Issues that managers need to consider when undertaking research relating to the cyber environment

Trim, P.R.J. and Lee, Yang-im

This is a copy of a chapter published in: Trim, P.R.J. and H.Y. Youm (eds.) (2015) Korea-UK Initiatives in Cyber Security Research: Government, University and Industry Collaboration, British Embassy Seoul, Republic of Korea, pp. 66-79.

Paper 12: Issues that managers need to consider when undertaking research relating to the cyber environment

Peter Trim and Yang-Im Lee

Introduction

The aim of this paper is to highlight the need for managers in a range of organizations to engage more fully in research relating to the cyber environment and in particular, to help them to undertake research to improve their understanding of what cyber threat intelligence involves. Attention is given to how managers and academic researchers can work together and engage more fully in social science cyber security research.

It is hoped that academics, researchers and managers in a variety of organizations will find this paper of interest as it makes explicit a number of factors that govern partnership arrangements involving supplier organizations, retail organizations and distributors. Furthermore, attention is given to such issues as partnership development in the context of making the organization more robust and better able to put in place policies and procedures relating to counteracting the growing number of cyber threats.

Background

With reference to a cyber risk report featured in Management Today (2014), it is clear that insider crime is an issue and managers are aware of DDos attacks, the work of hackers and the threat posed by viruses and malware. Indeed, one-third of incidents can be attributed to malware that has been designed to steal data and because of this greater attention needs to be given to situational awareness across industrial sectors, cooperation between organizations throughout the public and private sectors, and information sharing across borders (Gibson, 2014). What needs to be remembered is that malware can be in a system for 200 days or more before it is detected (Jopling, 2014). Another key point to note is that there are a large number of tools that can be downloaded and used to commit cyber attacks and in addition, there are a lot of people that have the ability and/or intent to use these tools (Bach, 2014). With regards to rapid change that is shaping the business environment, it is clear that academic researchers need to undertake research that allows them to better explain the complexities that are giving rise to new business models and which require new forms of decision-making to be deployed. When a cyber attack is launched upon an organization, it is likely that the impact will have an effect both upon the organization itself, partner(s) organizations, and various customer groups. If the impact is severe and a major disruption occurs, senior management must ensure that the image and the reputation of the organization and its partner(s) is restored as soon as possible. Hence it is essential that a risk communication strategy is in place. Indeed, ENISA (2011: 3) make clear the fact that an organization's risk management strategy encompasses a communications policy that is embedded within the management of risks approach.

According to Trim and Lee (2014: 80-81), "A risk communication strategy must therefore be grounded in the business continuity management planning framework and if an impact does occur, the recovery process can be as rapid as possible owing to the fact that the procedures are adequately documented and those in charge or associated with the recovery process are competent to ensure that it goes ahead as planned".

Key issues and challenges for managers

The process of internationalization has focused the attention of managers on a range of important activities including environmental scanning; the changing landscape of retailing; and in particular, how retailers formulate and implement strategies (Akehurst and Alexander, 1995; Howe, 1998, p. 215). This brings to the surface a number of issues such as the type of business; the location of the business; how goods are to be selected, distributed, and displayed; and how channel partners are managed (Walters, 1979, p. 215; Lewison and DeLozier, 1986, p. 45 and p.63; Lewison, 1997, p. 8; Morganosky, 1997, p. 269; Martin et al., 1998, p.114; Siguaw et al., 1998, p. 99). The concept of reciprocal relationships vis-à-vis channel partners has received attention (Sparks, 1995), and so too has technology utilization. As regards the latter, managers in the retail sector are becoming increasingly aware of how connectivity and interactivity between organizations is facilitating business relationships and how strategic management intelligence decision-making needs to take into account cyber threat activity. What is important to note, is that the cyber environment in which organizations compete and form cooperative working relationships with other organizations, is undergoing constant and rapid change and forcing managers to think in terms of managing risk and uncertainty more pro-actively than they did in the past. Indeed, the range of threats and the problems associated with inadequate security systems, is forcing managers to think more about putting in place a corporate security system that incorporates counterintelligence. The reason why managers need to give this attention is because employees are increasingly engaging in remote working and as a consequence criminals will have more opportunity to steal sensitive information (Jones, 2014). This is a highly relevant observation bearing in mind that managers are confronted with the challenge of managing the due diligence process in association with third parties and supply chain activities (Jones, 2014). The problem becomes more complex in the sense that a large amount of data that employees handle is no longer stored in the company's data centre and also, it is known that "52 per cent of workers use 3 or more devices daily" (Hardy, 2014). Selman (2014) is clear that a structured cyber security model has a number of advantages and has highlighted risk assessment, supplier profiling, supplier assurance and compliance, and this can be considered widely and placed in the context of a partnership arrangement involving companies from both the private and public sectors. One way forward is for senior management to engage more deeply in threat intelligence and this means that managers need to collect and analyse data and information from a number of different sources, and to formulate policy to deal with these threats (Samtani, 2014). This can be facilitated by placing data/information in an active cyber defence cycle (incident response, threat and environment manipulation, threat intelligence consumption, and asset identification and network security monitoring) (Samtani, 2014). What managers need to be aware of is that "individual threats have multiple vectors" and because of this they need to formalize the process of identifying threats and classifying threats, so that all the points of attack are covered (Tailor, 2014). By adopting a more focused view as to what strategic intelligence represents (Trim and Lee, 2007), it should be possible for senior managers to think in terms of making the organization more resilient (Trim and Lee, 2008a). This can be achieved through the development and deployment of strategic cyber security management models, frameworks and software packages.

