http://dx.doi.org/10.5392/IJoC.2011.7.3.071

Professional Security Management and Investigation for the New Competitive Advantage

Mark Button
Institute of Criminal Justice Studies
University of Portsmouth, Portsmouth, Hampshire, United Kingdom

Julak Lee
Department of Protection & Security Management
Kyonggi University, Gyeonggi-Do, Korea

Hakkyong Kim
Department of Police Science
Korean National Police University, Gyeonggi-Do, Korea

ABSTRACT

This paper is mainly associated with setting out an agenda for the transformation of security by creating a new framework for a security system, which can maximise its effectiveness. Noticeably, this research shows empirically that crimes are getting a major cost to organisations, which if reduced by security and investigations could reap substantial rewards to the finances of an organisation. However, the problem is that the delivery of security is frequently delegated to personnel (e.g. security guards) with limited training, inadequate education, and no real commitment to professionalism –'sub-prime' security, finally causing security failures. Therefore, if security can be enhanced to reduce the crime cost, this will produce financial benefits to business, and consequently could produce a competitive advantage. For this, the paper basically draws upon Luke's theoretical framework for deconstructing 'power' into three dimensions. Using this three-dimensional approach, the paper further sets out a model of how security can be enhanced, utilising a new Security Risk Management (SRM) model, and how can this SRM model create competitive advantage in business. Finally, this paper ends with the six strategies needed to enhance the quality of security: refiguring as SRM, Professional Staff, Accurate Measurement, Prevention, Cultural Change, and Metrics.

Keywords*: Competitive Advantage, Crime Cost, Fraud, Sub-prime Security, Security Management, Security Risk Management*

1. INTRODUCTION

In the increasingly globally competitive markets, organisations are always looking for innovations to enhance their competitive advantage and reviewing their costs to ensure they are as low as can be. There is one area, however, that is neglected by many organisations and that is the security (and investigations) they utilise to protect themselves. It is all too often seen as a grudge cost to satisfy insurance requirements with the cheapest chosen, and/or the quality of security procured does not meet the standards desired [16]. Some aspects of security, most notably the security guard, are also frequently perceived as incompetent, ineffective and a costly burden [28][9][18]. This perception does vary to other aspects of the security system, but ultimately most organisations do not realise the full potential of more effective security with a more appropriate orientation. Given that crimes against organisations generally amount to significant sums, organisations are missing out on potentially large savings in costs (and therefore increased profits) through refocused and better security. This paper will argue for a reconfiguration of security management and investigations, which it will show could reap benefits to organisations, delivering the new competitive advantage. It will start by showing the huge cost of crime to business, before moving on to examine how too much security is 'sub-prime'. The paper will then set out a model of how security can be enhanced utilising a new model, and how this can bring 'competitive advantage'.

2. THE COSTS OF CRIME

* *Corresponding author. E-mail : julaklee@hanmail.net*
Manuscript received Jun 16, 2011 ; accepted Jul.30, 2011

www.kci.go.kr

Unlike the general measurement of crime, the extent and costs of crime to business has not been the subject of the same level of research. In part, this reflects the general challenges of measuring crime [30]. At a national level in the UK, the Home Office has extrapolated data from the UK crime statistics to estimate crimes against the commercial and public sector for 1999–2000 [22]. It found there were about 70,000 robberies, 960,000 burglaries, 29 million thefts from shops, 40,000 thefts of commercial vehicles, 60,000 thefts from commercial vehicles, 270,000 thefts by employees, 1.4 million thefts by others, 3 million acts of criminal damage, and 9.2 million cases of fraud or forgery. The same report also sought to estimate the costs of such crime, including the actual losses and the costs of security measures, as well as the costs to society at large. It found that a burglary cost £2,700, theft from a shop cost £100, theft of a commercial vehicle cost £9,700, theft from a commercial vehicle cost £700, criminal damage cost £890, and robbery or a till snatch cost £5,000 [22].

The Home Office also conducts a commercial victimisation survey. This is based upon over 6000 telephone interviews with retailers and manufacturers. The last survey from 2002, found nearly three quarters of retailers had experienced a crime which included: 70 per cent any property crime, 25 per cent burglary, 23 per cent violent crime as the most common. For manufacturers, 53 per cent had suffered any crime with any property crime experienced by 48 per cent, burglary by 22 per cent, and violent crime by 7 per cent. It also found 18 per cent of retailers, 7.6 per cent of manufacturers had been the victim of an external fraud and 3.7 per cent and 1.6 per cent respectively of internal fraud [40]. The same survey estimated the costs of crime. For retailers, the median cost of theft by customers was £35 with a maximum reported of £26,000 and burglary was £1350 with a maximum £180,000. The most expensive median was theft of vehicles, when not recovered which was £7000, with a maximum reported of £60,000. For manufacturers, theft of vehicles not recovered was also the most expensive median at £5,000 with a maximum of £60,000. For burglary, the median was £1000, maximum £170,000, fraud by employees £1200 maximum £180,000, and fraud by outsiders median £100, but a maximum of £1,000,000.

There are also a number of measures of fraud that are regularly published by private organisations, with one of the most salient, the KPMG Fraud Barometer. There have also been studies to estimate the costs of fraud. The UK National Fraud Authority (NFA) has estimated that fraud cost of the UK economy amounts to £38 billion. The economic climate at the time of writing (May 2011) has not been good, and a common theme in crime trends in the past has been that as the economy declines, with resulting increasing unemployment and rising inequality, property crimes rises, although the strength of the relationship is contested [4][38]. The current economic difficulties have, however, been marked by still decreasing general crime, but rising fraud as the following graphs reveal.

