exists because transactions involve risk, as we do not have perfect competition.

Noorderhaven [27] observes that in context of a transaction relationship, if adequate security safeguards are in place for a transaction to go ahead, then it is not a trust transaction. However, if the actual information security safeguards and controls in place are less than adequate, a trust-based relationship is assumed as the existence of trust is inferred.

To expand on this, risk is present in a situation where the possible damage may be greater than the possible return [28]. Therefore, as stated [5], *"risk creates opportunity for trust"*. This is in harmony with Gefen et al. [14] and game theory [18, 20] that postulate that trust can *grow* and *evolve* over time.

It highlights the premise that trust can decrease uncertainty about the future and is a requirement for continuing relationships where parties have opportunities to act opportunistically [29]. This is in agreement with the theory that trust affects the trustor's risk taking behaviour [7]. To summarise, if the level of trust surpasses the perceived risk, one would engage in the relationship. Nevertheless be cautious, as trust is the positive view of risk exposure as *"trust is risk*" [30].

3.2 Trust and Security

Camp [1] is an advocate that both *"technical competence"* and *"good intent"* are required to ensure security. She further emphasises that: efforts at securing systems should involve not only attention to networks, protocols, machines and policies, but also a thorough understanding of how social agents (individuals and parties) participate in, and contribute to trust. One can lose sight of the fact that conventional security technology, if implemented perfectly, still does not equate to trust [19].

Although it may be desirable, 100% security is not feasible and it is commonly accepted that not all risk can be eliminated [31]. This residual or inherent control risk is based on the notion that additional investments in controls or safeguards will not eliminate this type of risk. This means that the various company stakeholders are forced into a trust-based relationship.

It is widely accepted that reduced risk and increased trust are both likely to increase the likelihood of engaging in transactions [14]. DeMaio [32] champions that one should try to build business environments based on each party's willingness and ability to continuously demonstrate to the other's satisfaction that all dealings are honest, open, and that the 'rules' are followed. DeMaio states, *"e-Trust is all about mutual assurance."*

3.3 Mutual Assurance and Confidence

Mutual assurances help to build confidence between the various company stakeholders in a similar manner as with the hunters in the Stag Hunt/Assurance game. In the same manner, VeriSign can provide confidence that an active key-holder has signed a document and it can be assumed that the document is untainted because of VeriSign's independence. Therefore, it follows that auditors verify a company's financial statements (validation) and provide assurances. The only difference is that VeriSign and the Stag Hunt game provides the assurance in real-time, something the auditing profession needs to address.

Mutual assurance should exist between stakeholders, reassuring each other that the risks are mitigated to an acceptable level and that the degree of (un)certainty is appropriate. The adage of *"trust but verify"* should exist as the various stakeholders demonstrate to each other, via objective and independent audits, that the agreed upon best practices are maintained.

The confidence that the various company stakeholders have in their relationship is determined by two factors: one being the level of trust and the other the perception of how adequate or inadequate the controls are that govern the conditions of the arrangement [33]. To achieve a favourable relationship between the stakeholders, one has to find the right *balance* between trust and control.

Fig. 2 illustrates how trust and controls work together in securing a transaction or a business process. Triangle A, B, D is the *Control* area and triangle A, D, C is the *Trust* area. The line E, F is a hypothetical positioning of the company's Risk Appetite. The area of the rectangle A, B, D, C is the business process area or transaction area. When one views the Risk Appetite line (E to F) one will note that the white area is protected by controls and the dark area is the 'risk' exposure or the area protected by trust. Depending on how much the parties '*trust*' each other will affect the positioning of the Risk Appetite line.

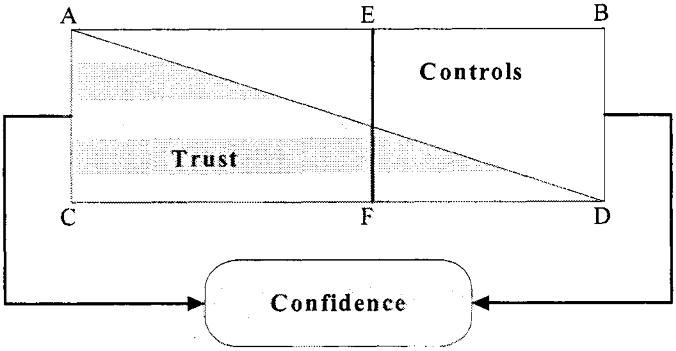

Fig. 2. The Relationship between Trust, Controls and Confidence.

However, to summarise: absolute trust and absolute control are two opposing extremities of approach for attaining confidence (personal communication, Todd, August 2005). The solution is somewhere in the middle ground between trust and control. There are those that argue the company should position itself on the trust side in an effort to reduce costs [34, 35]. However, practicalities and realism are *forces* that pull the solutions into the control end of the spectrum.