What needs to be noted, is that the cyber environment in which organizations carry out their daily operations, is witnessing a different degree of interdependency materialize. For example, global operations require that management put in place a technically proven and tested iGRC (integrated governance, risk and compliance) framework and system, which incorporates outsource contracts information and operational analysis necessary to operate

the controls and metrics necessary for sustained iGRC management in a cyber environment that will increasingly become dependent upon adaptive risk management (Trim and Lee, 2010, pp.1-2). Hence the need for management to engage in cyber intelligence. According to Mattern et al., (2014: 704): "Cyber Intelligence seeks to not only understand network operations and activities, but also who is doing them, why, and what might be next … …… Cyber Intelligence should drive the cybersecurity mission. Intelligence-led operations require (a) a proactive security posture, (b) a thorough, accurate, timely understanding of the threat environment, and (c) a commitment to decisions based on data".

Strategic cyber security management models

What is focusing the interest of academic researchers is the increasingly complex and integrated network structures that are evolving, which are resulting in a higher degree of interdependency between organizations. Of concern to managers are longer lead times and shorter product life cycles, and if additional factors such as governance, risk and compliance are included, it becomes increasingly obvious that risk assessment and risk mitigation need more attention. In order to manage risk more adequately during periods of increased uncertainty, most notably changes in market dynamics (Trim and Lee, 2010, pp.1-2), it is necessary for managers to adopt a more pro-active approach to studying threats in the external environment and to devise an adequate SLEPT (Social, Legal, Economic, Political and Technological) analysis that can be used by strategists to put in place a strategic cyber security management model that will counteract various cyber threats.

The substitutability of suppliers; their indispensability; and common interests all need to be taken into consideration (Krapfel et al., 1991), if that is the organization's risk appetite is to remain at an acceptable level. Siguaw et al., (1998) have empirically examined the effectiveness of suppliers' marketing orientated behaviours on channel relationships and have produced a conceptual model. They have also focused attention on a distributor's marketing orientation approach, and have covered such important topics as trust, cooperative norms, commitment and satisfaction. Siguaw et al., (1998, pp.106-107) have provided research findings which indicate "that a supplier's market orientation affects the distributor's market orientation, and commitment to the relationship". Baker et al., (1999) support this view and suggest that commitment is very important, and is based on perception and cooperative norms. Distributors adopt the supplier's marketing orientation approach, because managers based in the distributor are committed to achieving higher financial returns, the outcome of which is increased levels of satisfaction.

It is worthwhile at this point to reflect upon advice given and acknowledge the fact that a cyber attack can come from a number of sources. Although the necessary controls may be in place, it may not prevent an attack getting through because the controls have not been implemented effectively (Clelland, 2014). It is sound advice therefore for management to test each control and ensure that it performs to the level required (Clelland, 2014).

