

**Southern Universities
Management Services**

Security Benchmarking

Report Number 1010/06

**Southern Universities
Management Services**

Security Benchmarking

Report Number 1010/06



**Southern Universities
Management Services**
Management Consultants

Claire Taylor
July 2006

CONTENTS

Page

1. EXECUTIVE SUMMARY	1
2. OBJECTIVE	3
3. CONTEXT.....	3
4. THE BENCHMARKING PROCESS	3
4.1 Background	3
4.2 Participant List	4
4.3 Process	4
5. HIGH LEVEL OVERVIEW OF FINDINGS.....	7
5.1 General Overview	7
5.2 Participant by Model	7
5.3 Average Expenditure by Model.....	8
5.3.1 Average Percentage of Expenditure on Outsourcing by Model.....	9
5.3.2 Average Percentage of Expenditure on Staff by Model.....	9
5.4 Security Expenditure as a Percentage of Total Institution Expenditure .	10
6. PERFORMANCE INDICATORS	11
6.1 Defining Performance Indicators.....	11
7. KEY LEARNINGS FROM THE STUDY.....	13
7.1 Strategy and Management Framework.....	13
7.2 Management Structure	15
7.3 Performance Management	17
7.4 Physical Security Measures	19
7.5 Models of Security	25
7.6 Risk Management.....	31
8. WAY FORWARD.....	34
9. PERFORMANCE INDICATORS	35
9.1 Strategic Quantitative PIs.....	35
9.2 Strategic Qualitative PIs	48
9.3 Operational Quantitative PIs	50
9.4 Operational Qualitative PIs.....	52
10. CONTACT LIST FOR PARTICIPANTS	53
11. ACKNOWLEDGEMENTS.....	54
12. CONTENTS LISTS FOR THE SUPPLEMENT TO REPORT 1010/06	54

SOUTHERN UNIVERSITIES MANAGEMENT SERVICES

REPORT NUMBER 1010/06

SECURITY BENCHMARKING

	Cross Reference
1. Executive Summary	
SUMS conducted a benchmarking exercise on behalf of our members into the provision of University Security. The aim of the study was to identify best practice across the breadth of provision of University Security Services and some useful measurements to help our members improve the service which they offer.	§ 2
Set against a context of internally and externally generated change, SUMS developed a questionnaire to understand what services are being offered, at what cost and within which model.	§ 3
26 SUMS members participated fully in the study.	§ 4.2
The questionnaire was comprised of four sections; the first collected contextual information about the institution, the extent of security provision and the roles and services involved; the second collected specific information about income and expenditure, equipment used and various awareness and prevention; the third collected information about staff and staffing and the fourth sensitive information.	§ 4.3
Key learnings emerged from the study in the following areas:	
<ul style="list-style-type: none">• Models of Security 18 institutions currently have a contract model of security, five are in-house, two have mixed models and at one institution security is provided by a wholly owned company. When considering what is the best model for a particular institution the following variables should be taken into account:	§ 7.5
<ul style="list-style-type: none">• Size of unit required• Level/extent of service the unit is required to run• Size of budget available• Employer/Employee relationship• Level of risk.	
The average expenditure for a contract security model is £407K and for in-house is £914K. This would seem to imply that where budgets are small, contract security is the most financially efficient model. Linking the level of budget to the level of services reveals costs of services which are not available through Security but are provided by other departments. So although the institution may appear to be saving money on their security budget by outsourcing, the other services are	

still required thus increasing institutional costs in total.

Security is beginning to focus less on physical security and more on support and duty of care roles such as improving the security awareness of students and staff. There is a general move towards the professionalism of security staff.

- Strategy and Management Framework and Structure § 7.3
An appropriate level of management and administration (strategy, framework and structure) is required to support whatever model for Security is chosen. Where the model is to contract out, to ensure an effective delivery contract management skills are required within the institution.
- Performance Management § 7.4
Performance management is underdeveloped and there is a lack of common data to assist appraisal. There is a clear difference between what we are able to measure and what it is important to measure. Although Performance Indicators (PIs) may be used and some institutions were explicit about the expected level of performance, others took measures but had identified no targets. There is no conclusive data to show a pattern of PI usage across the different models in use. PIs are examined in depth in section 6 of this report.
- Physical Security Measures. § 7.4
Institutions should define an access policy with access levels for buildings and customer types. Security departments should work with purchasing to identify recommended suppliers for security equipment and recommended maintenance agreements.
- Risk Management § 7.6
Security has a mixed involvement in risk management activities. The University of Bristol has completed a full risk assessment from a security standpoint and have used the results to drive resource savings and increase buy-in from stakeholders.
- Communications.
Good communication is required between Security and the rest of the institution on both a formal and informal basis. Good formal communication will provide the basis for a good relationship and should lead to the production of a set of management documentation with appropriate levels of input from stakeholders. Formal and informal communication can lead to higher awareness amongst students and staff.

2. Objective

SUMS conducted a benchmarking exercise on behalf of our members into the provision of University Security. The aim of the survey was to identify best practice across the breadth of provision of University Security Services and some useful measurements to help our members improve the service which they offer.

The report for this study has two main aims: to inform Members' Representatives of the high level learnings from the study and secondly to inform security managers of the measures that emerged from the benchmarking study. Therefore, the report is divided into two sections:

- **Report 1010/06;** this contains information about the benchmarking initiative, the process and key learnings, definitions of the performance indicators and within the appendices, aggregated analysis of the results of the study. This will be available to non members of SUMS.
- **Supplement to Report 1010/06;** this document contains performance indicator data at the institution level. As such data may be considered sensitive. SUMS members are asked to respect this constraint and not to distribute this document further. Supplement to Report 1010/06 will not be available to non SUMS members.

3. Context

The provision of security with higher education institutions is in a state of flux. Changes are being forced upon the sector from internal and external agencies. Internally, harmonisation and the single spine are initiating changes in the terms and conditions of staff. Externally changes in the requirements for licensing of security staff, contract and non contract (although this legislation is not yet in place), is leading many institutions to consider their Security model and the training they put in place to support delivery.

4. The Benchmarking Process

4.1 Background

SUMS, as a member based organisation, facilitates collaboration and the exchange of best practice. A number of collaborative studies are undertaken each year for members. This year, benchmarking of university services was chosen as the key collaborative initiative by the membership. They prioritised the services to be benchmarked and selected Security for the 2006 study.

In 2005-06 SUMS also completed security reviews at the Universities of Leicester and Hertfordshire. This benchmarking study informed those reviews.

SUMS attended a meeting of AUCSO (Association of University Chief Security Officers) early in 2006 to introduce the study and to gain an insight

into the important issues affecting university security. During this meeting and subsequent meetings with university security staff the need for security benchmarks was identified.

In 2002 HEFCE produced a report outlining the position of university security at that time and provided a set of recommendations for the provision of security within institutions. Four years on, SUMS was able to review the effect of the recommendations and update some of the HEFCE measures.

In 2006 Sodexho completed a survey entitled: "The 2006 Sodexho University Lifestyle Survey" that contained questions relating to the provision of security within universities. The results relating to these questions can be found in Supplement Section L.

4.2 Participant List

The following institutions took part in the SUMS Security Benchmarking Study.

Birkbeck, Brunel, City, IOE, KCL, LSE, Loughborough, Oxford Brookes, Roehampton, Royal Holloway, SOAS, Bath, Bristol, Cambridge, UEA, Essex, Exeter, Kent, Leicester, Plymouth, Reading, Southampton, Surrey, Sussex, Hertfordshire, Luton

The two returns for King's College (main sites and residences) have been amalgamated within the analysis to ensure that measures are as appropriate.

Of our SUMS members, Goldsmiths were undergoing a comprehensive review of security and therefore participation was not considered appropriate. The study was also considered inappropriate for AHRC.

4.3 Process

4.3.1 Questionnaire

A questionnaire was drafted to help us understand what is offered at each university, in what context and at what cost. The results of the survey will be used with other contextual information to analyse the provision of University Security Services.

A lead team made up of representatives from the Universities of Reading, Hertfordshire, Leicester and Loughborough was convened and met at Reading University on the 8th of February 2006. Input was also taken from Bernadette Duncan, Head of AUCSO for the South East. The lead group were responsible for testing the questionnaire and developing a set of performance indicators (more information is available on the key performance indicators in section 6 of this report).

The questionnaire was divided into four sections:

- 1) Context – made up of questions to give us a general overview of the security provision in each institution.
- 2) Specifics – more specific information on income/expenditure, systems and equipment used, incidents and incident reporting, awareness and prevention etc.

- 3) Staffing – information on the type and number of staff employed, training levels, benefits, shift systems and impacts of harmonisation.
- 4) Sensitive – information intended to gauge risk levels of the institution (this section was voluntary).

Members were divided into groups and the questionnaires were sent out in batches. Institutions had a specific amount of time to complete the questionnaire which was followed by a face to face meeting to discuss the questionnaire and gather information to fill in any gaps.

The form was sent out and completed electronically using Microsoft Excel™ which caused some issues early in the study but in the end made the collation of data much easier for analysis and presentation.

4.3.2 Meetings

The purpose of the face to face meetings at individual institutions was to gain a better understanding about their context for security provision. The scope of the meeting was the questionnaire but there was also an opportunity to gain more general information about the institution.

By meeting face to face, discussion about the purpose of the study led to greater buy in from the security contacts. In preparation for the meeting, each contact had completed the questionnaire (or had gathered as much information as they could) and sent it back. Analysis of the return before the meeting meant that each meeting was better directed and gaps were filled in the questionnaires.

In general the meetings were a key aspect of the study and although some took longer to complete than expected will remain part of the SUMS benchmarking process.

4.3.3 Collation

Electronic copies of the returns were collected and a data stripping mechanism was written in Microsoft Excel™. The data was then imported into a Microsoft Access™ database. Queries were written to collect and present the data in a form appropriate for analysis. Calculation of the key performance indicators was also done within the database. Data was exported back into Microsoft Excel™ to prepare charts for the presentation and this report.

4.3.4 Presentation

Results and key learnings from this study were presented at a meeting held at Birkbeck on the 13th of July 2006. Two thirds of the security contacts who had contributed data to this study attended along with some Member Representatives.

The presentation covered the following:

- 1) A review of the SUMS Security Benchmarking Study
A review of the methods used for the benchmarking initiative, the key findings and discussion.
- 2) Management of Security Provision
Whether in-house or contract, security is a service which is generally seen as a cost centre. As such, questions can be raised about value for money

and expected service levels. What indicators are appropriate to use? Some of the measures driven from the benchmarking study were covered with their uses in defining Service Levels. Richard Law talked about the Bath experience of drawing up Service Level Statements for security.

3) Closed or Open?

What is the general picture of an institution? What levels of access control are in place and what technology is used? What are the levels of incidents and how do institutions capture and measure them?

4) Models of Security

There are various security models in place amongst the SUMS membership. The various models were explored and the implications assessed on the services offered, terms and conditions of security staff and the budgets required to support them. Gary Jackson spoke about his experiences of bringing security in-house at Southampton.

5) Assessing the Need for Security

Bristol has recently undertaken an exercise to analyse the security requirements for the activities and buildings they support. Jerry Woods, Head of Security, covered the process and the changes made in light of their findings.