4 A Trust Strategy

Strategy, by its nature, concerns itself with the future. Companies today operate in an uncertain world where the markets have become increasingly more competitive. The Turnbull Report [36] emphasises that taking risks is what companies do. It is the justification for profit and therefore the identification and assessing of risks is required so that the risks are appropriately managed.

A company should craft a strategy considering their relationship with their various stakeholders. An important aspect of this strategy is managing the uncertainty of future events i.e. managing and containing the risks to an acceptable level. The board of directors should consciously attempt to *build* and *safeguard* trust between them and their investors.

Todd [35] researched trust in the technical arena, specifically focusing on e-commerce. He divided trust into two domains and had subsections in each domain. Todd based his research on Gerck's work [37]. Gerck appears to have originally divided trust into these two domains, *establishing* and *ensuring* trust. Additionally, Gerck focused on trust and risk refinement as a means of reducing uncertainty.

For the purpose and focus of this paper, the domains have been renamed to *Building* and *Safeguarding* trust and the subsections have been modified accordingly. From the study of the concept of trust it appears that one builds trust over time and then one needs to safeguard trust due to its fragile nature. The following are points (Table 1) which must be taken into account when one considers building and/or safeguarding trust.

Table 1. Building and Safeguarding Trust.

Building Trust	**Safeguarding Trust**
Benevolence/Openness	Risk Management
Ability/Competence	Security Safeguards and Controls
Integrity/Predictability	Compliance
Constant Communication	Recourse Mechanisms
Ethics	Governance
Assurances	'Assurances'

A company, in their strategy, should attempt to mitigate their risks to an acceptable level by reducing the value of opportunistic behaviour from occurring. Moreover, information security audits should be preformed to assure that the technical side of security is adequate as security helps to safeguard trust. Additionally, assurances help to establish trust in the level of confidence placed in the information. The assurances establish a more accurate level of trust *(the truth)* as to the condition of security safeguards and controls. To refer back to the Stag Hunt/Assurance Game, it is the assurances provided by one hunter to the other that keep them *'confident'* that both parties are committed to the hunt. If not, insecurities 'creep' in and alternatively a hunter may decide to hunt a rabbit and the Stag Hunt collapses. Establishing trust sets a level of confidence.

5 Conclusion

Trust and information sharing between the various company stakeholders has taken place since formal commerce began. The information's integrity is of utmost importance, especially the information found within financial statements. This information needs to be trusted. However, the various stakeholders have their own goals and motivations in addition to the shared goals. Conflicts of interest arise and each party is vulnerable. Each also needs to trust the other to have integrity, benevolence, and ability. Companies should have a trust strategy to guide them in building and safeguarding trust, with independent and objective assurances being part of this strategy.

To have a positive outcome, trust needs to increase and uncertainty needs to be reduced to an acceptable level. This could be through assurances provided by auditors *validating* the *reliability* and *accuracy* of the information (the auditors report on the system of internal controls and the accuracy of the financial statements) or through evolving relationships (as discussed in game theory). *To avoid unfavourable behaviour, uncertainty needs to be contained and the level of trust needs to surpass the perceived risks.* This will ensure that a relationship will flourish. Within a competitive society, the various company stakeholders cannot enter into partnerships with blind trust, believing that everyone will do the right thing [38].

The development of cooperative behaviour and mutual trust should be a goal of all company stakeholders. One cannot escape that trust and controls affect confidence and is the acceptance of a degree of insecurity (as shown in Fig. 2). In conclusion, both *"technical competence"* and *"good intent"* are required to ensure security [1]. Therefore, *confidence in information security management requires trust and trust requires information security to help safeguard it.*

Acknowledgement

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

1. Camp, L.J.: Designing for Trust. In: Falcone, R., Barber, S., Korba, L., Singh, M., (eds.): Trust, Reputation, and Security: Theories and Practice. Springer-Verlag; Berlin Heidelberg New York (2002) 15-29.
2. Ratnasingham, P., Kumar, K.: Trading Partner Trust in Electronic Commerce Participation. (2000) http://portal.acm.org/citation.cfm?id=3598.
3. King II Report: King Report on Corporate Governance for South Africa. Institute of Directors in Southern Africa (2002) 17-19.
4. Handfield, R.B., Nichols Jr., E.L.: Supply Chain Redesign: Transforming Supply Chains into Integrated Value Systems. Financial Times Prentice Hall, New Jersey (2002).
5. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not So Different After All: A Cross-Discipline View of Trust. Academy of Management Review. Vol. 23(3) (1998) 391-404.
6. Johnson-George, C., Swap, W.C.: Measurement of Specific Interpersonal Trust: Construction and validation of a scale to assess trust in a specific other. Journal of Personality and Social Psychology. Vol. 43(6) (1982) 1306-1317.
7. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review. Vol. 20(3) (1995) 709-734.
8. Pearce, W.B.: Trust in interpersonal communication. Speech Monographs. Vol. 41(3) (1974) 236-244.
9. Berger, C.R., Calabrese, R.J.: Some Explorations in Initial Interaction and Beyond: Toward a developmental theory of interpersonal communication. Human Communication Research. Vol. 1 (1975) 99-112.
10. Berger, C.R.: Communicating Under Uncertainty. In Roloff, M., Miller, G. (eds.): Interpersonal Processes: New directions in communication research. Sage, Newbury Park USA (1987) 39-62.
11. Mishra, A.K.: Organizational Responses To Crisis: The centrality of trust. In Kramer, R.M., Tyler, T.R., (eds.): Trust in organizations: Frontiers of theory and research. Sage, California (1996) 261-287.
12. Abrams, L.C., Cross, R., Lesser, E., Levin, D.Z.: Nurturing Interpersonal Trust in Knowledge-sharing Networks. Academy of Management. Vol. 17(4) (2003) 64–77.
13. Larzelere, R.E., Huston, T.L.: The Dyadic Trust Scale: Toward understanding interpersonal trust in close relationships. Journal of Marriage and the Family. Vol. 42 (1980) 595-604.