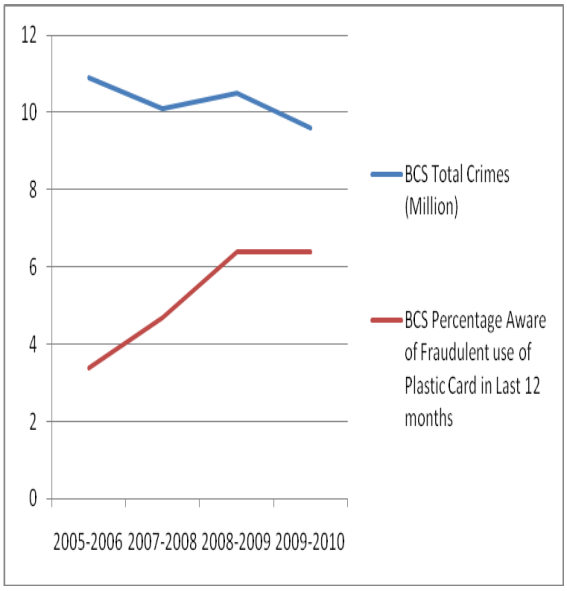

Fig. 1. Comparing the Rate of Credit Card Fraud to Total Crime in England and Wales

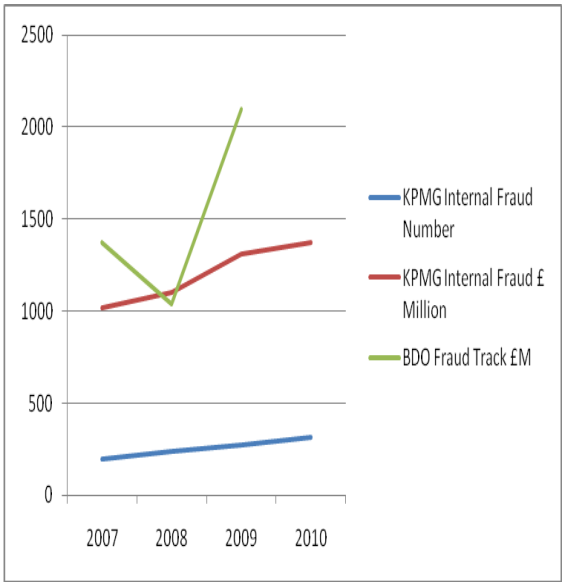

Fig. 2. The KPMG Fraud Barometer/BDO Fraud Track 2007-2010

At an organisational level, research by Gee *et al* [15] has found the average loss to fraud and error for an organisation is 4.5 percent of revenues. In the USA, the Association of Certified Fraud Examiners (ACFE) in their 2006 *Report to the Nation*, which only focuses upon 'occupational fraud' (so excludes external frauds), found the median estimate of losses from corporations revenues was 5 per cent, which if replicated across the world, would amount to $2.9 trillion [2]. Clearly there are some organisations leaking more than 5 per cent in staff fraud which in a large organisation amounts to significant sums of cash. Fraud alone, therefore, is a major cost to organisations which if reduced by security and investigations could reap substantial rewards to the finances of an organisation.

At an industry and organisational level, there is generally

www.kci.go.kr

not a culture of measuring the costs of crime. One of the few exceptions is retailing. In the UK, the British Retail Consortium (BRC) conducts regular surveys of the extent of crime against retailers. In 2005, it found that the average annual losses over the past five years were £2.24 billion [6]. Subtracting the £700 million costs of security from these annual losses, the near £1.5 billion left could be read as the cost of security failure. Depending on the interpretation of the data, it could be stated that despite £700 million invested by retailers in security, there was still £1.5 billion worth of failure or, alternatively, that the investment in security is the reason why failures are held at that level and are not much more costly.

There are also the hidden costs of crime. Many crimes – though not violent – increase fear in employees ultimately increasing stress and impacting upon performance. Employees sometimes may actually experience some form of workplace violence. The International Crime Victimisation survey shows that in Western Europe, 3.6 per cent of men and women have experienced assault at work, with 7 per cent of women experiencing a sexual incident. This compares to North America, where 2.5 per cent of men and 4.6 per cent of women had experienced assault, with 7.6 per cent of women experiencing a sexual incident. In England and Wales, the survey found 3.2 per cent of men and 6.3 per cent of women had been assaulted, with 8.6 per cent of women experiencing a sexual incident [27]. The costs of this problem are illustrated by the fact that in the USA, it has been estimated that between 3 and 7 million working days are lost each year as a result of workplace violence.

3. 'SUB-PRIME' SECURITY

If the quality of security protecting many countries organisations/businesses was operating to the maximum possible, one would have to accept the current level of crime and therefore the costs that result are at a level that cannot be reduced further. However, there is a great deal of evidence to demonstrate that this not the case and the quality – to use the increasingly ubiquitous term – is 'sub-prime'.

3.1 Security guards

> It occurred to me that it was an absurd idea of law enforcement to put an isolated, ill-paid, ill-equipped, security guard in a situation where he might have to confront a gang of seven or eight highly motivated robbers with weapons [32].

Let us begin with the security guards. These are in many ways the symbols of the poor quality of security generally. As the quote from Ross McLeod above demonstrates, putting poor quality security staff in positions to defend organisations is an absurd idea, but is often very common. There is much evidence to illustrate some of the poor quality of security officers. Perhaps the first illustration of quality is the labour turnover in this occupation, which in 2007, Infologue estimated to be 28 per cent in the UK [23]. Even a large and successful security company as Securitas experienced labour turnover of 38 per cent across its European companies during the first six months of 2008 [39]. The structural problem of high labour turnover reflects disquiet over poor conditions of employment. Long hours (50+ per week), pay around the minimum wage, limited career opportunities and basic levels of training [33][42][9]. Many of these issues also arise in South Korea [11][10]. The consequences of these conditions have implications for the commitment of staff to their tasks and an increased chance of security failure. A few examples will further highlight how some of the negative aspects of the occupational culture lead to poor performance.