Copies of the presentations are available on the SUMS website:

www.sums.org.uk/

4.3.5 Data Set Availability

Electronic copies of specific subsets of the data will be available to those who took part on request. The entire dataset is too large to publish and the formulation of a database to allow access to the data is not within the scope of this study. Therefore if more detailed information is required about any particular aspect of this study (for example, Essex were interested in the specifics of the shift allowances for in-house security staff), requests can be made by phone or email.

5. High Level Overview of Findings

5.1 General Overview

The general picture of our members is one of a university open to vehicle and pedestrian access with buildings open during the daytime and either physically or electronically shut down at night. Some institutions have barriers or gatehouses at vehicle entrances. Some institutions have secondary security points at important areas (e.g. 24 hour libraries or Learning Resource Centres).

5.2 Participant by Model

Models of security are defined in the following way:

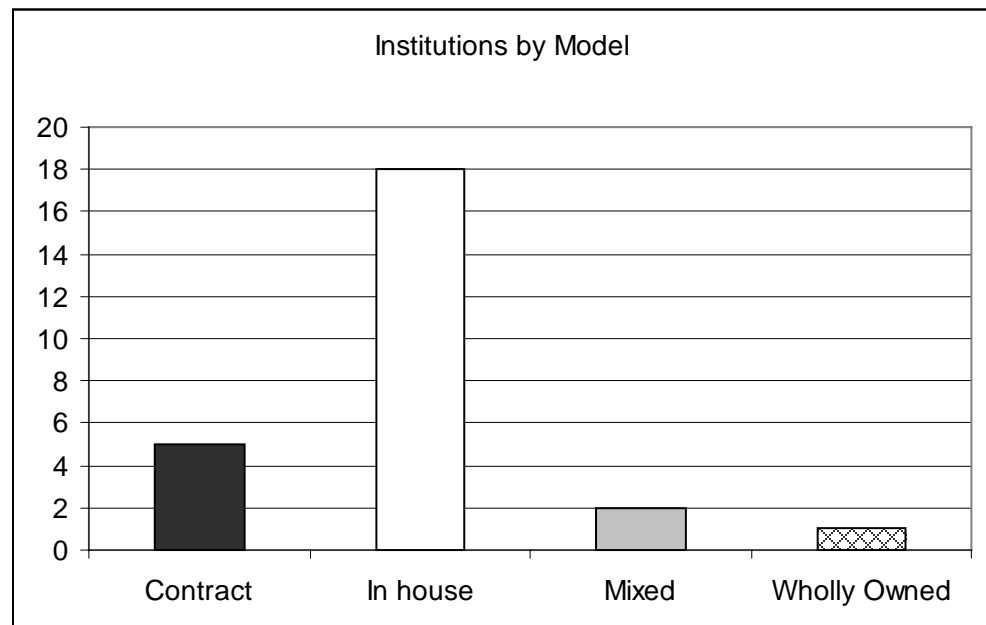
Contract – Majority of security staff are provided through a contract with an external company. Some in-house staff may be employed in management of the contract or in specific areas of the university.

In-house – Majority of security staff are employed by the university. Some contract staff may be employed in specific areas or used for supplementing if required.

Mixed – Where there is no clear majority or more than one model is used on different campuses.

Wholly owned – where the institution has set up a wholly owned company whose objective is supply security staff and services to the institution. The wholly owned company employs the staff although they may also require contract staff in specific locations or for supplementation.

The following chart shows what models were found amongst the respondents to the study.



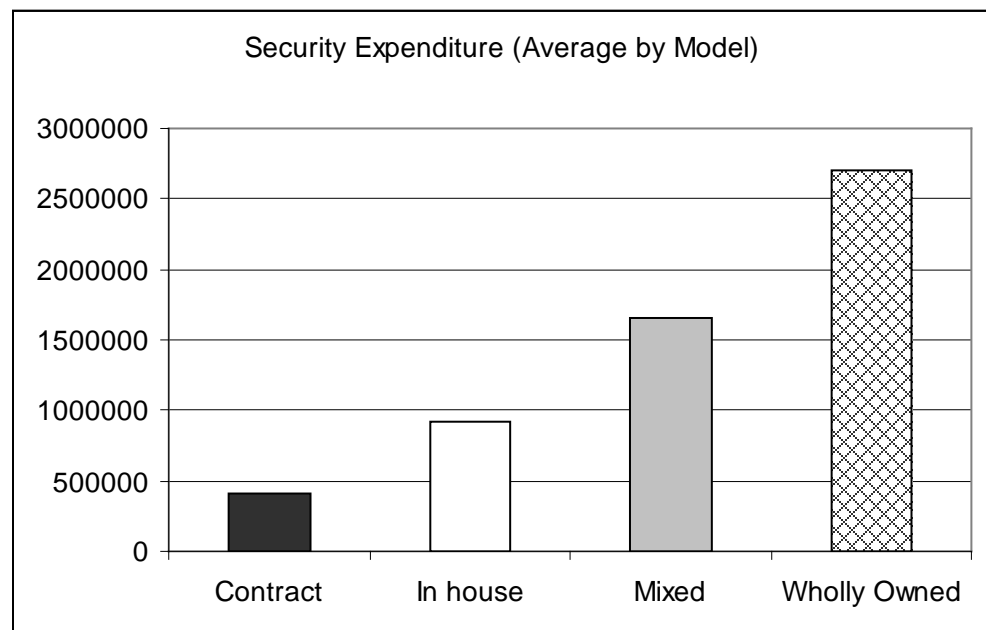
Across the SUMS membership there are five contract models, two mixed, 18 in-house and one wholly owned.

Other ways of categorising institutions are:

- 1) Whether they are broadly campus or non campus institutions.
Across the SUMS membership there are nine non campus institutions and 17 campus institutions.
- 2) Where they are based.
Across the SUMS membership there are six London based institutions, four city centre based institutions, seven suburban institutions and nine out of town institutions.

5.3 Average Expenditure by Model

This chart provides a comparison of the total expenditure of each institution on security averaged by the model. There is no scaling for size in this chart, that information is available later in the report (see section 9.1.2.4).

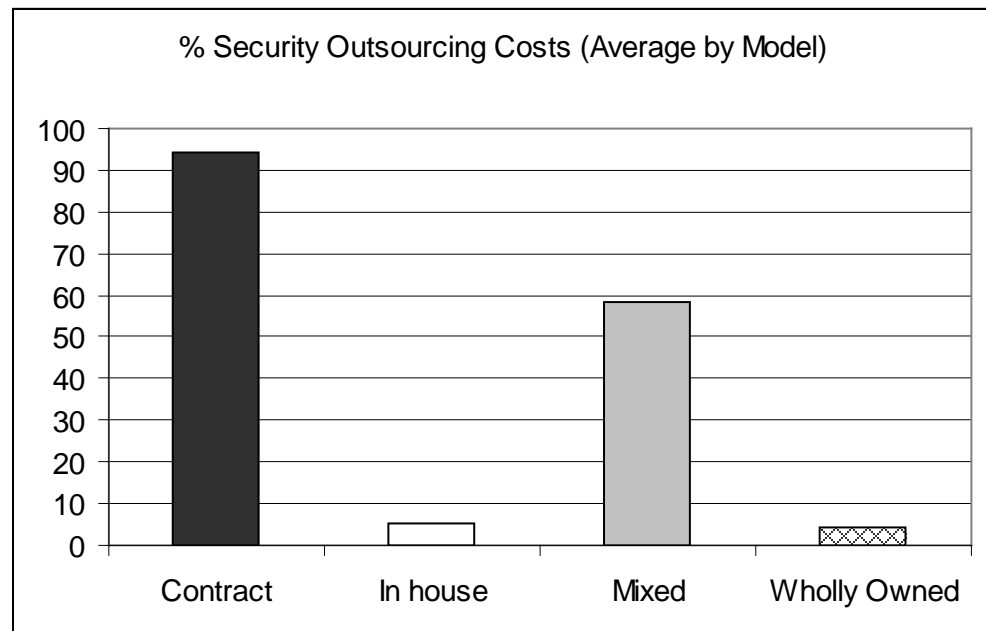


The average for contract security is £407K and the average for in-house is £914K.

Institutional level information is available in Supplement Section F.

5.3.1 Average Percentage of Expenditure on Outsourcing by Model

This chart provides a comparison of the percentage of security expenditure on outsourcing averaged by the model. There is no scaling for size in this chart.

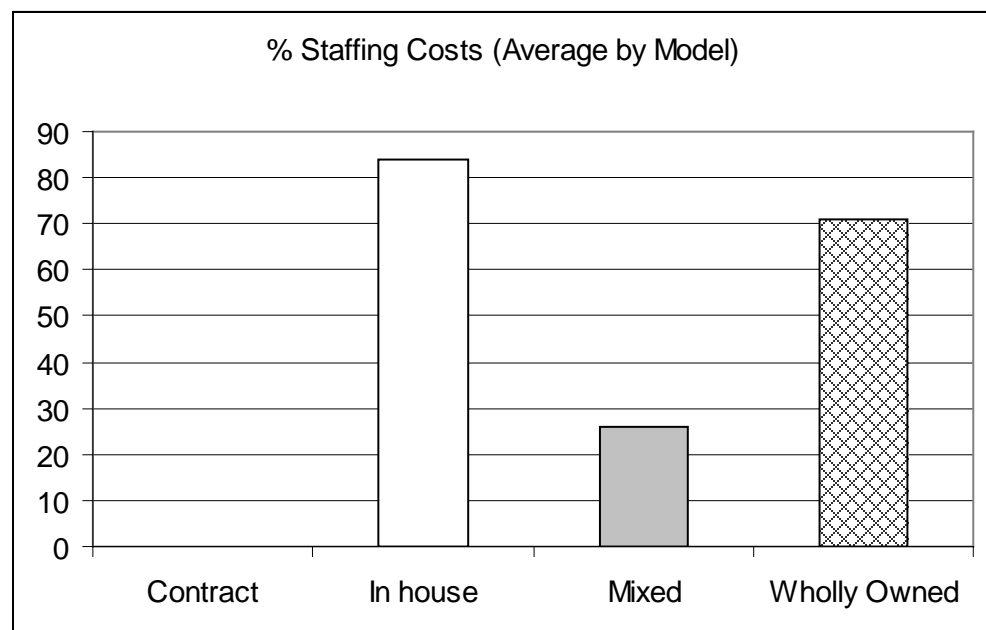


This is as we would expect. Most in-house models will use some contract staff for specific areas (e.g. libraries) or for supplementing.

Institutional level information is available in Supplement Section F.

5.3.2 Average Percentage of Expenditure on Staff by Model

This chart provides a comparison of the percentage of security expenditure on staffing averaged by the model. There is no scaling for size in this chart.



Staff costs from the study are a total of the following aspects:

Total Staffing, Conferences/Training, Staff overtime, Non contract staff expenditure, Recruitment, Uniforms, Training, Travel and subsistence.