14. Gefen, D., Rao, V.S., Tractinsky, N.: The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification. IEEE Computer Society (2002) http://csdl.computer.org/comp/proceedings/hicss/2003/1874/07/187470192b.pdf.
15. Von Neumann, J., Morgenstern, O.: Theory of Games and Economic Behaviour. Princeton University Press, Princeton USA (1953).
16. Kimbrough, S.O.: Foraging for Trust: Exploring Rationality and the Stag Hunt Game. (2005) http://opim.wharton.upenn.edu/~sok/sokpapers/2005/itrust-2005-final.pdf.
17. Murphy, P.: Game Theory Models for Organizational/Public Conflict. Canadian Journal of Communication. Vol. 16(2) (1991) http://info.wlu.ca/~wwwpress/jrls/cjc/BackIssues/16.2/murphy.html.
18. Hayes, F.: Is Game Theory Useful for the Analysis and Understanding of Decision Making in Economics? (2005) http://www.maths.tcd.ie/local/JUNK/ econrev/ser/html/game. html.
19. Khare, R., Rifkin, A.: Weaving a Web of Trust. (1998) http://www.w3j.com/7/s3.rifkin.wrap.html
20. Axelrod, R.: The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration. Princeton University Press, New Jersey (1997)
21. Zand, D.E.: Trust and Managerial Problem Solving. Administrative Science Quarterly. Vol. 17(2) (1972) 229-239.
22. Clarke, T.: Theories of Corporate Governance: The Philosophical Foundations of Corporate Governance. Routledge UK (2004) 11.
23. Kydd, A. H.: Trust and Mistrust in International Relations. Princeton University Press, Princeton USA (2005) 7-12.
24. Axelrod, R.: The Evolution of Cooperation. Basic Books, New York (1984).
25. Partington, A. (ed.): The Oxford Dictionary of Quotations, 4th ed. University Press, New York Oxford (1996).
26. Humphrey, J. Schmitz, H.: Trust and Inter Firm Relations in Developing and Transition Economies. Journal of Development Studies. Vol. 34(4) (1998) 33-61.
27. Noorderhaven, N.G.: Opportunism and Trust in Transaction Cost Economies. In: Groenewegen, J., (ed.): Transaction Cost Economics and Beyond. Kluwer Academic, Boston (1996) 105-128.
28. Luhmann, N.: Familiarity, Confidence, Trust: Problems and Alternatives. In: Gambetta, D.G., (ed.): Trust: Making and Breaking Cooperative Relations. Basil Blackwell, New York (1988) 94-107.
29. Limerick, D., Cunnington, B.: Managing the new organization: A Blueprint for Networks and Strategic Alliances. Jossey-Bass, San Francisco (1993).
30. Camp, L.J.: Trust and Risk in Internet Commerce. The MIT Press, England (2000).
31. Greenstein, M., Vasarhelyi, M.: Electronic Commerce: Security, Risk, Management and Control, 2nd ed. McGraw-Hill, New York (2002).
32. DeMaio, H.B.: B2B and Beyond: New Business Models Built on Trust. John Wiley & Sons, USA (2001).
33. Cox, R., Marriott, I.: Trust and Control: The Key to Optimal Outsourcing Relationships. Gartner database (2003).
34. Fukuyama, F.: Trust: the Social Virtues and the Creation of Prosperity. Free Press USA (1996) 27.
35. Todd, A.: The Challenge of Online Trust: For online and offline business. (2005) http://www.trustenablement.com/trust_enablement. htm#RiskManagement.
36. Turbull Report. Internal Control: Guidance for Directors on the Combined Code. The Institute of Chartered Accountants in England & Wales (1999/2005).
37. Gerck, E.: End-To-End IT Security. (2002) http://www.nma.com/papers/e2e-security.htm.
38. Bavoso, P.: Is Mistrust Holding Back Supply-Chain Efforts? Optimize, and InformationWeek (2002) http://www.optimizemag.com/printer/014/ pr_squareoff_yes.html.