Partnership related issues and research

At this point, it is useful to reflect and to suggest that during the initial stage of a partnership's development, a governance mechanism helps to integrate the various decision-making processes but needs to be viewed as flexible. This is due to the complexity of the socio-cultural environment and the business conditions that prevail and which are subject to change. Another point that should be noted is that senior managers may contemplate

establishing a hybrid organizational partnership culture that embraces national cultural traits, however, in the context of the cyber environment, it is most likely that because of the high degree of Internet linkage, technology itself becomes the greatest influencer as regards organizational configurations as opposed to an individual organization's value system and power oriented relationships.

It is obvious, therefore, that the concept of partnership needs to be placed in a wider context than is the case at present, and a partnership arrangement needs to be viewed from the perspective of mutuality. This being the case, the term partnership will become increasing understood as a method for fostering continual learning as staff in partner organizations adopt a pro-active, adaptive and risk sharing approach to doing business. Trim and Lee (2008b, p.223) have provided a useful interpretation of what a partnership arrangement constitutes: "An all embracing mutually oriented mechanism that allows staff within an organization to identify, devise and implement a legal instrument that results in combined ownership, an integrated management model that is underpinned by a hybrid organizational culture, which gives rise to a clearly defined mission statement and marketing strategy".

Business intelligence

A host of factors can be identified by managers that shape retailing landscapes, but speed of new product development and marketing mix considerations (Walters, 1979) are considered to be very important. Managers will, because of the level of complexity, need to avoid falling into the trap of thinking in terms of traditional retailing methodology and instead, need to adopt a forward thinking marketing approach that focuses on identifying and satisfying unmet needs. Meeting customer expectations is central to a retailing strategy being successful, however, establishing mutually oriented channel partnership arrangements that embrace facilitating technology are at the heart of the situation. Managers will need to embrace the strategic marketing concept (Aaker, 1984) more fully and also, develop a better appreciation and understanding of the role that marketing intelligence officers play (Trim and Lee, 2005; Trim and Lee, 2007). Another point that needs emphasising is that marketing intelligence officers need to possess analytical and interpretive skills. They also need to be aware of and have an appreciation of what business intelligence (BI) is and can deliver. For example, Maguire and Suluo (2007, p.21) state: "The future of retail BI will be defined by the retailers that have figured out how to maximize customer satisfaction and profitability with the right combination of quality products, friendly and efficient service, unique value, a differentiated shopping experience, and a business model that truly serves its community-locally and globally. This will be accomplished by starting with understanding the customer and then linking that insight into every decision that is made, from merchandising to marketing to distribution to store operations to finance, so that retailers can predict how to best serve their customers' ever changing needs and desires".

Managers, strategists, marketing intelligence officers, marketing researchers and organizational specialists concerned with business continuity need to be involved in identifying future cyber threats. Hence research needs to be undertaken to link firmly with corporate intelligence activities. This means that managers need to authorize industry forecasts and engage in scenario planning. As regards an organization's vulnerability, Sheffi (2005) has highlighted a useful and some would argue necessary approach to resilience and what emerges from the discussions is that there are several ways to reduce an organization's level of risk. One way is to identify and select trustworthy business partners that avoid opportunistic behaviour, and this may support the argument for a collectivist approach to

decision-making. Hence business-to-business relations can be viewed from the stance of "mutual market responsibility" (Walters, 1979, p. 214) and should this be the case, managers can implement what is known as an integrated systems approach that relies upon up-to-date marketing intelligence that incorporates an ethical approach to data collection and usage (Carrigan and Kirkup, 2001, pp. 415-435).

Partnership development

By ensuring that each organization in the partnership arrangement has a recognizable mission statement and also, that each of the mission statements is underpinned by a set of similar values, managers can reduce each of the organization's level of vulnerability. Managers in retail organizations do evaluate existing business relationships, negotiate new partnership arrangements, and deal effectively with local government (Lowe and Wrigley, 1996, pp. 13-16; Christopher and Juttner, 2000, p. 119; Porter et al., 2000, pp. 24-25 and pp.29-35), however, in the years ahead it will become even more important than it is at present to undertake a Cyber Security SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. This is because staff based in the Corporate Intelligence function need to relate better to staff based in the other departments and functions if that is a more appropriate governance framework is to be implemented (Trim and Lee, 2010, p.2).