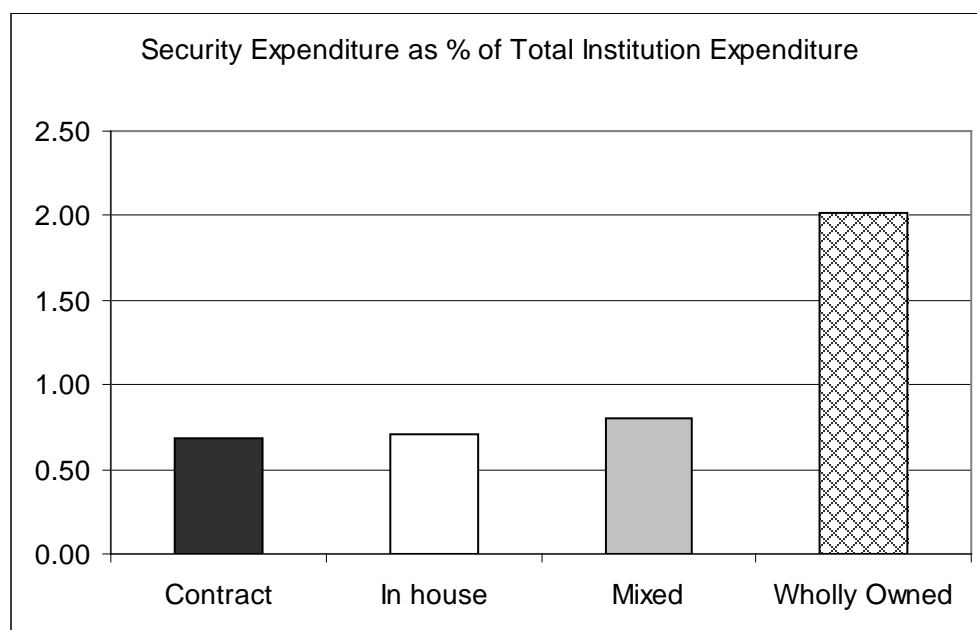
When considering spending levels on staff, the HEFCE report 02/30 stated that between 60 and 70 % of total security spending should be on the staff budget (quoting from Croner's Practical Premises Security).

Only three institutions meet Croner's recommendation with average spend for In-house models at 84%. The wholly owned model is just outside the recommended levels though this does not take into account whether actual spending levels are appropriate.

Institutional level information is available in Supplement Section F.

5.4 Security Expenditure as a Percentage of Total Institution Expenditure

This chart provides a comparison of the security expenditure as a percentage of the total institutional expenditure averaged by the model.



There is no significant difference between the values for contract and in-house across our respondents.

Institutional level information is available in Supplement Section F.

6. Performance Indicators

6.1 Defining Performance Indicators

6.1.1 What is a Performance Indicator (PI)?

A PI is a quantifiable measure which the achievement of moves an organisation along a path to realising its vision, strategic and/or operational plans.

Thus having defined their vision and completed a strategic and operational plan, a security department will be in position to define some PIs which will ensure that they meet the targets in their plans.

6.1.2 What Makes a Good PI?

A PI should be a **SMART** goal. There are many definitions of what SMART could stand for but here we've used Specific, Measurable, Agreed upon, Realistic and Time based.

- PIs should be specific, they should be well defined and be understandable to anyone who has a basic knowledge of the subject
- They should be measurable, it should be clear whether a goal has been achieved or how far away we are from achieving that goal
- They should be agreed upon amongst the stakeholders
- They should be realistic, achievable with the constraints of available resources, knowledge and time
- Lastly they should be time based, there needs to be a time frame within which to achieve the goal or to measure the PI.

PIs can be split into certain groups. They can either be strategic or operational and they can either be quantifiable or qualifiable. Strategic PIs will be used at a higher level and will be linked to the vision and strategic plan. These PIs will tend to exist on a longer time frame or be measured once a year. Operational PIs will be used at a lower level and be linked to the operational plan or assignment instructions. They will be measured on a more frequent basis and be used on either a weekly or monthly basis.

Quantifiable PIs are those which can be measured. Qualifiable PIs are more subjective, perhaps a simple yes/no answer is all that is available. Neither is more valuable than the other and it is not true that all things that can be measured make good PIs.

6.1.3 Using PIs Within the Security Context.

There is a certain amount of reticence within the University sector generally to use PIs and this is reflected within security departments.

Areas which will benefit from PIs are those which are controllable. For example an institution may believe that highly visible patrols are key to preventing petty crime on campus. Their strategic plan states that cutting petty crime is a key objective and that they will do this by implementing high visibility patrols. Their PI should not be on the outcome (decreasing petty crime) since this is not directly in their control, however the PI should be on the number of days in the year they have completed the planned number of high visibility patrols. Another university decide that actually the way to cut petty crime is to increase the awareness of crime prevention amongst staff

and students. One PI might then cover the number of staff and students who receive security inductions and another PI might cover the number of insecurities reported by officers on patrol.

When considering indicators it is important to understand where comparisons across institutions are valid and where the indicators are more appropriately used within an institution or compared to local levels. In some areas of the questionnaire, responses were too inconsistent to make comparison valid. Where possible, it may be of more value to compare underlying behaviours or processes which lead to better results to see if these are applicable across institutions. AUCSO has a key role here in spreading good practice throughout the sector.

One example of an area in which inconsistencies make comparison difficult is budgets. In some institutions budgets could not be accurately broken out of estates budgets so estimates were used. Where security budgets could be broken out, there were so many different inclusions that comparisons on budgets will have to be done at a high aggregated level.

Another area is incidents. Not all institutions could provide incident numbers for 2004/05. Where institutions could provide incident numbers, some could not break out the types of incident and for others the definitions of incidents were very varied.

6.1.4 Performance Indicators Developed by the Lead Team.

A set of performance indicators was developed by the lead team. These are outlined in the appendices to this report with definitions, advantages, disadvantages and uses. Where applicable data was collected within the study, aggregated charts are available in these appendices.

A single page with the indicators in a table is given in Supplement Section B.

Where there are charts in the following sections, which are averaged by model, institutional level information sorted by Location and Type are available in the appropriate section of the Supplement to Report 1010/06.

7. Key Learnings From the Study

7.1 Strategy and Management Framework

Management documentation is an output of a good management structure with good communications upwards, downwards and out into the rest of the organisation.

Documentation is required internally within the department to define direction. Departments need internal documentation for operational staff, to define working practices and priorities. Documentation is required for those outside the department to ensure that stakeholders know what is available to them and what is expected of them. Well written, easily available documentation (through a website or on the intranet) will increase the prominence of the Security Department and the buy in of stakeholders to their activities.

Management documentation includes a Vision, Strategic Plan, Service Level Statements/Agreements and Operational Plans/Assignment Instructions. Each Security Department should start with a vision and develop a strategy to deliver that vision. Input should be taken from the Institution Vision and Strategy to ensure that they are aligned and from interested parties (both internal and external to the department). Once the strategy is in place service level statements or agreements can be drawn up and operational plans can be written to meet the strategy and any agreements in place.

7.1.1 Vision Statements

A vision is an over-riding idea of what the organization should be. Often it reflects the dream of the founder or leader. A vision must be sufficiently clear and concise that everyone in the organisation understands it and can buy into it with passion.

Examples of Visions:

Brunel: To provide a safe and secure environment for students, staff and visitors and to provide high levels of customer service.

RHUL: To minimise the risk to all College property and to safeguard the safety of all members of and visitors to the College.

UEA: To assist UEA in its quest to be a centre for higher education excellence through the provision of high quality access and security services.

7.1.2 Strategic Plans

The strategy is one or more plans that will be used to achieve the vision. Key objectives need to be identified and certain aspects of the security provision covered. There is a lot of detail in the security tool-chest from HEFCE about this section. It is important that the security strategy ties in with other departments and is agreed with the various stakeholders.

7.1.3 Service Level Statements or Service Level Agreements

Aspects of and acceptable levels of service provided should be agreed with the stakeholders. It is important to achieve appropriate levels of security rather than just set levels. For example there was no real service level agreement in place between Hertfordshire and Unisecure, the wholly owned company. Hertfordshire pay the bill each year but have little input into what levels of security was supplied. The key driver for SUMS involvement in the

Hertfordshire Security Review was to determine whether the security provided was appropriate for the context.

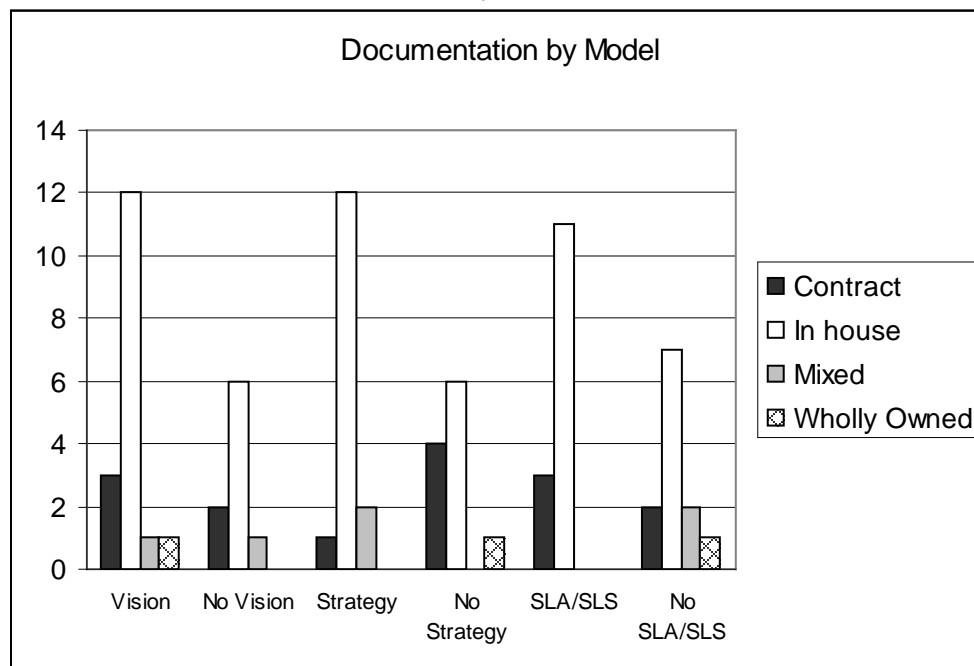
Examples of SLAs can be found on the following websites:

<http://www.bath.ac.uk/security/services/>

http://www.lse.ac.uk/collections/security/service_levels.htm

7.1.4 Position of Institutions with Respect to Above Documentation

The following chart shows the position of institutions with respect to management documentation and is shown by model.



From this chart it can be seen that there is mixed availability of documentation. There are approximately one third of in-house respondents who do not have a vision, another third who do not have a strategy and just over a third who do have Service Level Agreements/ Statements in place. With regard to contract models, one concern is that most institutions did not have a strategy in place. It is more important for contract models that a service level agreement is in place between the institution and the contract provider to ensure that appropriate service levels are met. This will also aid contract management over the course of the contract and the tendering process when the contract is up for renewal.

With the above documentation in place and an understanding of the commitment required, resource levels can be set and operational plans (assignment instructions) can be written to achieve the required service levels.

Institutional level information is available in Supplement Section C.

7.1.5 Management Accounts

A clear picture of the cost of provision of university security will be aided by a well defined set of cost centres and appropriate management accounting practices.

7.2 Management Structure

It is important within any department that there is a clear and simple management structure in place with appropriate line and executive management upwards through the organisation. Within Security there is an essential difference between operational management and non operational management.

Appropriate line and executive management will ensure that Security has good visibility amongst the decision making bodies of the Institution. This will lead to Security having appropriate influence in decision making and the securing of budget and capital funding for projects.

Of the respondents to this study, Executive Responsibility for Security fell to the following positions:

Position	Number of Institutions
Secretary & Registrar, Secretary, Registrar	12
Pro Vice Chancellor, Vice Chancellor	7
Principle	2
Director of Resources	2
Director of Facilities Management	1
Director of Finance	1

* One of the respondents did not give data for this question.