In one study published on security officers at one of the case study sites, Armed Industries (a manufacturer of aircraft for the military), all staff were supposed to show their passes when entering the site [9]. On gate three, which was one of the quietest and dullest posts the researchers spent two hours with the security officer. During that period, six people did not show their pass. Some of the staff just walked past, completely ignoring the security officer, others said hello, but failed to show their pass. The security officer didn't do anything, claiming that he knew that they worked in the factory and held passes. He told the researchers, 'I don't get paid enough to chase after them!' During another observation session with a female security officer, the researchers asked her on what 'random' basis she selected vehicles. She replied, 'I do a search when I feel like it. I try and pick the easy ones where you can have a quick look' [9]. Hainmüller and Lemnitzer [19] have also observed the link between high labour turnover, low pay and poor training and poor performance in screening at airports by security officers. They argue [19]:

> The causal links between these variables and screening performance are straightforward. Without receiving proper training, screeners will hardly know what to look for … A similar causal link applies to low pay. It is one of the well-proven findings of labour economics that 'you get what you pay for'. Low pay discourages highly skilled workers from applying… The causal mechanism between turnover and performance is as follows: as with most tasks, the performance of screening increases with experience. If, as found in one study (there is high labour turnover) … security checkpoints are rarely staffed with experienced personnel.

These few examples nonetheless demonstrate the impact of structural conditions and occupational culture on the performance of security officers. This paper does not dwell too long on security officers because it is important to investigate the security managers who not only hire them, but who also construct the socio-technical security systems to protect organisations. Here there are also quality issues, but also some of the greatest potential for improvement to security overall.

3.2 The management of security

www.kci.go.kr

When most organisations reach a particular size, they begin to employ managerial specialists to service general management. Most of these are driven by the size, complexity of the organisations and in some cases statutory requirements (such as safety and audit staff). The range and balance of these types of personnel vary between organisations, according to size and business needs. A large-sized organisation will typically have some of the following managerial specialists employed: Human Resource (or Personnel), Health and Safety, Facilities, Purchasing, Marketing, Public Relations, Accounting, Risk, Information Technology, Quality, and of course Security, to name the most popular. Security managers form part of this range of support functions, and generally carry out a wide range of tasks (see Table 1).

Recent research, based upon the Institute of Directors, FTSE100 companies amongst others, has shown that many regard the security function as making an exceptional contribution to their organisations and being ranked only marginally lower than human resources, marketing, and finance [18]. However, the 'professional' status of security managers falls behind some of the other specialist functions. In the UK, a good indicator of an occupation becoming a 'profession' is the representative body receiving 'Chartered Status'. 'Royal Charters', which have been granted since the Thirteenth Century, are now conferred by the Sovereign on advice of the Privy Council, 'for bodies that work in the public interest (such as professional institutions and charities) and which can demonstrate pre-eminence, stability and permanence in their particular field' [37]. To achieve a 'Royal Charter', the Privy Council Office specifies the following criteria as the basis for consideration [37]:

(a) the institution concerned should comprise members of a unique profession, and should have as members most of the eligible field for membership, without significant overlap with other bodies.

(b) corporate members of the institution should be qualified to at least first degree level in a relevant discipline;

(c) the institution should be financially sound and able to demonstrate a track record of achievement over a number of years;

(d) incorporation by Charter is a form of Government regulation as future amendments to the Charter and by-laws of the body require Privy Council (ie Government) approval. There therefore needs to be a convincing case that it would be in the public interest to regulate the body in this way;

(e) the institution is normally expected to be of substantial size (5,000 members or more).

It is worth considering the position of security managers vis-à-vis some of the most comparable other management functions, as set out in Table 1.

Table 1. Selected management and management support functions compared

Management Function	Professional Body	Chartered Status and Year Achieved
Security	The Security Institute	Not yet achieved
Risk	Institute of Risk Management	Not yet achieved
Facilities	British Institute of Facilities Management	Not yet achieved
Quality	The Chartered Quality Institute	2006
Public Relations	Chartered Institute of Public Relations	2005
General Management	Chartered Management Institute	2002
Health and Safety	Institution of Occupational Health and Safety (IOSH)	2002
Human Resources	Chartered Institute of Personnel and Development	2000
Purchasing	Chartered Institute of Purchasing and Supply	1992
Marketing	Chartered Institute of Marketing	1989

As the table shows of the various management functions listed, the only functions that have not achieved Chartered status alongside security are facilities and risk. These two are also much further along the route to Chartered status with larger memberships, suites of professional courses and feeder courses from higher education establishments accredited by them. The Security Institute has only just launched entry level qualifications (Certificate in Security Management) which is sub-degree level, and it remains to be seen how even this low level award is taken up by the industry.

When further evidence is illustrated concerning the characteristics of security managers, it is further demonstrated how security managers lag behind other support functions. There is a common perception that security managers are former police officers or ex-servicemen. Unfortunately there has not been much recent research to quantify this. The most recent research carried out by Hearnden [20][21], found no fewer than 86 per cent of security managers were recruited from a military or police background. In 1991, this had declined to 76 per cent and 61 per cent by 1993. If the research was conducted today it would probably show dominance of the military and police, but not to the same scale. Given that security management is often a second career, it is no surprise to discover the average age found by Hearnden [20] was 50.2 years. Hearnden [21] also discovered some negative orientations concerning training and education. Of the surveyed security officers he found:

www.kci.go.kr

- 62 per cent had no vocational qualifications and managers rated the possession of them as the fourth least important attribute of a good security manager.
- 38 per cent had not attended in the previous two years at least one outside course or seminar.
- 59 per cent worked for organisations which had no formal training needs analysis.
- 40 per cent were unable or unwilling to identify a single personal training requirement.