Owing to the fact that change in the business environment means that a partnership strategy locks partner organizations into a location strategy (Wrigley, 1994, p.7; Alexander, 1996, p.24 and p.26), managers need to possess the mindset to negotiate with local government representatives and various other interested stakeholders (Trim, 1999). They can be aided in their efforts by in-house and external researchers who, working in unison with marketing staff and staff from other business functions, identify issues and concerns of importance to senior management, and undertake research and intelligence studies that are aimed at providing answers to recurring problems (both cyber and non-cyber). Researchers will be called upon to identify and then interview industry experts in order to establish key industry drivers; undertake studies to validate the predictions of industry analysts; and organize a number of in-house seminars, workshops and focus groups that are aimed at validating or identifying trends in consumer buyer behaviour for example. By working closely with marketing intelligence officers, strategists and competitive intelligence officers, it should be possible for researchers to outline how changes in government regulatory policy results in new market opportunities.

The degree of integration between a retail organization and its suppliers is strongly influenced by the way in which each organization participates in the business relationship and the how managers exercise their responsibilities within the partner organizations. A high level of customer service is closely related with the issue of how retail organizations can create fitness through internal and external harmony. Hence a continuous relationship building process is perceived as essential (Beckett-Camarata et al., 1998, p.78). This can be interpreted from the stance of achieving a sustainable competitive advantage and refocuses the strategy-structure debate. One can think in terms of appropriate organizational design (Germain and Droge, 1997), and how the sharing of information results in a cost advantage. Cost related information is normally classified as confidential and sensitive and can be a source of strategic risk because of the vulnerability aspect (Christoper and Juttner, 2000, p.119). However, information sharing is necessary for developing trust and may be considered a key aspect of doing business (Trim and Lee, 2006). Selecting appropriate channel members is important with respect to an organization achieving vertical marketing

integration and ultimately a sustainable competitive advantage (Cespedes, 1995; Kumar et al., 1995; Weitz et al., 1995; Siguaw et al., 1998).

Trust in the context of a partnership arrangement

Doney and Cannon (1997, p.36) have built on Ganesan's (1994, pp.3-4, and p.15) work; and the work of Kumar et al., (1995); and have provided useful definitions of trust. It is clear, that trust is composed of two components: one is perceived credibility (which refers to the ability to perform satisfactorily a given task) and the other is benevolence (which requires that short-term benefits are given-up for a long-term relationship and mutual benefits). It can be suggested, therefore, that trust is a pivotal element in the strategy process when two or more organizations attempt to build a strong, continuous relationship. Krause and Ellram (1997, p.30) have examined some of the key elements of trust building (such as two-way communication, top management involvement in the development of relationships, the role of liaison teams, and the volume of purchasing from partner suppliers), and have indicated that managers in retail organizations must invest in training and education programmes. Managers in supplier organizations can show that they are committed to partnership development by investing in up-to-date equipment, and training and education programmes that improves the skill and knowledge base of their employees (Ganesan, 1994, p.13; Doney and Cannon, 1997, p.47).

According to Mattern et al., (2014: 704): "A proactive posture relies on well thought out and dynamic defenses, informed by intelligence, to address both actual and potential threats. Ideally, this approach relies on the full spectrum of an organization's capabilities-from network defense, to public relations, legal efforts, and other business operations. Proactive positioning also relies on a comprehensive and accurate understanding (and in as near real time as possible) of one's own network, and the ability to collect and integrate information sources outside of that network to fully assess the threat environment". Possibly a transformational as opposed to a transactional form of leadership is required. Trim and Upton (2013: 53) have stated: "A transformational leader places a high emphasis on trust and trust-based relationships, and considers that employees need to be in harmony with the organization's objectives. This can be interpreted as an individual employee having the same value system as their peers (and other employees) and that there is a match between the employee's value system and the organization's value system, hence internal mutuality".