Of the respondents to this study, Line Management for Security fell through the following departments:

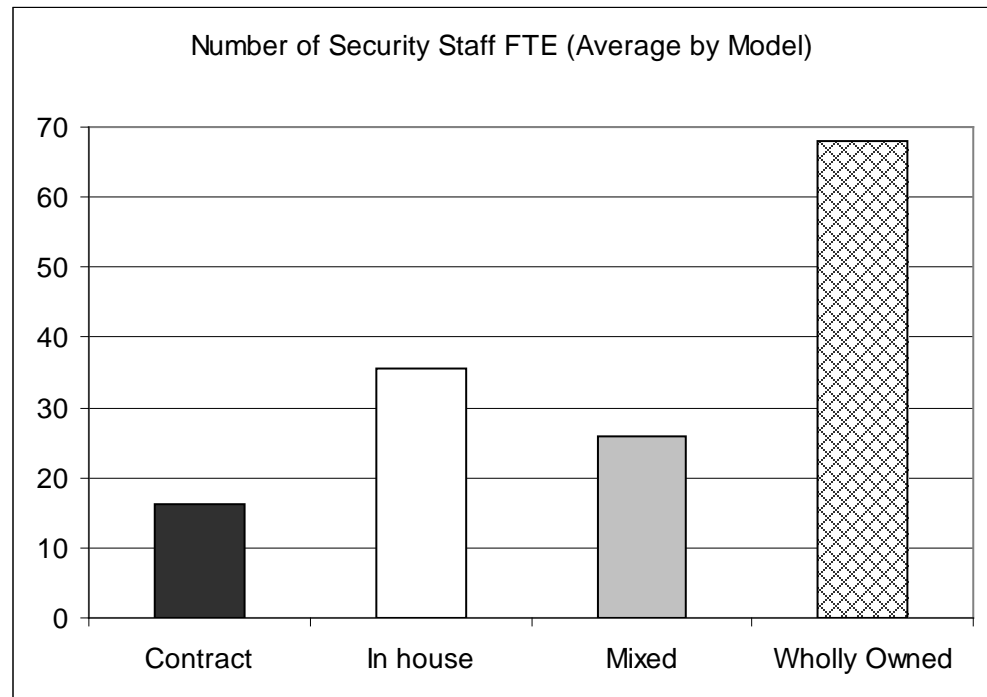
Department	Number of Institutions
Estates, Estates & Facilities, Property	21
Hospitality	2
Human Resources	1
Learning Facilities	1
The Secretariat	1

Appropriate levels of operational management with efficient reporting lines downwards through Department will ensure that Security is run effectively. Management of Security is unlike management in other university departments with the issues of managing shift workers and night staff.

In larger departments, these roles can be split with Deputy Heads of Security with specific responsibilities for Operations. In smaller departments it is vital that the Head of Security has a good balance between their strategic and operational focuses.

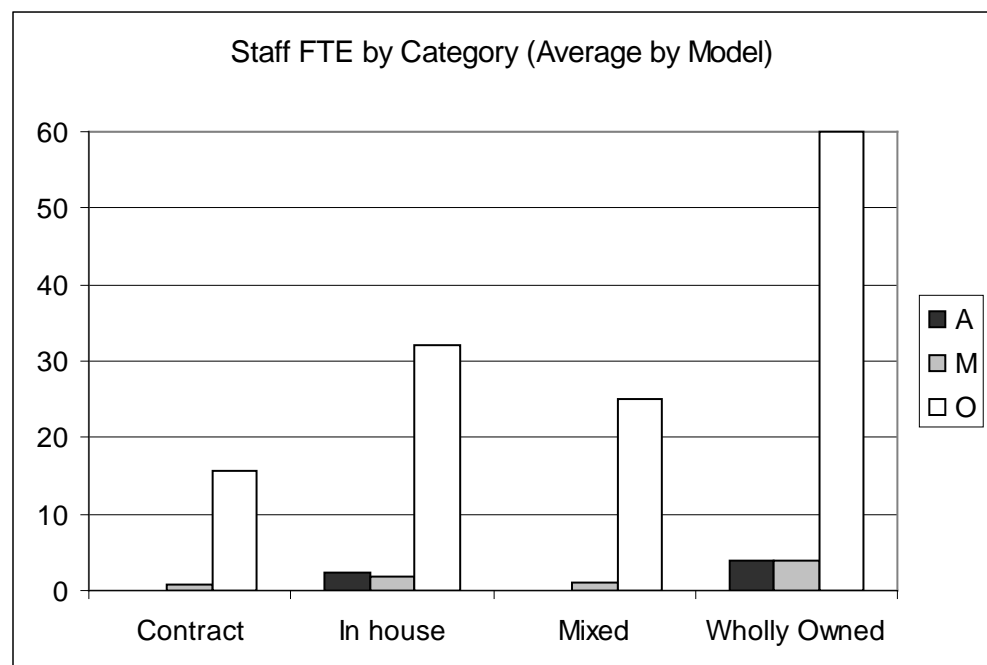
Within the security departments surveyed here there have been a variety of administrative commitments (parking permits, management of ID cards, management of lost property etc.). It is essential that there is a suitable level of administrative support to meet these commitments. This will ensure that operational staff concentrate on operational activities and management staff on management tasks. It is expected that management will sometimes get drawn into operational matters when supplementary staff are needed but this should be an irregular occurrence.

The following chart shows the number of staff FTE working within the Security Department by model.



Institutional level information is available in Supplement Section H.

The following chart differentiates between types of staff within the security department.



* Where A indicates Administrative staff, M Non-operational Management staff and O Operational staff.

Institutional level data on this subject can be found in Supplement Section H.

It is important to note that although contract models will have defined operational management structures within the contract staff, strategic management of security and contract management of the security contract will be required internally.

For those respondents with contract security models (including KCL since it holds contracts with four different suppliers across its various sites) it appears that management of security falls under one person (generally Facilities Manager) with various other responsibilities. One contract model offers a head of security within that model. Within the University of London contract with Reliance (which applies across three of our respondents) there is no one head of security responsible for managing the contract across the various institutions comprising of over 60 contract staff.

The importance of internal security management also holds true for the wholly owned model. The institution must have an internal strategy for security which is fulfilled by the company rather than strategy being set externally to the institution.

7.3 Performance Management

The Vision, Strategy and Service Level Agreement/Statement documents will indicate what is important to achieve and the priorities of the Security Department. From these Performance Indicators (PIs) can be identified. There is a clear difference between what we are able to measure and what it is important to measure.

For more information about Performance Indicators please go to section 6 of this report.

Internally 12 from 24 respondents use PIs within their performance management activities, five use some and seven do not use any PIs. Although Performance Indicators may be used, some institutions were explicit about the expected level of Performance whilst others took measures but had identified no targets. There is no conclusive data to show a pattern of PI usage across the different models that our respondents use.

Examples of Performance Indicators:

UEA.

1. To reduce the overall number of crimes and incidents by 5%.
2. To reduce the incidents of vandalism by 5%.
3. Regularly liaise with Maintenance and PODS and contribute to new build planning and construction meetings to achieve the requisite reductions in crime and vandalism.
4. To meet the targets set as part of the Divisional Health and Safety Plan and annually review all health and safety risk assessments.
5. To maintain short-term sickness absence at less than 2.5% and refer all long-term sickness absence to the UEA Occupational Health Unit.
6. To introduce a customer survey to measure achievements in meeting service standards by September 2004.

UEA are currently completing a Crime Reduction Strategy that will set additional, more challenging performance indicators.

Brookes:

As part of the contract the following are measured at each of the sites: 1) Contracted Hours 2) Punctuality 3) Patrol records 4) Training. There was no information given on the targets for these measures or how often these targets were achieved.

Plymouth:

Measures include: Reported incidents, Complaints, Compliments, No. of security staff, FTE dedicated security staff, Security expenditure, Security expenditure as % of turnover, Average no of days sickness per security staff, Average no. of training hours per security staff.

It is important that Performance Indicators are integrated into the appropriate documents and decision making processes. Should stakeholders require a higher level of service or a new area to be secured, using a resource model (along side agreed service levels) will imply new resource commitments.

One other area which impacts on Performance Indicators is around the prioritisation of services. Emergency responses may infringe on Security's ability to meet everyday service levels. There must be an agreed prioritisation of tasks so that operational staff know what is important and stakeholders understand responses when multiple calls are made on Security resources.

7.3.1 Learnings from Bath

The following bullet points were taken from the presentation by Richard Law, Security Manager at Bath University given at the meeting on July 13th.

Service Level Agreement

- Original recommendation in 2002 review
- When interviewed members of University staff and Security staff were seeking clarification as to the role of Security
- A review of management processes identified a lack of documented roles and responsibilities
- 2006 SLA constructed by the Head of Security Services and adopted following consultation
- Available on Internal University Security website.

Advantages

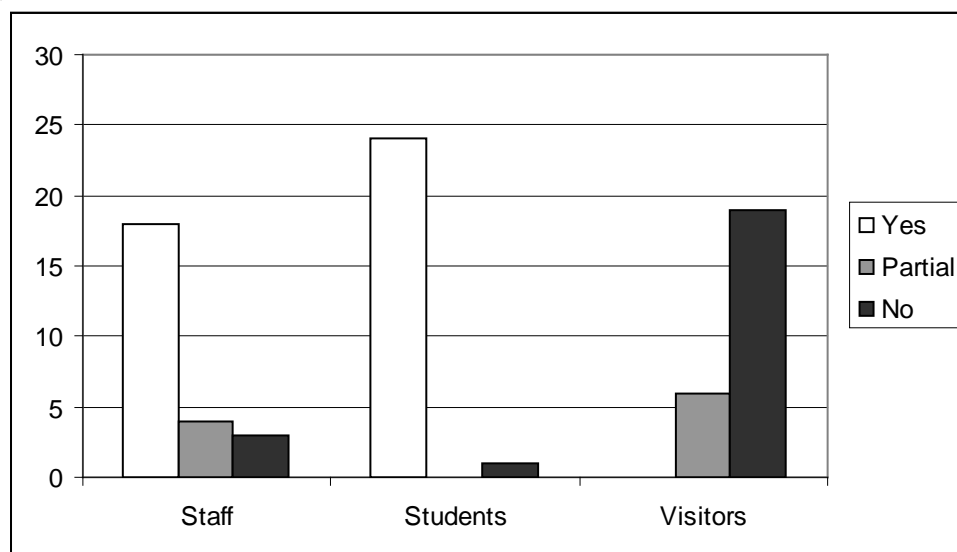
- Clearly identifies the services offered
- Sets out the expectations of customers by security
 - Cash bags sealed
 - 14 days notice to staff events
 - Completed application – car park permits
 - Etc.
- Clarifies areas that are not the responsibility of Security
- Allows for objective setting during staff appraisals
- Identifies areas for key performance indicators.

7.4 Physical Security Measures

7.4.1 ID Cards

Nearly all respondents offer ID cards to Students with only one unable to do so. However it is not mandatory to wear an ID card and in some institutions it is not mandatory to carry the ID card. Most respondents offered ID cards to staff though some had either a partial response (offering ID cards to staff in particular departments only e.g. hospitality, security) and some offered no ID cards for staff (this may be due to issues with the IT support required to create and maintain staff databases).

The following chart shows how many institutions are able to supply ID cards to Staff, Students and Visitors.