Again one must stress that the research is dated and since it was published, there has been an expansion in higher education related to security. Nevertheless there are still many working in the industry as a second career after the military or police to supplement their pensions, who have not undertaken any further education or training, or that which they have is of a relatively low level. In many areas, self-perpetuating ex-military and ex-police appoint subordinates and successors from the same background as themselves.

This second career mentality does have some negative consequences. It may influence many managers' orientation as the job is a supplement, and it is something that many have achieved through their experience, rather than qualifications. For some, there is little incentive or desire for further training and education. When security management is juxtaposed against other managerial specialisms, such as personnel, safety, risk etc., these are dominated by people who have made it a first choice career, who are in it for the long haul and as a consequence are prepared to invest time in securing the appropriate development through training and education to achieve their position.

Perhaps another illustration of the lack of commitment to training and education amongst many managers are the limited learning routes into security management. Training and educational achievement are of marginal importance in the broader security occupation. There is no recognised industry benchmark qualification for entrance and there are only a limited number of Higher Education courses provided by Universities, when compared to other specialisms, such as safety and computer security [8]. Although this is beginning to change with the Security Institute, launching a Certificate and Diploma in security management aimed as entry level awards. It remains to be seen, however, to what extent these will become the currency of entrance to managerial positions in the security industry.

There is not a great deal of research to assess the quality of security management, but there is a degree of anecdotal evidence. In a study of the value of security, Gill *et al* [17] found some damning criticisms of security management. It is worth repeating verbatim some of the comments they recorded:

> …most senior security people are just plain thick. Many cannot write basic policy or process, as much as they may understand what needs to be achieved and they cannot articulate a business case' [17].

Another interviewee in their study stated:

> From police and military I have seen a few who are good and there has been a missing of significant opportunities for business. Especially the ex military, they are like kids with no organisational awareness. Their people skills and ability to understand cultures of business are lacking because they have not grown up in a business environment. In something like nuclear work then a military background maybe important. The greater the competitive environment in which a company participates the less easy it is to appoint someone from a military background. There needs to be the most effective cultural fit [17].

Evidence has also been found of some security managers lacking knowledge and understanding of how to prevent problems from occurring and been too reactive. As Challinger argues [12]:

> Some security decisions appear to be made after a breach of security has occurred. Some are made when it is simplistically assumed that continued security is no longer needed. Some are made when it is feared that business will be lost if security is not in place to reassure customer.

Challinger also goes on to argue that many decisions made in security are not based upon evidence. In the well established professions, such as medicine, a doctor will prescribe a treatment or advice on preventative measures that are based upon scientific evidence, and will also no doubt keep up to date on the latest advances through reading appropriate journals and attending conferences. Perhaps another good illustration of the quality of some security managers is their influence in the boardroom. As Garcia argues [13]:

> A common theme of customers of security professionals alike is that the business for security must be made in order to acquire the resources necessary to protect assets. It is agreed that this is a necessary step, but there appears to be a lack of preparation by many security professionals in making this case, particularly compared to their peers in other divisions across the enterprise.

There are many challenges to getting security taken seriously in the boardroom. To many boards, it is not considered as a priority, and security is not also integrated into the broader strategies [12]. Some consider security is not a problem because they wrongly believe there are no problems of staff theft, fraud or comparable incidents. Some boards actually consider security a nuisance getting in the way of the core business and creating bureaucracy. Worse, some boards might even consider security is the enemy harassing 'honest' staff. Therefore the skills required by a

www.kci.go.kr

security manager need to include the ability to persuade board managers by talking their language and fitting their agendas. Unfortunately for many organisations, there is a belief anyone can do security [12].

4. COMPETITIVE ADVANTAGE

> …the business of security has shifted from protecting companies from risks, to being the new source of competitive advantage [15].

This paper has demonstrated how much crime costs organisations and then the limited quality of security that is utilised to protect them. If security can therefore be enhanced to reduce the cost, as a result of an investment that does not amount to more than the benefit, this will produce financial benefits to an organisation. If benefits reaped are better than competitors, this could produce a competitive advantage.

The National Health Service (NHS) in the UK is one of the largest organisations in the world. In the late 1990s, it was realised there was a fraud problem, and new structure was created with a strategic approach to tackling fraud. The approach was initially targeted at fraud alone – subsequently extended to security – and research has demonstrated very positive results. The NHS Counter Fraud and Security Management Service (NHSCFSMS) reckons to have saved the NHS £811 million from fraud, which amounted to a 12 to 1 return on the investment in the NHSCFSM [36]. Even if such returns can be yielded that only half as good on fraud alone, it demonstrates the potential cost benefits to organisations. Indeed, as the quote from Briggs and Edwards above illustrates, there are already some realising the potential benefits of more effective security. What is required, however, is more than pursuing strategies to enhance the quality of security, although these are welcome. What is required is a reconfiguration of the way that security is done.