Engaging in research

Managers operating in the international business environment are involved in a range of data and information gathering exercises relating to market structure; how legislation affects retailing operations; how local retailers can explore product-market opportunities; and how cultural knowledge can aid promotional activities. McAuley (2004) has acknowledged the importance that culture plays in consumer decision-making and suggests that marketers need to be politically aware. Managers can choose between a number of market entry strategies when launching new business ventures abroad. This has resulted in opportunities for retail organizations (Davies and Fergusson, 1995, p. 104) and to some degree changed the emphasis of business-to-business relationships. What can be deduced is that as market opportunities evolve, business relationships are both stimulated and nurtured. However, managers engaged in research seldom authorize ethnographic studies of any kind and this is regrettable because this type of research, which can be placed in a socio-cultural context, can provide evidence relating to how personal relationships are formed; how individuals can be

motivated to develop and maintain personal bonds; and how trust between managers in different organizations can be maintained in times of uncertainty. Ethnographic research can also provide insights into how peer group decisions are made and can highlight the important characteristics of non-formal human interaction (socializing activity). Ethnographic research has the added advantage of providing insights into how the role of power within an organizational setting influences and shapes relationships and organizational activities (both within and between departments) and how power struggles, shape business policy. A partnership arrangement is affected by power struggles from time to time and this needs to be recognized in order that risk reduction is achieved. The role that power plays in relationship building has been addressed by Hingley (2005, pp.66-75) and it can be argued that power play activities and politicking can have consequences vis-à-vis organizational vulnerability.

Methodological approach: fitness for purpose

As regards acquisition strategy, Burt and Limmack (2001, p.18) suggest that takeover strategies do not always meet the expectations of the various stakeholders, and issues such as related versus unrelated diversification spring to mind. Pre-acquisition strategy activity can be researched using qualitative research methods. Both observational research and an attitudinal research survey can be undertaken to explain the activities of the parties involved. It is relevant to note, however, that a great deal of pre-acquisition activity is of a secretive nature and not open to outside scrutiny. Turning to the external environment, although economic analysis is useful it is not always appropriate vis-à-vis understanding the structure of retailing, and the impact that legislation has on business operations (Dawson, 2000; Davies and Itoh, 2001). Another point that has been recognized as influential in retailing, is the role played by small and medium-sized retail organizations. The conceptual framework put forward by Hutchinson et al., (2005, pp.162-168) is useful with respect to exploring the international marketing strategies of small and medium-sized retail organizations and covers a gap in the body of knowledge. The in-depth personal interview method can be used to establish how senior managers in small companies make the decisions that they do and can be used to provide evidence of multi-tasking activity.

It is generally agreed that the qualitative research paradigm provides researchers with a means to obtain insights into various management issues and problems, and Easterby-Smith and Thorpe (1997, p.51) are right to suggest that the qualitative research approach provides an opportunity to understand better the processes associated with management learning.

The grounded theory approach allows the concepts derived from the primary data collection process to be analyzed and the results compared with the theoretical ideas/concepts contained in the relevant literature. It is this flexibility that is not only intellectually stimulating, but enables researchers to think in terms of developing theory, adding to what exists in the form of inductive theory-generating research (Orton, 1997, p.421) and extending the life of a research project.

We are of the view that the grounded theory approach is an acceptable theory building/theory development, methodological approach that involves a number of steps: ‘open coding’, ‘axial coding’, and ‘selective coding’ (Strauss and Corbin, 1990; 1998). Suddaby (2006) is supportive of this view and points out that when using the grounded theory approach, researchers need to be as transparent as possible about the methodological approach itself. We consider the research approach justified as it provides a basis for understanding a complex and interesting phenomenon (Suddaby, 2006, p.636). Indeed, grounded theory can

be viewed as complex, for example, during the axial coding process, the following paradigm model should be adopted: "(A) Causal conditions → (B) Phenomenon → (C) Context → (D) Intervening conditions → (E) Action/interactional strategies → (F) Consequences/outcomes" (Strauss and Corbin, 1990, p.99). One of the advantages of the paradigm model is that it represents a logical approach, which allows researchers to think systematically about establishing causal conditions and thus provides a basis for understanding how a set of relationships are linked. It also allows researchers to add density and precision and these can be considered additional strengths.

Conclusion

Managers in public and private sector organizations need to think about undertaking various forms of qualitative research and quantitative research, on a regular basis, in order to collect data relating to the cyber environment in order to keep up with cyber threats and their possible impacts. Joint research projects can be undertaken with university researchers, and ways can be found to cooperate across industry sectors.