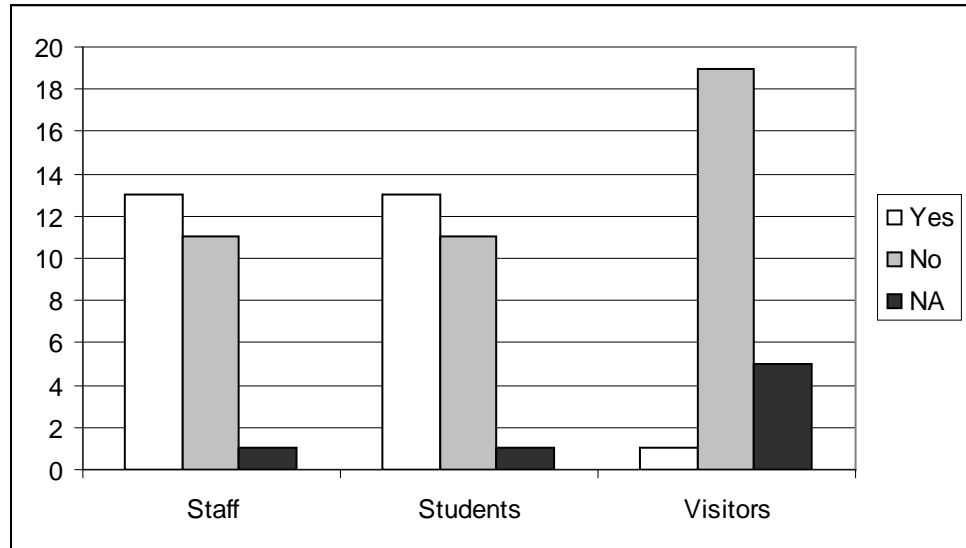
Management of ID cards is mixed with some security departments picking up responsibility for the creation of cards.

7.4.2 Access Control

14 members have a full (though not necessarily single) access control system, eight have part of their estate closed by access control at certain times of the day and three have no access control at all. Birkbeck did not supply information here.

Of those with mixed access control, issues with departments choosing own access control solutions and mergers were the main reasons given.

The following chart shows the number of institutions which offer single access cards for all systems.

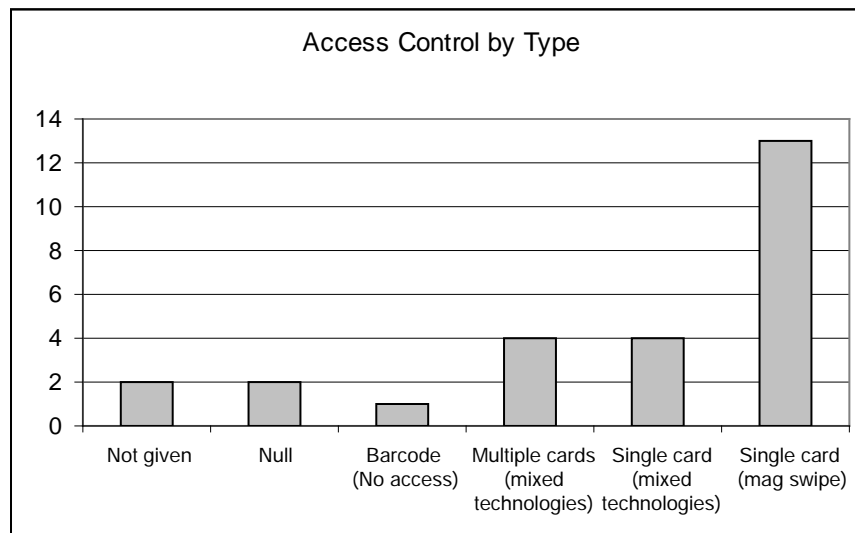


There is only one institution which is able to offer visitors cards which include access. Other institutions were able to offer small numbers of temporary cards to contractors.

Management of Access Control is mixed with some institutions managing access control outside of security. Some departments enable cards created elsewhere for the various buildings the user requires.

7.4.3 Access Control Systems

The following chart shows how many institutions use different access control systems.

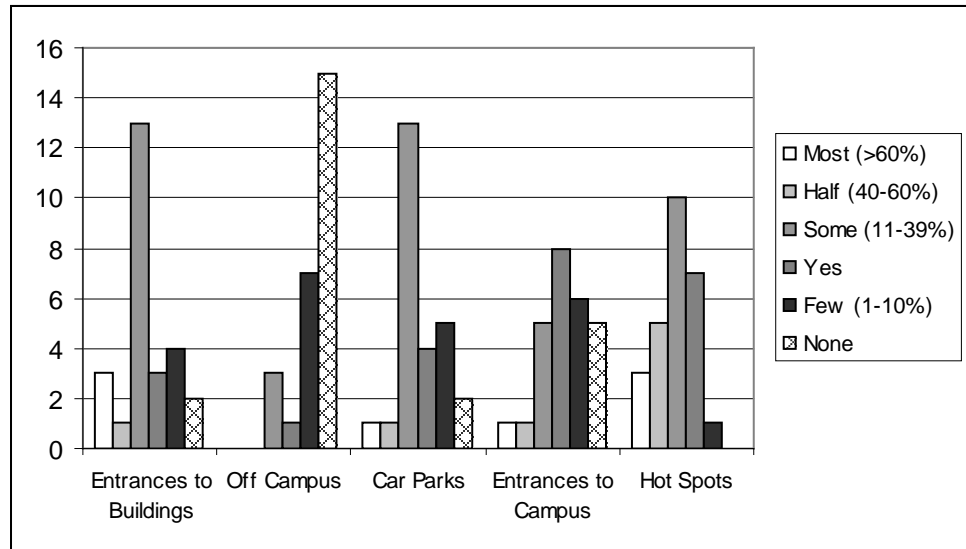


The majority of respondents who gave information for this section are using a single card with a magnetic swipe technology. Four institutions are using a single card with multiple technologies included on that one card and another four are using multiple cards with single technologies. One institution has a card with bar code technology which is not used for access control. Birkbeck and Surrey did not supply data for this question.

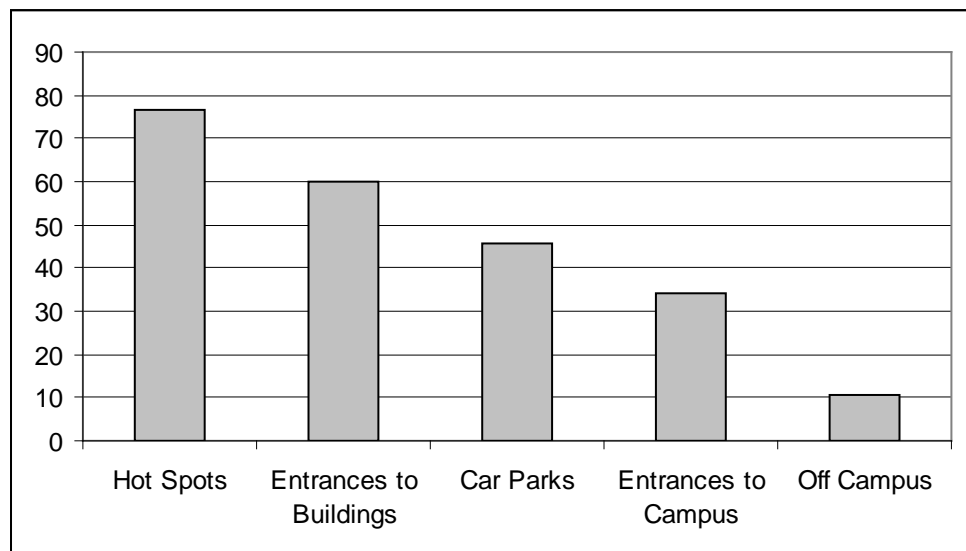
7.4.4 CCTV Usage

Data from the study concerning the usage of CCTV cameras was of mixed quality. Some respondents were able to give percentages of cameras, others gave text responses. All responses were converted to text according to the key. For example, the response “most” means that between 60% and 100% of the institutions cameras are in that position.

The following chart gives the location of cameras within the institution.



This chart shows the likelihood of an institution placing CCTV cameras at the given locations.



Using a weighting it can be seen that our members are most likely to put CCTV cameras in the following places: Hotspots; Building Entrances; Car parking areas; Campus Entrances; Off campus.

One key measure missing from this information is the percentage of internal cameras.

There are mixed opinions on whether CCTV is a deterrent to crime or whether its main use is as a monitoring and recording device to be used to determine what happened. Of the respondents to this study:

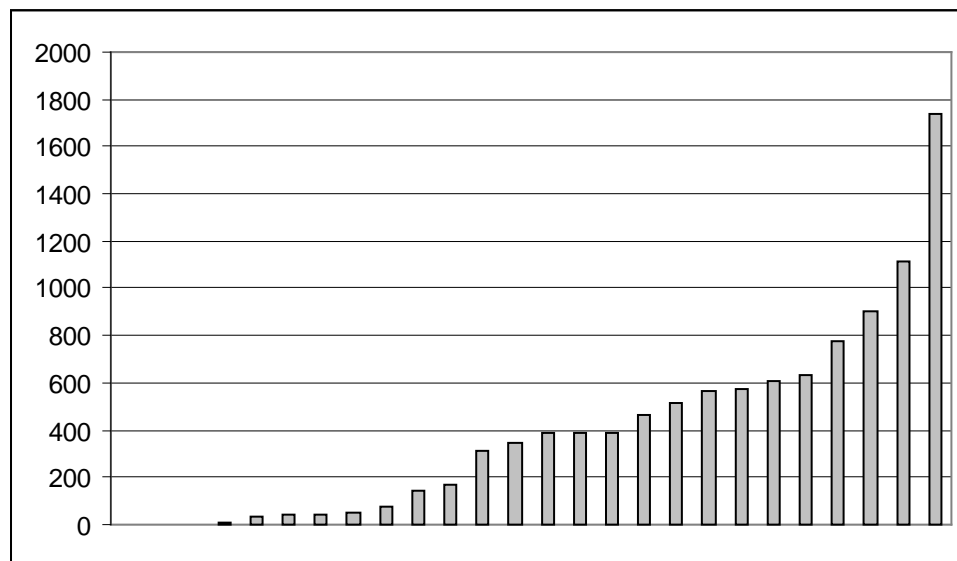
- 19 institutions monitor their cameras centrally, seven monitor some or most of their cameras centrally and one does not monitor centrally
- 19 institutions have most or all digital cameras, two have none
- Five institutions use dummy cameras, 22 do not
- All institutions record cameras
- There was a mixed response to whether the Security Department are responsible for monitoring all CCTV cameras on site. There seems to be a move to create centralised control rooms which pick up departmental cameras at night.

Recommendations for physical security measures:

- Consider the different requirements of buildings and user groups. From the understanding of the strategy of security (a bricks and mortar or customer focus) it should be possible to define an access policy and define a CCTV policy. It is important to keep access models simple; irrespective of the technology used people will need to interact with the access control system too
- Consider which areas require which different levels of physical security and within the policy document define levels of security provision as appropriate. For example Luton has a completely open environment with no internal access control except at the library where they have barriers
- It is important that departments/faculties work together with security to implement physical security provision on new builds and refurbishments. Of the respondents, ten institutions are involved in defining security requirements during the design phase, ten have some involvement in design and five have no involvement in estates planning/design at all
- Access control should be available from a small number of suppliers whose systems work with other systems already installed. Maintenance contracts should be considered when purchasing systems. The recommendation here is that the security department works with the purchasing department to define preferred suppliers and preferred maintenance contracts.