4.1 Reconfiguring as SRM

From their research on the value of security, Gill *et al* [17] were able to identify two models of security manager (ideal types). The main characteristics of the model are set out in Table 2. The 'traditionalists' are associated with ex-military and police personnel, while the 'modern entrepreneurs' tend to be from more conventional business backgrounds. It is, however, important to add a caveat to the model that not all ex-military and police fit the former category and that not all those from business backgrounds fit the latter. The authors have met security managers from the police and military who would fit into the latter category, as well as 'traditionalists' with no police or military experience. The model, however, does provide a useful basis for debate on the kind of security manager required. There are clearly parallels to the debates in the 1970s and 1980s over personnel management, with many advocating and embracing human resource management (HRM) as a more appropriate model, in which the functions of personnel are more closely aligned to the business objectives of an organisation [1][24]. The clear drift of Gill *et al*'s report is that more security managers should become 'modern entrepreneurs'.

Table 2. Gill *et al*'s model of security managers

Traditionalists	Modern Entrepreneurs
- Security is a service function. - Necessary cost on bottom line. - Experience of police and military important in running security. - Organised by command and control. - Success measured in arrests.	- Security part of business process. - Security integral to all activities. - Importance of influencing people and policies. - Emphasis on change management. - Importance of objectives, strategy, measurement, ROI and impact on bottom line. - Business skills more important than security expertise.

It is important to note here this paper is not arguing that former members of the police, the military and other comparable occupations should be banned from the private security industry (although restrictions do exist in some countries). They can bring valuable experience and be part of networks that are very useful to enhancing security [5]. Rather those who become security managers should also have undertaken appropriate professional training and or academic study in security.

The most important change towards making security the source of competitive advantage is a reconfiguration of security management towards Security Risk Management (SRM). This requires changes similar to the transformation of personnel HRM. During the 1970s and 1980s, personnel management transformed to HRM with a new orientation and higher status [24]. This was achieved without any direct statutory intervention. The HRM experience offers some valuable insights on the 'route map' to professionalisation.

A number of strategies were pursued by personnel managers in order to achieve the status of a profession. McGee [31] contrasts the status of personnel managers in the 1970s and early 1980s to the situation today. He paints a picture of personnel managers with few if any specialist qualifications, neglected in strategic decision-making in the organisations they served, criticised by major government reports, such as the Donavon Commission as lacking professionalism, and represented by more than one professional association, with many not represented at all. This contrasts with a situation in which HRM has become a dominant model and where personnel functions are integrated into the broader strategic goals of the organisation. Although in some cases the transformation from personnel to HRM has been little more than name changes [1]. The two main representative associations, the Institute of Personnel Management and the Institute of Training and Development, merged in 1994 to create the Institute of Personnel and Development, which has since achieved the prestigious 'Chartered' status. Almost all those working in

www.kci.go.kr

HRM/personnel belong to this organisation, which boasts over 130,000 members. The Chartered Institute of Personnel and Development (CIPD) has a staff of 260, lobbies for the profession, is represented on many key forums, produces various publications, and runs seminars and conferences as well as providing a local branch structure.

Most significantly the CIPD has established a membership framework that begins with Affiliate, Associate, Licentiate and Graduate; rising to the Chartered grades from Chartered Member and Chartered Fellow to Chartered Companion. These grades carry weight, with many job advertisements specifying a particular level or an expectation that such a grade will be achieved. The membership grades – depending upon the level – can be achieved through training, higher education and assessment of professional competence. The CIPD also has a code of ethics that if breached can lead to expulsion, something which in many situations means an end to working in HRM/personnel. The CIPD also does much to manage the image of the profession to ensure it is portrayed in an appropriate light.

Learning from this experience, enhancing security management requires the following initiatives. First security management needs to be reconfigured to more closely meet the needs of business. There are five principles to redefining security management as Security Risk Management (SRM):

(a) Integrating security in the core aims of the organisation*:* Security risk management should be aligned as far as practicable in the broader aims of the organisation rather than acting as a separate function that services the main organisation. This also requires security managers to demonstrate generic business skills, engage in their lexicon and be able to exert influence on other members of management and the board. This also means that security specialists should be represented on the board and in some organisations where security is a particularly important issue, a security director should actually be on the board.

(b) Using security risk management to secure competitive advantage: The effective use of the most up-to-date security risk management techniques can bring competitive advantage. For example utilising the latest strategies that might bring a 10 per cent reduction in losses which are costing £50 million per annum amounts to a £5 million saving (minus any additional costs of the new technique).

(c) Evidence-based actions: To achieve the above, it is necessary for SRMs to engage more in research and to learn from the experience of peers. They need to be aware of what works, to monitor research on the latest security (and other relevant) strategies, to conduct isomorphic learning and to share experience at appropriate professional events. They also need to be more willing to embrace research in order to assess the effectiveness of their strategies.

(d) Using metrics to monitor performance: To maximise evidence-based action, SRMs also need to maximise the use of metrics to enable performance of different strategies to be monitored and to enable ROI decisions to be made more effectively. Indeed, Gill *et al* [18] found only four in ten of the commercial organisations they surveyed collected data that could be used to measure the value of security.

(e) Agents for cultural change: Underpinning all of the above is the need for a root and branch cultural change to the way security is done. SRM is a key to this change, and needs to emulate a model of professional practice that breeds greater respect and influence. The SRM has the ability to change the way security is done in their organisations and across society as a whole. This paper will now focus upon just a selection of the key features of an SRM approach to reap competitive advantage.

4.2 Professional staff

The most important is professional staff. To achieve this, security managers and prospective managers need to undergo education and training that provides them with the skills to pursue a SRM agenda. This requires appropriate vocational, undergraduate, and postgraduate awards. It is not just the security managers who need to change. As with any major change in an organisation, it is also important SRM is embraced up to the very top of an organisation. The Board and senior managers also need to embrace a SRM mentality. More general managerial training, undergraduate and postgraduate courses, and most significantly MBAs need to develop appropriate options in their courses that demonstrate the benefits of investing in security and in-particular a SRM type approach. This is woefully lacking in most managerial courses.