There is no doubt that developments in digital marketing and online payment systems will fashion the way in which business is conducted, and because of this, research needs to be undertaken into how now business models are evolving and what this means for customers and society. By adopting a pro-active approach to researching aspects of the cyber environment, it should be possible to identify immediate and future areas of concern and add to the security and intelligence body of knowledge. It should also allow managers to identify skill gaps and how these gaps can be eradicated through training and educational programmes.

List of recommendations

Recommendation 1: Managers in various organizations need to engage in research with academic researchers to establish the effects (eg., reputational damage) that are caused by cyber security impacts.

Recommendation 2: Managers based throughout a business partnership arrangement need to undertake research into a hybrid organizational culture and establish how such a culture influences the development of a particular business model.

Recommendation 3: Managers in various organizations need to undertake research to establish how staff can engage in and contribute to research projects that study the link between how workers interface with technology.

Recommendation 4: Managers in various organizations can undertake research that studies the adaptive and risk sharing approach to doing business, and link the research findings with the organizational learning concept.

Recommendation 5: Managers can undertake research into how senior managers design a strategic partnership arrangement and how cyber security knowledge transfer occurs that results in a high level of organizational resilience.

Recommendation 6: Organizational staff can undertake qualitative and quantitative research that identifies how individual managers relate to each other in a cross-cultural setting and how a particular business model is formed, implemented and evaluated through time.

Recommendation 7: Studies can be undertaken on a regular basis to establish how effective security policy is implemented with respect to staff working practices in relation to the company working environment, and in particular, what employees do when they take home company owned laptops or use alternative devices to undertake their work.

Recommendation 8: Working with academic researchers, managers can undertake research into developing strategic partnership arrangements with other organizations and establish how a strategic cyber security management model can be developed that promotes and reinforces the concept of mutuality, which gives rise to information sharing.

Recommendation 9: Managers can undertake research into how certain types of cyber attacks should be dealt with and how this can result in a company wide, holistic view of security being implemented.

Recommendation 10: Research can be undertaken that establishes how an organization can be made more resilient through the development and deployment of strategic cyber security management models and frameworks, and cyber security software packages.

Recommendation 11: Research can be undertaken that focuses attention on improving a partner organization's cyber security strategic intelligence capability in relation to new product launches, timely market entry strategies and defensive retaliatory actions against competitors for example.

Recommendation 12: Managers need to think more deeply about security breaches and the wider impact that these might have on customers and society.

Recommendation 13: Research needs to be undertaken in the area of cyber security awareness in order to establish how security training and security education, can be enhanced and how sustainable working relationships can be established between private sector and public sector organizations.

Recommendation 14: Research can be undertaken to establish how managers can undertake risk management and how individuals in organizations can be held accountable for the risk management process, and what type of leadership style is appropriate for managing risk.

Recommendation 15: Management should undertake, on a regular basis, studies relating to cyber security situation(al) analysis and establish how business impact analysis can be formalized.

Recommendation 16: Research can be undertaken to establish what senior management need to do in order to put in place a risk communication strategy and how a communication policy is to be coordinated across business functions. (The risk communication process needs to include all the stakeholders: suppliers, external organizations (eg., design companies), manufacturers, wholesalers and retailers for example).

References

Aaker, D.A. (1984). *Strategic Market Management.* Chichester: John Wiley and Sons.

Akehurst, G., and Alexander, N. (1995). The internationalization process in retailing. *The Service Industries Journal*, 15 (4), pp.1-15.

Alexander, N. (1996). International retail expansion within the EU and NAFTA. *European Business Review*, 96 (3), pp.23-35.

Bach, R. (2014). Government's response to the evolving threat. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Baker, T. L., Penny, M. S., and Siguaw, J. A. (1999). The impact of supplier's perceptions of reseller marketing orientation on key relationship constructs. *Journal of the Academy of Marketing Science*, 27 (1), pp.50-57.

Beckett-Camarata, E. J., Camarata, M. R., and Barker, R. T. (1998). Integrating internal and external customer relationships through relationship management: a strategic response to a changing global environment. *Journal of Business Research*, 41, pp.71-81.

Burt, S., and Limmack, R. (2001). Takeovers and shareholder returns in the retail industry. *The International Review of Retail, Distribution and Consumer Research*, 11 (1), pp.1-21.