7.4.5 Incident Analysis

The chart below shows the number of incidents recorded for 2004/05 for the respondents.



Institutional level data can be found in Supplement Section G.

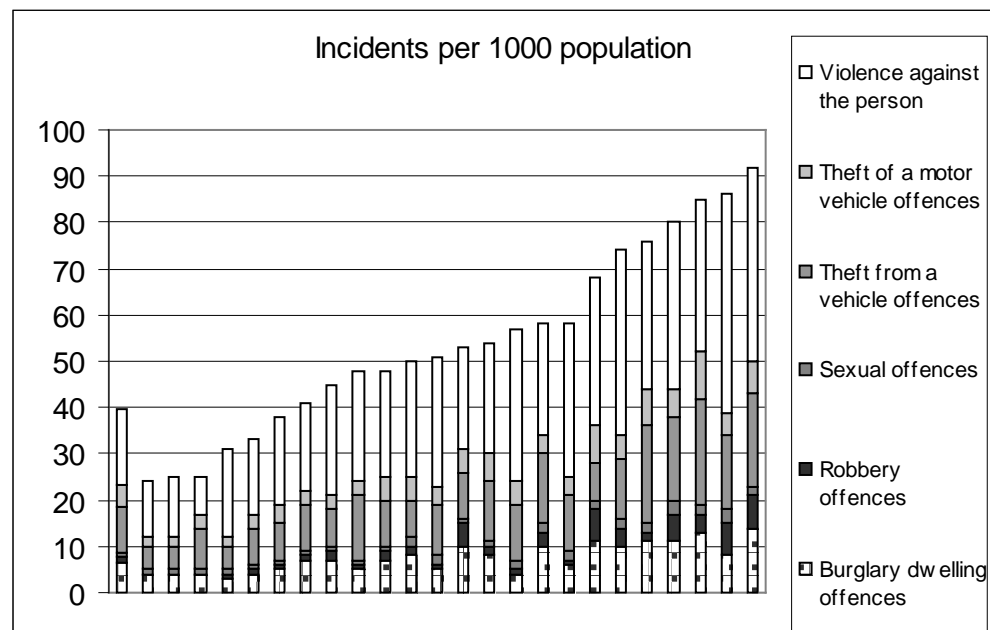
The variation in the number of incidents recorded is very high. Three institutions were unable to supply incident numbers either because they do not have a recording mechanism or they did not feel that the levels of recorded incidents were a true reflection of the actual level of incidents.

At the other end of the scale are respondents who capture a large range of incidents (including alarm responses) and have electronic incident capture mechanisms (either databases written in-house or supplied commercially). It is not necessarily the case that having electronic incident capture increases the number of reported incidents. One of the respondents with a database supplied one of the lowest incident numbers for the year.

Incident comparison between respondents is not appropriate. It is clear that numbers depend too much on what is counted as an incident within a particular institution and the method of recording an incident. Barriers to recording of incidents could be an inefficient paper reporting system. There are also barriers to the reporting of incidents. six respondents stated that they did not have any under-reporting issues. Other institutions all stated that there was some under-reporting with reasons given including:

Societal barriers, dual reporting to police, no obligation to report incidents to security, no obligation to report off campus incidents to security (which may occur in residences), resistance to report minor incidents (“not worth reporting”).

The following chart shows the crime rates for the local boroughs for our respondents.



Institutional level data can be found in Supplement Section I.

The bar on the left hand side is the national average. The lowest five are Canterbury (Kent), Guildford (Surrey), Runnymede (RHUL), Colchester (Essex) and Bath. The top five are Islington (City), Westminster (Kings, LSE), Bristol, Camden (Birkbeck, IOE, SOAS) and Reading.

In comparing institution incident numbers with local crime numbers it is clear that there is in general a lot less crime reported in universities (this statement is made with the caveat that this takes into account a level of under-reporting which is also present in the general population). There are a couple of hotspots identified in the statistics where institutions have more crime than their local areas e.g. levels of theft (non car related) are higher institutionally in Sussex, Essex and Exeter than in their local areas. All these institutions are campuses based outside city centres.

Recommendations for Incident Analysis:

- Across the sector there should be a definition of incident types in line with national standards. This could then be used to compare institutions with like institutions in other areas of the country. It could be used to compare institutions with the local picture available from the Police
- Information to capture as part of incident in line with national standards. This could then be analysed to ensure that appropriate levels of security are offered at certain locations or at certain times of the day or year
- Electronic reporting and recording of incidents. Decreasing the administrative barriers to reporting and recording of incidents will lead to a truer level of reporting which in itself will enable security to improve resource availability
- Institutions should work with their local police forces to analyse crime levels on and off campus which impact on their staff and students.

7.5 Models of Security

One of the key learnings from this study is that there is not one recommended model of security for institutions. Rather than this there are a series of dimensions along which institutions will need to pitch themselves which will then imply a model of security. Broadly speaking, these dimensions appear to be the following:

- Size of unit required
- Level/extent of service the unit is required to run
- Size of budget available
- Employer/Employee relationship
- Level of risk.

Choosing the model of security should be an informed decision rather than one arrived at by historical tradition. The institution should work out the balance of the different dimensions to reach a compromise and a model.

7.5.1 Size of Unit Required

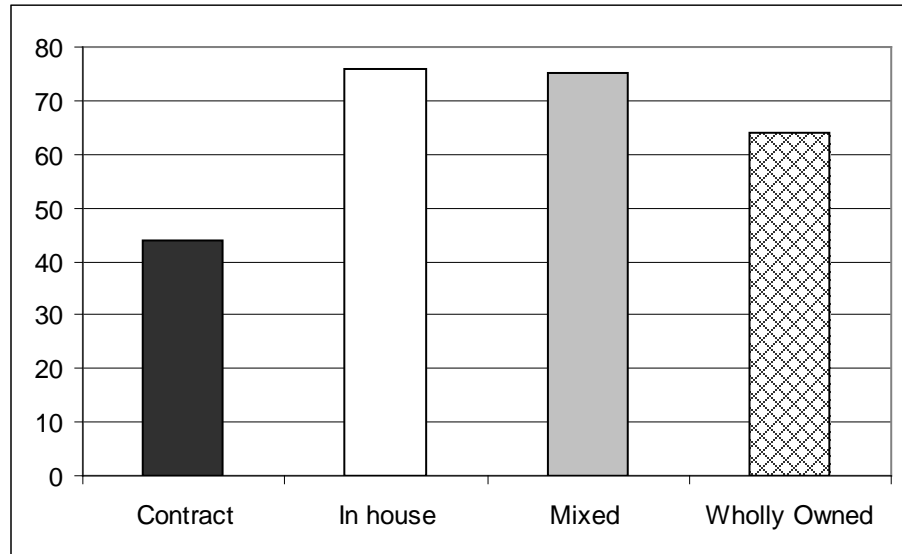
The average size of a department for contract models is 16.1 FTE and for in-house models 35.6 FTE. This is a total of all staff (administrative, management and operational). Where the unit required is small in size it may be more viable to operate from a larger pool of operational staff that can be found within a contract staff.

7.5.2 Level/Extent of Service

Within the questionnaire was a section detailing the various services that could be offered by the security department. Respondents were asked to complete the section and indicate which services were offered by security and which were either outsourced or supplied by other departments within the institution. Where they offered services not listed they were invited to list these as well.

The chart below has been created in the following way.

- Each service was weighted evenly
- Where there was NA or Null response this was discounted from the analysis
- Where the service was offered in part only, it was counted $\frac{1}{2}$
- Where other services were offered, these were added to the weighting
- A percentage of services offered per institution was calculated
- The chart is an average by model.



Institutional level data can be found in Supplement Section D.

Contract security models appear to offer a lot less of the services than in-house or mixed models offer (some of these services may be offered by other departments).

Where there are low levels of service required a simple contract with low levels of training required from the contract staff may suffice and may be the cheapest option. Where high levels of service are required (for example highly trained operational staff to provide first response in all emergencies on site) a professional trained in-house staff may be more appropriate although these services will be available from contract at a higher price.

Certain services seem to be bought from contract as general practice across the respondents. In particular door staff (with the appropriate door licence) are supplied by contract to the Student Unions of most institutions. One other area supplied by contract and not in-house is the dog unit at Southampton.

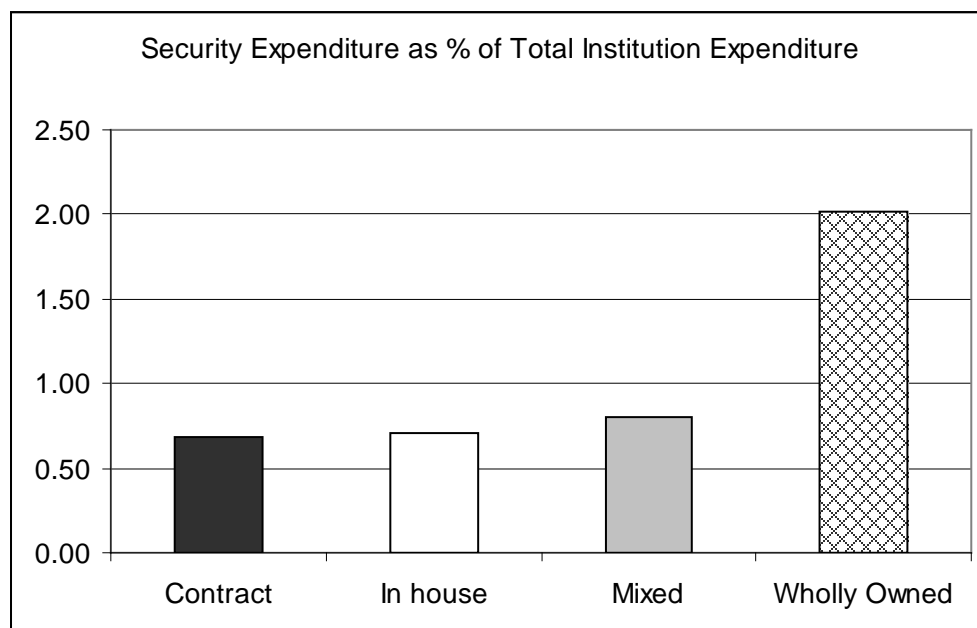
7.5.3 Size of Budget Available

The average expenditure for a contract security model is £407K and for in-house is £914K.

This would seem to imply that where budgets are small, contract security is the most financially efficient model. This allows those institutions to budget more effectively since most staff costs (on costs, on going training, sickness and holiday cover) are paid through the contract hourly rate.

Linking the level of budget to the level of services available might perhaps hide certain costs of services which are not available through security but could be available from other departments. So although the institution may appear to be saving money on their security budget by outsourcing, the other services are still required thus increasing costs to other departments.

Information relating the amount of money spent on security as a percentage of the total expenditure of the institution can be found in the following chart.



There is no significant difference between the values for contract and in-house across our respondents. The wholly owned model is an outlier although there is a large surplus generated which provides a better return than the surplus generated by the institution as a whole.

Information relating the spend on security per customer FTE to model can be found in the Performance Indicator section at 9.1.2.4.

Institutional level data can be found in Appendices C & F.

For contract models the following ranges of pay per hour are apparent at institutions which responded with hourly pay rates (expected to be the amount the institution pay per contracted hour rather than the amount paid to the security guard by the contractor) in the staffing section of the questionnaire:

Security Officers – from £6.18ph to £12.27ph
Supervisors – from £6.72ph to £15.00ph

Note that the lower ends of the scale relate to those institutions out of London whilst the upper ends of the scale relate to institutions in the centre of London.