The re-configuration cannot take place in a vacuum. The changes need to be built upon a sound professional infra-structure which equips security managers to carry out these functions and promote the importance of security and a SRM approach to Boards and senior managers. The professional association for security managers needs to aspire to Chartered status to demonstrate security management has become a profession. This will require a number of reforms. It will need to create a membership structure based on training, higher education and professional competence. Learning routes will need to be created such that people looking to enter the ‘profession’ undergo an appropriate training course or higher education award to achieve an entry membership. Given the large numbers already working in security, opportunities should also be created for those who can demonstrate professional competence through an accreditation process.

4.3 Accurate measurement

www.kci.go.kr

Central to this approach is accurate measurement of the costs of the security and investigations, but also of the problems of crime. One of the most significant hidden costs is fraud, and reliance on detected cases is flawed. The most accurate measures of fraud are fraud risk measurement exercises. The principles of these measures are focusing upon a particular type of transaction, such as procurement fraud. Then, identifying a statistically valid sample of transactions and investigating them to a higher standard than normal auditing processes to identify whether they are fraudulent or not was needed. From this, it is possible to identify the numbers of frauds (Fraud Frequency Rate - FFR) and losses (Percentage Loss Rate - PLR) to a particular level of statistical confidence [14]. Such approaches can also be used for other security risks.

4.4 Prevention

Prevention is also important and in *Doing Security*, the first author has set out a three-dimensional approach to preventing harm to an organisation [8]. Security systems are ultimately about getting people to behave or not behave in a particular way. It is about achieving outcomes, and therefore it is about power. The security decision-maker, A, wants B to do something or not to do something. To achieve an outcome, a security manager has a wide array tools at his/her disposal, and a useful way to conceptualise this is to use three dimensional conception of power of Lukes [29].

At the base level, power seems a relatively simple concept: the ability of A to get B to do something they otherwise would not do. This is only part of the picture, however, and this first dimension, as Lukes [29] would call it, forms the foundations of less visible forms of power. For Lukes, there are another two dimensions to power, the second of which, involves a critique of the first and is where A prevents an issue of conflict from emerging so that B still pursues a course of action that if that issue had arisen, B might have pursued differently. As Lukes writes [29]:

> ...the two dimensional view of power involves a qualified critique of the *behavioural focus* of the first view and it allows for consideration of the ways in which *decisions* are prevented from being taken on potential issues over which there is an observable *conflict* of *interests*, seen as embodied in express policy preferences and sub-political grievances.

The third dimension provides a further critique of the earlier two views, and is a consideration of ways in which potential issues are kept out of decision-making so as to influence the decision-making of an actor, without them even realising it. In this case, it would be a scenario where A pursues a course of action because B has created an environment, which means A will follow that course of action, without realising B wanted that to occur. In short, it is the creation of social conditions that encourage a type of behaviour that the subjects are not observably aware of.

To put these in a security context, if a security officer asks a 'youth' to leave a shop when they do not wish to and they do, that could be considered as an example of the first dimension of power. An example of the second, might be where a security officer's mere presence leads a 'youth' not to enter the shop when they want to. The third dimension could be illustrated by a 'youth' not even wanting to enter the shop because sub-consciously they have been influenced not to do so, hence the behaviour of the 'youth' had been influenced without there been any observable conflict. How the different dimensions apply to different security measures is further illustrated by figure 3 below.

A security system should be based upon the primary measures of making 'it' - with the 'it' being most crimes, incidents etc - never happen. As such the third dimension power of Lukes and the numerous initiatives that fall within their ambit should provide the primary basis for security systems. Nevertheless, it is important to note that the first and second contribute to the third and ultimately one has to build a system based upon all three. Ultimately, the design of the security system is very important influencing the ultimate risk of targeting [41]. The burgeoning research and literature under the broad terms of crime prevention, crime reduction, crime science, security etc provides much to learn for designing security systems.

THIRD DIMENSION Primary measures	**Creating mentalities to achieve outcomes subconsciously** *Changing malefactors' behaviour* Social measures Deterrence *Refocusing the behaviour of malefactors* Situational measures Design Image and reputation
SECOND DIMENSION Secondary measures	**Presence** Officer presence Product presence
FIRST DIMENSION Tertiary measures	**Effective human element** Verbal questions <> Verbal requests (making use of universal and select legal tools) <> Verbal threats <> Coercion <> Call the manager and/or police

Fig. 3. Three dimensions to creating security

4.5 Cultural change

Creating a culture such that crime is much less likely to affect it is also important. Much has been achieved in some organisations focusing upon developing anti-fraud cultures. Fraud awareness training based upon regular training for *all* staff, newsletters, E-mails, fraud awareness periods should all be used to mobilise the honest majority. Such training should cover:

- Types of frauds and scams
- Expectations of behaviour;
- Examples of fraudulent behaviour;

www.kci.go.kr

- The damage fraud does to an organisation;
- What happens to those detected defrauding;
- How to report fraud.

Frequently, frauds occur because procedures are not followed properly. Staff are not properly supervised, authorisations which are suppose to happen are overridden, and separate duties become merged, to name a few. It is important that the training also highlights to staff the importance of following procedures correctly and not deviating from them.

Publicity is very important. Some organisations bring to light cases of fraudsters who have been caught, and highlight the sanctions that have been applied. Some list their activities to show how active they are. They also highlight the damage fraud has done to the organisations. It should also highlight how to report fraud, if it is suspected. Publicity should also highlight the latest scams, which staff need to be aware of. These are all important elements of raising the profile of the issue to make fraud less likely to occur. Creating deterrence by highlighting the penalties applied to those who breach rules and the law is also important, and organisations should embrace a full range of sanctions, not just the criminal law.