Carrigan, M., and Kirkup, M. (2001). The ethical responsibilities of marketers in retail observational research: protecting stakeholders through the ethical 'Research Covenant'. *The International Review of Retail, Distribution and Consumer Research*, 11 (4), pp.415-435.

Cespedes, F. V. (1995). *Concurrent Marketing: Integrating Product, Sales and Service.* Boston, Massachusetts: Harvard Business School Press.

Christopher, M., and Juttner, U. (2000). Developing strategic partnership in the supply chain: a practitioner perspective. *European Journal of Purchasing and Supply Management*, 6 (2), pp.117-127.

Clelland, J. (2014). Why are businesses breached following successful security audits? *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Davies, G., and Itoh, H. (2001). Legislation and retail structure: the Japanese example. *The International Review of Retail, Distribution and Consumer Research*, 11 (1), pp.83-95.

Davies, K., and Fregusson, F. (1995). The international activities of Japanese retailers. *The Service Industry Journal*, 15 (4), pp.97-117.

Dawson, J. (2000). Viewpoint: retailer power, manufacturer power, competition and some questions of economic analysis. *International Journal of Retail and Distribution Management*, 28 (1), pp.5-8.

Doney, P. M., and Cannon, J. P. (1997). An examination of the nature of trust in buyer-supplier relationships. *Journal of Marketing*, 61 (April), pp.35-51.

Easterby-Smith, M., and Thorpe, R. (1997). Research traditions in management learning. In: Burgoyne, J., and Reynolds, M. (Eds). *Management Learning: Integrating Perspective in Theory and Practice*. London: Sage Publications, pp.38-53.

ENISA. (2011). *Risk Management*. European Network and Information Security Agency, pp.1-108. Source:http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-process [accessed 27 February, 2011]

Ganesan, S. (1994). Determents of long-term orientation in buyer-seller relationships. *Journal of Marketing*, 58 (April), pp.1-19.

Germain, R., and Droge, C. (1997). Effect of just-in-time purchasing relationships on organizational design, purchasing department configuration and firm performance. *Industrial Marketing Management*, 26, pp.115-125.

Gibson, C. (2014). Improving the UK's cyber resilience. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Hardy, A. (2014). Endpoint security for the modern enterprise. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Hingley, M.K. (2005). Power imbalance in UK agri-food supply channels: learning to live with the supermarkets? *Journal of Marketing Management*, 21 (1-2), pp. 63-88.

Howe, W. S. (1998). Vertical marketing relations in the UK grocery trade: analysis and government policy. *International Journal of Retail and Distribution Management*, 26 (6), pp.212-224.

Hutchinson, K., Quinn, B., and Alexander, N. (2005). The internationalization of small to medium-sized retail companies: towards a conceptual framework. *Journal of Marketing Management*, 21 (1-2), pp.149-179.

Jones, N. (2014). The changing cybercrime and fraud landscape. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Jopling, P. (2014). Areas to address in cyber security. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Krapfel, R., and Salmond, D., and Spekman, R. (1991). A strategic approach to managing buyer-supplier relationships. *European Journal of Marketing*, 25, pp.22-37.

Krause, D. R., and Ellram, L. M. (1997). Critical elements of supplier development: the buying-firm perspective. *European Journal of Purchasing and Supply Management*, 3 (1), pp.21-31.

Kumar, N., Scheer, L. K., and Steenkamp, J-B. E. M. (1995). The effects of supplier fairness on vulnerable re-sellers. *Journal of Marketing Research*, 32 (February), pp.54-65.

Lewison, D. M. (1997). *Retailing.* Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Lewison, D. M., and DeLozier, M. W. (1986). *Retailing*. Columbus, Ohio: Merrill Publishing Company.

Lowe, M., and Wrigley, N. (1996). Toward the new retail geography. In: Wrigley, N., and Lowe. M. (Eds). *Retailing Consumption and Capital*. Harlow: Longman Group Limited, pp. 3-30.

Maguire, S., and Suluo, H. (2007). Chapter 2: Business intelligence: Benefits, applications, and challenges. In Xu, M. (Ed). *Managing Strategic Intelligence*. Hershey, PA: Information Science Reference , pp.14-34.