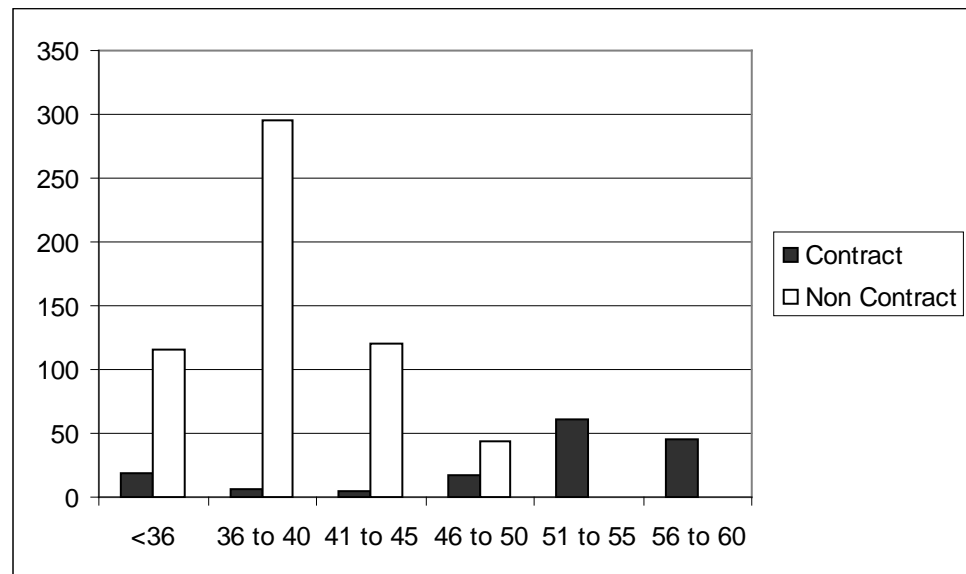
7.5.4 Employer/Employee Relationship

Terms and conditions for staff employment within the Higher Education sector have been under close scrutiny with the HERA Single Spine and implications of harmonisation. Traditionally, contract security staff work long, unsocial hours and low basic pay which is made up by shift allowances and plenty of paid overtime. Contract rotas are designed around 12 hour shifts with an average of over 50 hours per week.

University staff are harmonising and moving to a 36 hour working week with on average three hours of contracted paid overtime. One point to note is that most university staff outside of the security department abide by the European Working Time Directive. This has special restrictions on the

average working week (including overtime) and the number of hours (worked in a single shift and over a 24 hour period) completed by night shift staff. However there is a note concerning an exemption of this clause “in the case of security and surveillance activities requiring a permanent presence in order to protect property and persons, particularly security guards and caretakers or security firms”.

The following chart shows the number of operational staff (headcount) working certain ranges of hours (average per week). The chart differentiates between contract staff and non contract staff rather than by the model which they work within. This recognises that there are contract staff working within some in-house models.

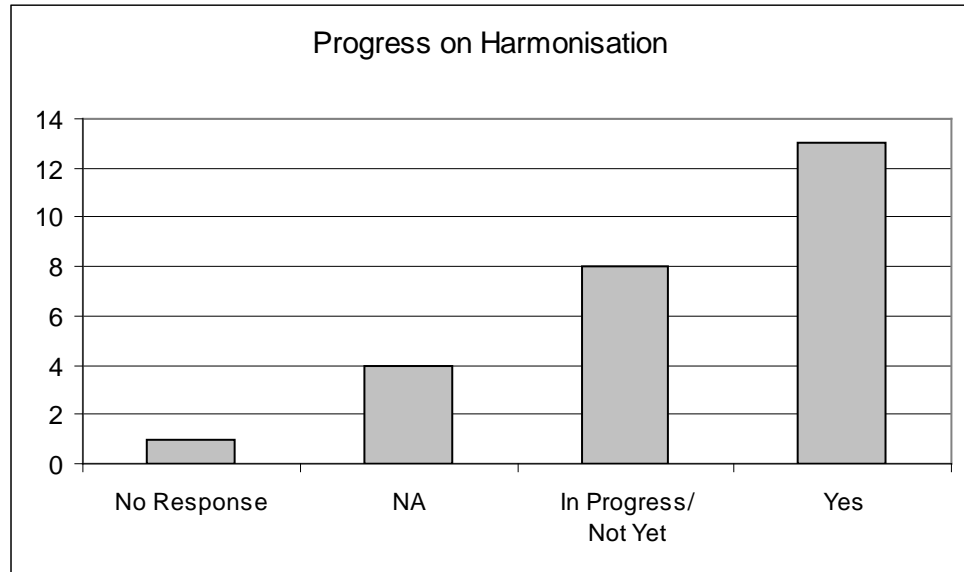


Institutional level data can be found in Supplement Section C.

For contract operational staff, the average number of working hours per week is over 50. There are a few contract security officers at 35 hours (at City and SOAS) and the maximum average working week is 60 hours.

For non contract operational staff, the average working week is 39 hours. This includes contracted overtime where applicable.

The following chart indicates how many respondents have gone through the harmonisation process.



Of our institutions harmonisation is not applicable to four (those who have no in-house staff working within their contract models); a total of eight are in the process of harmonising or will be going through harmonisation in the near future and 13 have completed harmonisation with various impacts.

Of the respondents who have harmonised or have identified harmonised hours, the average is 36. In the security sector shift patterns imply that perhaps more than harmonised hours will be worked. The average contracted overtime agreed is three hours (totalling the 39 hour working week identified above).

Southampton has completed harmonisation with their in-house security staff but has agreed a 48 hour working week. This is out of line with other harmonised institutions; Southampton does not have paid overtime for their operational staff.

Here are some comments made in the questionnaire concerning the harmonisation process: "Staff costs have rocketed"; "unions are holding up process"; "impacts on service delivery"; "effects were catastrophic and still being felt"; "Reduction in one FTE"; "Resource implication, and rosters had to be adjusted, but successfully implemented about two years ago".

There is an informal concern amongst respondents on the impacts of harmonisation on the pay packets of their staff. Supposing an institution is competing with contract companies to attract the best security staff. If it can only guarantee 39 hours per week, the pay rate per hour must increase to stay in line with weekly pay packets from the contract company who may be able to guarantee 56 hours per week. If the hourly rate for in-house staff is higher then the institution will have to compromise either by increasing the security budget to cover increased staffing costs or by decreasing the number of staff available at any one time.

There seems to be a general move within the in-house models to make their staff more professional in terms of training, appearance (uniforms, marked vehicles) and equipment. Decisions along these lines should be linked to the strategic objectives of the department.

7.5.5 Level of Risk

Risk is something which affects the amount and type of security that needs to be supplied to protect the customers and property of the institution. Risks can be formulated as either opportune crime, premeditated crime, reputational and terrorist/activist. The level of perceived risk to the university from these areas can be assessed with input from stakeholders and appropriate levels of security put in place to counter each risk.

Where there are high levels of risk from terrorist or other activist groups, institutions should consider the importance of a trusted, vetted, professional in-house security model. Where risks from these areas are nil, the normal CRB checks required of most contract security companies may be all that is needed.

This subject will be covered in section 7.6 in more detail.

By taking these five factors into account the institution will be able to come to a considered decision on the model that will best fit their requirements.

7.5.6 Learnings from Southampton

The following notes were taken from the presentation by Gary Jackson, Head of Security at Southampton University given at the meeting on July 13th.

At the University of Southampton a decision was made to bring security in-house in the 2005/06 academic year. They were looking for an improved service, a higher level of training of staff and an increase in the amount of control the university had over the services supplied. There was concern over the perception of the security department within the student population. Southampton recognised that there would be significant financial implications of bringing security in-house.

The decision was taken in May 2005 with a view to implement in August 2005. This did not take into account the timelines required to advertise, interview, recruit and train the new security staff. Southampton improved the appearance of the security department by supplying new uniforms and new vehicles, with the particular aim of improving the visibility of the security around the campus. This is balanced by the use of covert security officers.

As part of the effort to bring new security staff into the department, the Chief Security Officer provided the following documentation: Standard Operating Procedures, Terms of Reference, Contracts and job descriptions, Service Level Agreements, Operational Orders (Op Orders), Computerised daily data, Crime/Incident Reporting. This would provide all the information that new staff would need and would also serve as a set of documentation for stakeholders.

Financials considerations which must be taken into account when moving to an in-house model include:

- Setting pay levels to attract the 'right' staff
- Paying contract staff during recruitment and training of in-house staff (understanding that this process takes a number of months where significant numbers of staff are required)
- Advertising costs

- Training costs involved in training staff to appropriate levels (where training costs would previously have been met through the hourly contract rate)
- Equipment costs (where equipment costs such as uniforms would previously have been met through the hourly contract rate).

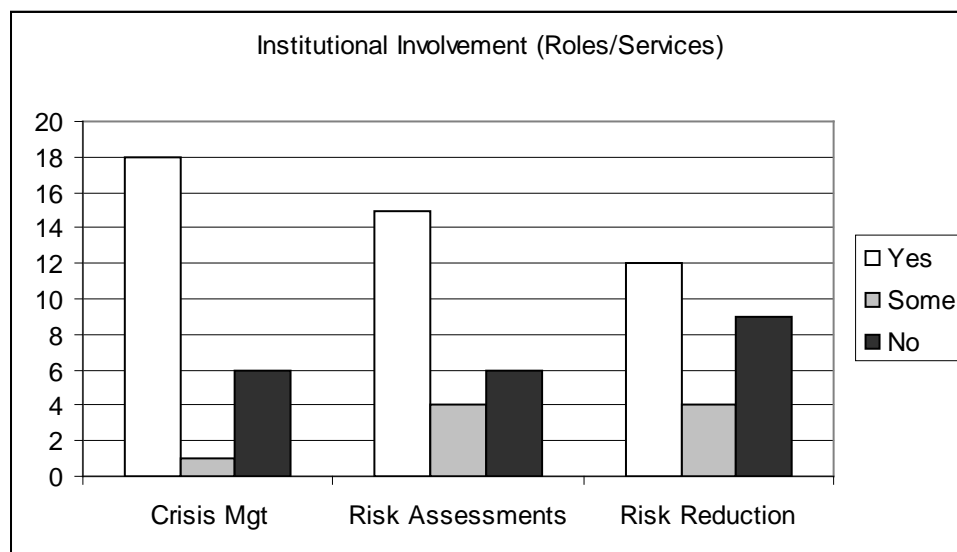
7.6 Risk Management

In the questionnaire there were several references to risk and crisis management activities.

In the roles and services section, institutions were asked whether they had involvement in:

- Crisis / Disaster / Major Incident Management
- Risk Management
 - Risk Assessments
 - Risk Reduction Planning.

The following chart shows the institutional involvement in risk management activities as indicated in the Roles and Services section of the questionnaire.



18 institutions reported involvement in Crisis Management, one had some involvement and six had none. 15 institutions reported involvement in Risk Assessment, four had some involvement and six had none. 12 institutions reported involvement in Risk Reduction activities, four had some involvement and nine had none.