4.6 Metrics

Metrics are also important in an overall strategy, as they enable an organisation to show the benefit the security and investigations function is having on the organisation. At their simplest, they are 'quantitative measures' compared overtime for example the financial loss to shop-theft in a retail unit over a monthly basis. It is the periodic assessment of same metrics over time which distinguishes them from ordinary measures i.e. a one-off assessment of the loss to shop-theft in a shop. The other important aspect of them is that they are used to inform organisational decision-making. Metrics are very common in modern business organisations and the few listed below give a flavour of the types of metrics used.

- Freight cost per mile (Total expenditure on freight divided by mileage)
- Cost per square foot (Total warehouse operating costs divided by size)
- Website conversion rate (Percentage of unique visitors to website who buy something)
- Average revenue per user (ARPU)

Central to security and investigations making effective use of metrics is the need to make them cost orientated. A sample is given below:

- Value in £ of losses per day
- Cost in £ of arresting and prosecuting shoplifter
- Value in £ of goods seized by security staff from detained shoplifters
- Value in £ of discrepancies in deliveries
- Cost in £ of incident of violence against staff
- Value in £ of fraudulent transactions

Also very important is the need to show a Return on Investment (ROI) of what has been invested in security and investigations.

$$ROI = \frac{(\text{Gain from Investment} - \text{Cost of Investment})}{\text{Cost of Investment}}$$

Specifically applied to security this would be:

$$ROI = \frac{(\text{Reduction in Security Losses \$} - \text{Expenditure on Security Resources})}{\text{Expenditure on Security Resources}}$$

For example, if a $100 million per year organisation with an above average fraud loss rate of 8 percent ($8 million per year fraud losses) invested $500,000 in counter fraud resources over a two year period and the rate had reduced to $6 million by the end of year 1 and $5 million by the end of year 2, then the reduction in fraud losses would be $5 million minus the $500,000 invested which would be $4.5 million divided by $500,000 which would = 9. So the return on investment over a two year period would be 9 (where organisations pursue redress these gains can also be added to the gain from investment).

5. CONCLUSION

This paper has shown how crime costs organisations a significant amount, and that in many bodies the security and investigation that is utilised to combat these risks is sub-prime: most notably security officers and security managers. This paper has argued for a reconfiguration of security management, which it is argued could lead to a competitive advantage for many organisations. The change advocated has parallels to the transformation of personnel to HRM. It is rooted in five major principles of moving the management of security towards Security Risk Management (SRM) based upon integrating security into the main aims of an organisation, utilising the latest techniques and strategies to reduce risks, pursuing evidence based actions, utilising metrics to monitor performance, and security managers becoming agents of cultural change. The paper ended with some examples of strategies, which can be deployed to help reap the competitive advantage: Refiguring as SRM, professional staff, accurate management, prevention, developing an anti-fraud culture, and metrics.