Management Today (2014). Are you ready for a cyber attack? *Management Today* (September), pp.28-29.

Martin, D., Howard, C., and Herbig, P. (1998), The Japanese distribution system. *European Business Review*, 98 (2), pp.109-112.

Mattern, T., Felker, J., Borum, R., and Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27 (4), pp.702-719.

McAuley, A. (2004). Seeking (marketing) virtue in globalisation. *The Marketing Review*, 4 (3), pp.253-266.

Morganosky, M. A. (1997). Retail market structure change: implications for retailers and consumers. *International Journal of Retail and Distribution Management*, 25 (8), pp.269-274.

Orton, J.D. (1997). From inductive to iterative grounded theory: zipping the gap between process theory and process data. *Scandinavian Journal of Management*, 13 (4), pp.419-438

Porter, M. E., Takeuchi, H., and Sakakibara, M. (2000), *Can Japan Compete*? Houndmills, Basingstoke: Macmillan Press Ltd.

Samtani, T. (2014). Cyber security – The most important business priority. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Selman, D. (2014). Defence cyber protection partnership – Working together to better protect defence information. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage.* Cambridge, Massachusetts: The MIT Press.

Siguaw, J. A., Penny, M. S., and Baker, T. L. (1998). Effects of supplier market orientation on distributor market orientation and the channel relationship: the distributor perspective. *Journal of Marketing*, 62 (July), pp.99-111.

Sparks, L. (1995). Reciprocal retail internationalization: the Southland Corporation, Ito-Yokado and 7-Eleven convenience stores. *The Service Industry Journal*, 15 (4), pp.57-96.

Strauss, A., and Corbin, J. (1990). *Basics of Qualitative Research.* Newbury Park, CL: Sage Publications.

Strauss, A., and Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. London: Sage Publications.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, 49 (4), pp.633-642.

Tailor, A. (2014). Hiding in plain sight – What's really happening on your network. *The Future of Cyber Security 2015 Conference*. Prospero House, London Bridge, London, 19th March.

Trim, P. R. J. (1999). The corporate intelligence and national security (CINS) model: a new era in defence management. *Strategic Change*, 8 (3), pp.163-171.

Trim, P.R.J., and Lee, Y-I. (2005). The role of marketing intelligence officers in strategic formulation and implementation. In: Coate, P. (Ed). *Handbook of Business Strategy, 2006.* Bradford: Emerald Group Publishing Limited, pp,125-130

Trim , P.R.J., and Lee, Y-I. (2006). Vertically integrated organizational marketing systems: a partnership approach for retailing organizations. *Journal of Business and Industrial Marketing*, 21 (3), pp.151-163.

Trim, P.R.J., and Lee, Y-I. (2007). Chapter four: A strategic marketing intelligence framework reinforced by corporate intelligence. In: Xu, M. (Ed). *Managing Strategic Intelligence*. Hershey, PA: Information Science Reference, pp.55-68.

Trim, P.R.J., and Lee, Y-I. (2008a). A strategic marketing intelligence and multi-organizational resilience framework. *European Journal of Marketing***,** 42 (7/8), pp.731-745**.**

Trim, P.R.J., and Lee, Y-I. (2008b). A strategic approach to sustainable partnership development. *European Business Review***,** 20 (3), pp.222-239.

Trim, P.R.J., and Lee, Y-I. (2010). A security framework for protecting business, government and society from cyber attacks. *5th IEEE International Conference on System of Systems Conference (SoSE): Sustainable Systems for the 21st Century*, Loughborough University, 22nd to 24th June (pp.1- 6).

Trim, P.R.J., and Lee, Y-I. (2014). *Cyber Security Management: A Governance, Risk and Compliance Framework.* Farnham: Gower Publishing.

Trim, P.R.J., and Upton, D. (2013). *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training.* Farnham: Gower Publishing.

Walters, D. (1979). Manufacturer/retailer relationships. *European Journal of Marketing*, 13 (7), pp.179-222.

Weitz, B. A., Castleberry, S. B., and Tanner, J. F. (1995). S*elling: Building Partnerships.* Chicago*:* Richard D. Irwin.

Wrigley, N. (1994). After the store wars: towards a new era of competition in UK food retailing. *Journal of Retailing and Consumer Service*, 1 (1), pp.5-20.