REFERENCES

[1] M. Armstrong, *Handbook of Human Resource*

www.kci.go.kr

Management Practice, Kogan Page, London, 2006.
[2] ACFE, *2006 ACFE Report to the Nation*, Retrieved 5th May 2011 from http://www.acfe.com/rttn/2010-highlights.asp, 2010.
[3] BDO Stoy Hayward, *As the Credit Crunch Bites so do the Fraudsters*, Retrieved 8th August 2008 from http://www.bdo.co.uk/BDOSH/Website/bdouk/websiteContent.nsf/vAll/C257D5D7693D5D9A80257478004944C3?OpenDocument, 2008.
[4] S. Box, *Recession, Crime and Punishment*, MacMillan, London, 1987.
[5] R. Briggs and C. Edwards, *The Business of Resilience*, Demos, London, 2006.
[6] British Retail Consortium, *BRC Retail Crime Survey: Cost of Crime Up, Violence against Staff Up*, Retrieved 20th August 2007 from http://www.brc.org.uk/details04.asp?id=766&kcat=&kdata=1, 2005.
[7] British Retail Consortium, *Retail Crime Survey Key Facts 2005-2006*. Retrieved 20th August 2007 from http://www.brc.org.uk/showdoc04.asp, 2007.
[8] M. Button, *Doing Security: Critical Reflections and an Agenda for Change*, Palgrave, Basingstoke, 2008.
[9] M. Button, *Security Officers and Policing: Powers, Culture and Control in the Governance of Private Space*, Ashgate, Aldershot, 2007.
[10] M. Button and H. Park, "Security Officers and the Policing Of Private Space in South Korea: Profile, Powers and Occupational Hazards", Policing and Society, vol. 19, no. 3, 2009, pp. 247-262.
[11] M. Button, H. Park, and J. Lee, "The Private Security Industry in South Korea: A familiar tale of growth, gaps and the need for better regulation", Security Journal, vol. 19, 2006, pp 167-179.
[12] D. Challinger, *Corporate Security: A Cost or Contributor to the Bottom Line*, In M. Gill (Ed), Handbook of Security, Palgrave, Basingstoke, 2006.
[13] M. L. Garcia, *Risk Management*. In M. Gill (Ed), Handbook of Security, Palgrave, Basingstoke, 2006.
[14] J. Gee, M. Button, and P. Bassett, *Fraud Loss Measurement – A Short Guide to the Methodology and Approach*, PKF, London, 2011.
[15] J. Gee, M. Button, and G. Brooks, *The Financial Cost of Fraud*, MacIntyre Hudson/CCFS, London, 2009.
[16] B. George and M. Button, *Private Security*, Perpetuity Press, Leicester, 2000.
[17] M. Gill, T. Burns-Howell, G. Keats, and E. Taylor, *Demonstrating the Value of Security*, Perpetuity Research and Consultancy International, Leicester, 2007.
[18] M. Gill, E. Taylor, T. Bourne, and G. Keats, *Organisational Perspectives on the Value of Security*, Perpetuity Research and Consultancy International, Leicester, 2008.
[19] J. Hainmüller and J. M. Lemnitzer, "Why do Europeans Fly Safer? The Politics of Airport Security in Europe and the US", Terrorism and Political Violence, vol. 15, no. 4, 2003, pp. 1-36.
[20] K. Hearnden, "Multi-tasking in British Business: A Comparative Study of Security and Safety Managers", Security Journal, vol. 6, 1995, pp. 123-132.
[21] K. Hearnden, *The Management of Security in the UK*, Centre for Extension Studies, University of Loughborough and SITO, Loughborough, 1993.
[22] Home Office, *The Economic and Social Costs of Crime, Home Office Research Study 217*. Retrieved 21st August 2007 from http://www.homeoffice.gov.uk/rds/pdfs/hors217.pdf, 2000.
[23] Infologue, *UK Security Guarding Industry Spotlight 2007*, Retrieved 4th July 2008 from http://www.infologue.com/user/strPage.asp?idLink=50, 2008.
[24] B. E. Kaufman, *The Development of HRM*. In P. Boxall, J. Purcell, and P. Wright (Eds.), Oxford Handbook of Human Resource Management, Oxford University Press, Oxford, 2007.
[25] KPMG, *Banks Suffer as Fraud Rides High*. Retrieved 8th August 2008 from http://www.kpmg.co.uk/news/detail.cfm?pr=3148, 2008.
[26] M. Levi, J. Burrows, H. Fleming, and M. Hopkins, *The Nature, Extent and Economic Impact of Fraud in the UK*, ACPO, London, 2007.
[27] E. Licu and B. S. Fisher, *The Extent, Nature and Responses to Workplace Violence Globally: Issues and Findings*, In M. Gill (Ed), Handbook of Security, Palgrave, Basingstoke, 2006.
[28] K. Livingstone and J. Hart, "The Wrong Arm of the Law? Public Images of Private Security", Policing and Society, vol. 13, no. 2, 2003, pp. 159-170.
[29] S. Luke, *Power: a Radical View, Macmillan*, London, 1974.
[30] M. Maguire, *Crime Data and Statistics*. In M. Maguire, R. Morgan, and R. Reiner (Eds) Oxford Handbook of Criminology, Oxford University Press, Oxford, 2007.
[31] A. McGee, *Corporate Security's Professional Project: An Examination of the Modern Condition of Corporate Security Management and the Potential for Further Professionalisation of the Occupation*, MSc Thesis, Cranfield University, 2006.
[32] R. McLeod, *Rarapolice – a Revolution in the Business of Law Enforcement*, Boheme Press, Toronto, 2002.
[33] D. Michael, *A Sense of Security? The Ideology and Accountability of Private Security Officers*. PhD Thesis, London School of Economics and Political Science, 2002.
[34] M. Nalla and M. Morash, "Assessing the Scope of Corporate Security: Common Practices and Relationships with other Business Functions", Security Journal, vol. 15, 2002, pp. 7-19.
[35] National Fraud Authority, *Annual Fraud Indicator*, National Fraud Authority, London, 2011.
[36] National Health Service Counter Fraud Service (NHSCFS), *Countering Fraud in the NHS: Protecting Resources for Patients. 1999-2006 Performance Statistics*, CFSMS, London, 2007.
[37] Privy Council Office, *Royal Charter*, Retrieved 8th

www.kci.go.kr

August 2008 from http://www.privy-council.org.uk/output/Page26.asp, n.d.
[38] R. Reiner, *Political Economy, Crime and Criminal Justice*, In M. Maguire, R. Morgan and R. Reiner (Eds.), Oxford Handbook of Criminology, Oxford University Press, Oxford, 2007.
[39] Securitas AB, *Interim Report January to June 2008*, Retrieved 20th August 2008 from http://www.securitas.com/Global/_DotCom/Interim%20Reports/2008_Q2/Securitas%20AB%20Interim%20Report%20January–June%202008.pdf, 2008.
[40] J. Shury, M. Speed, D. Vivian, A. Kuechell, and S. Nicholas, *Crime against retail and manufacturing premises: findings from the 2002 commercial victimisation survey*, Retrieved 23rd January 2008 from http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3705.pdf, 2003.
[41] N. Tilley, *Handbook of Crime Prevention and Community Safety*, Willan, Cullompton, 2005.
[42] A. Wakefield, *Selling Security – The Private Policing of Public Space*, Willan, Cullompton, 2003.

Mark Button
He is Reader in Criminology and Associate Head (Curriculum) at the University of Portsmouth specialising in security, counter fraud, and policing. In 2005, he obtained his PhD from London School of Economics and Political Science, UK. He is currently Director of the Centre for Counter Fraud Studies within the Institute of Criminal Justice Studies,

Julak Lee
He is an assistant professor of the department of protection and security management at Kyonggi University. He obtained Master's degree from the Michigan State University, US, majoring in Criminal Justice, and earned PhD in Criminal Justice from the University of Portsmouth, UK.

Hakkyong Kim
He is a professor of criminal investigation at Korean National Police University in the Republic of Korea. He earned his MSc degree in Risk, Crisis & Disaster Management from the University of Leicester, UK. In May 2011, he obtained his PhD in Criminal Justice (Risk & Crisis Management) at the University of Portsmouth, UK.

www.kci.go.kr