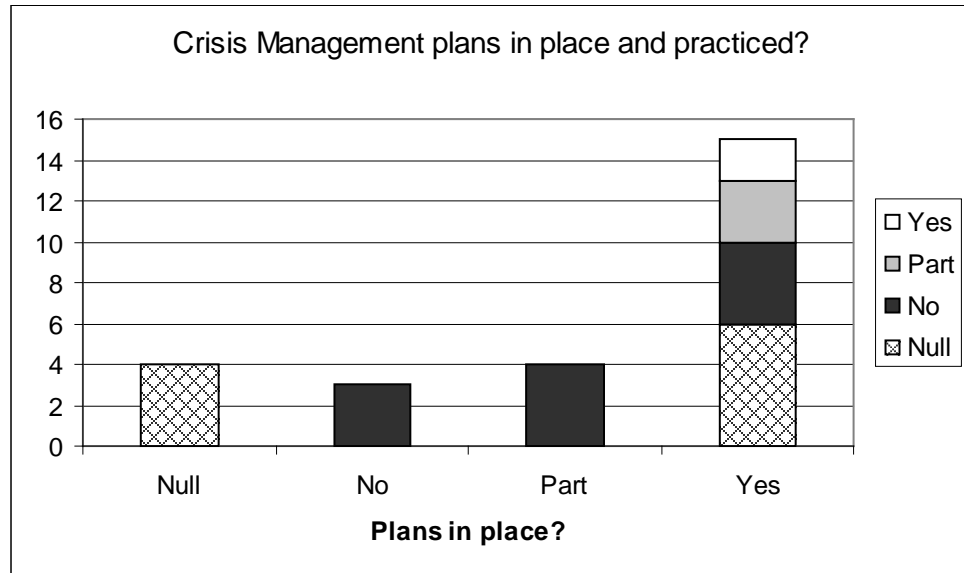
In the Specifics section of the questionnaire, institutions were asked:

- Do you have crisis response plans (with particular security focus) in place and are they regularly practiced?
- Have you completed a risk assessment (from a Security focus) and timetabled actions resulting from it?

Institutional level data can be found in Supplement Section C.

7.6.1 Institutional Involvement in Crisis Management Activities

The following chart looks at whether institutions had crisis response plans in place and whether they were regularly practiced.



Four institutions did not provide data for this question, three had no plans in place and four institutions had partial plans in place but did not practice. Of the 15 institutions that had plans in place, six did not indicate whether plans were practiced, four did not practice, three practice some of their plans (or practice irregularly) and two had completed practices regularly.

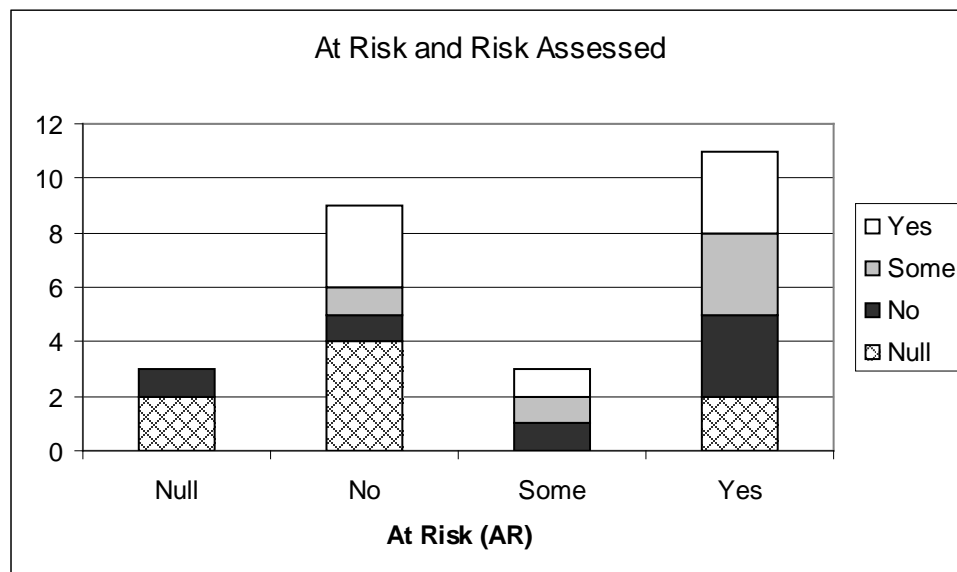
Institutional level data can be found in Supplement Section C.

7.6.2 Institutional Involvement in Risk Assessment Activities

Of the respondents six did not complete this question, seven had not completed a risk assessment, six had partially completed a risk assessment and seven had completed a risk assessment.

Institutional level data can be found in Supplement Section C.

In the sensitive section, institutions were asked to indicate whether they felt at risk from animal rights activists. The following chart shows whether those institutions who felt that they were are at risk at some level had completed risk assessments.



It is expected that those institutions who are at risk from animal rights activists have completed risk assessments and have crisis management plans in place. Of those 11 institutions which identified a risk, only three have completed a full risk assessment. One of those institutions which identified a risk did not have crisis management plans in place.

7.6.3 Learnings from Bristol

The following bullet points were taken from the presentation by Jerry Woods, Head of Security at the University of Bristol given at the meeting on July 13th.

The need for risk assessment

- No clear structure assessing buildings objectively
- Needed clear steer on minor capital spend
- Clear priorities for security/risk interventions
- Identified gaps in security
- Clear, logical assessment required for future use
- Annual update required.

Use of external consultants - advantages

- Limited time to conduct in-house
- Element of objectivity if carried out by consultants
- Able to draw on experience from other projects
- Lend weight to recommendations.

Use of external consultants - disadvantages

- Difficulty in selecting the right company
- Difficulty in understanding University organisation.

Use of consultants - costs

- White Young Green appointed – Integrated Protection department
- Phase 1 – initial assessment - £15K
- Phase 2 – survey/gap analysis - £10K
- Phase 3 – annual updates - £5K
- Phases 1 & 2 complete
- Phase 3 to start September '06 for 4 years.

Contents of assessment – phase 1

- Departmental activity assessed not building
- Risks split into four categories – opportune crime, premeditated crime, reputational and terrorist/activist

- Faculties & departments interviewed
- Impact x probability calculated per activity
- Security measures outlined per category
- Buildings then rated A-E (A being highest risk).

Phase 2 – surveys & gap analysis

- Surveys or more complex buildings conducted by consultants and building categories adjusted
- Security measures proposed – survey to dept
- Gap analysis conducted in-house to look at security shortfalls
- Security costs calculated and built into capital expenditure programme.

Changes made as a result of findings

- Changes made to nightly building checks – reduction of overnight staff cover
- Better able to plan expenditure over next few years
- Clearer priority of security requirements per building
- Clearer guidelines for departments when planning changes to activity.

Advantages/disadvantages of completing the project

- Relative objectivity of building categories
- Clearer financial planning
- Better able to target human resources
- *Took long time to complete – phase 1 two years*
- *Difficulty in designing assessment to start with – no precedent*
- *Difficulty in getting faculties/depts to meet with consultants.*

The University of Bristol has benefited from this approach to risk management and are willing to discuss their learnings with other SUMS members.

8. Way Forward

Many recommendations have been made throughout this report which individual institutions can take on board and implement as appropriate. However in order to move forward with the Benchmarking of University Security Services and provide more accurate management information there are two areas which require further work at a sector level.

Firstly in the area of incident reporting; a single set of incident definitions would significantly improve the comparison of institutions against their local environments. By identifying a set of data to capture when recording an incident, institutions would be able to identify patterns and make appropriate changes to their security provision. AUCSO have begun work in this area.

The second area is financial management reporting, which would benefit from a single set of definitions. By identifying a common set of security cost centres, the FEC cost of supplying security to an institution could be compared accurately.

Appendices to Report 1010/06

9. Performance Indicators

9.1 Strategic Quantitative PIs

9.1.1 Incidents

9.1.1.1 Number per Customer per Year by type

Definition: This is defined to be the total number of recorded incidents per 1000 customers FTE (where customer is defined to be a member of staff or a student and is calculated based on FTE returns to HESA) per year (dependent on a university start date for each year, this is generally August to July) by type.

Advantages: This gives a headline figure of level of incidents experienced by the institution.

Disadvantages: Comparing universities on their levels of incident is inappropriate for several reasons. Firstly, incidents in general are not controllable. Secondly the context of security behind each set of figures is significantly different. There may be value in comparing those institutions whose context is broadly similar (e.g. central London institutions, “out of town and up a hill” institutions). Thirdly, the definitions of incident differ from institution to institution. Some define alarm responses as an incident, others do not, yet others split between malicious alarm activations, fire alarms, lift alarms, panic alarms etc. Finally, the capture rate of incidents differs across institutions. It is accepted that there is some under-reporting of incidents. Estimates range from 5% to 30% with specific types of incident suffering under-reporting and specific cultural issues affecting reporting rates. Some universities consider their incident capture to be so inaccurate (either through under-reporting or systems issues) that they were unable to supply incident information for this study.

Uses: This PI should be used within the institution to measure trends over time. Each institution should compare their incident numbers with those generated by the local police force. Incident numbers by type of incident could be used to target specific incident types which could be controlled by the institution, for example, fire alarm responses.

No chart is included here since the quality of the data is not high enough.

Incident information is held in Supplement Section G and crime statistics in Supplement Section I.

9.1.2 Spending

9.1.2.1 Security Cost per Hectare per Year

Definition: This is defined to be the expenditure of the security department in 2004-05 divided by the total size of the university in that year.

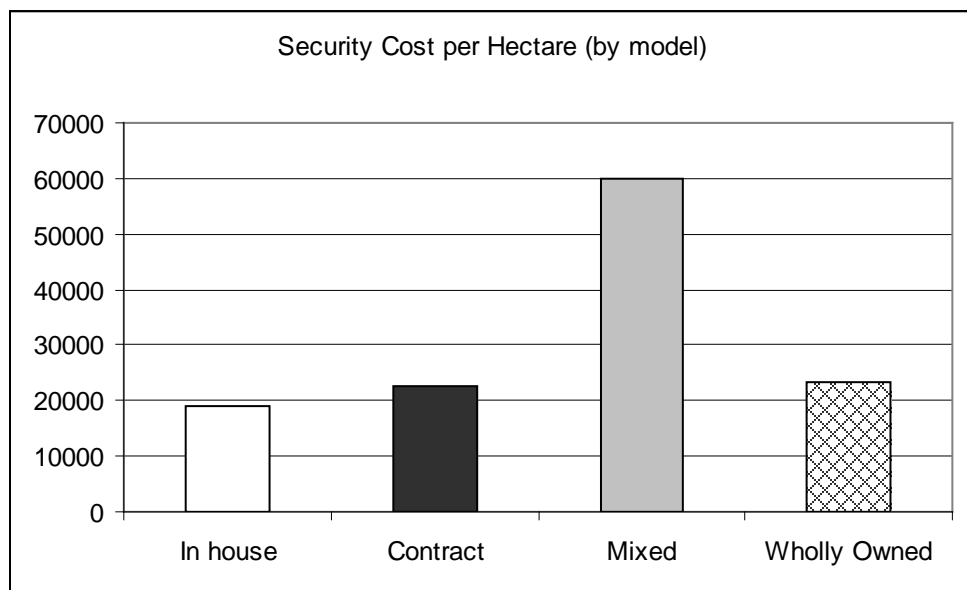
Advantages: This PI will give us an indication of how much each institution spends relative to its size.

Disadvantages: It has been difficult to compare expenditure items where different institutions use different cost centres and budgets vary in complexity. In order to simplify this measure we have excluded capital expenditure (this will be measured but not as a PI). Other issues include the fact that some campus universities will include large amounts of green field area within them which requires little security compared to building space. With the data

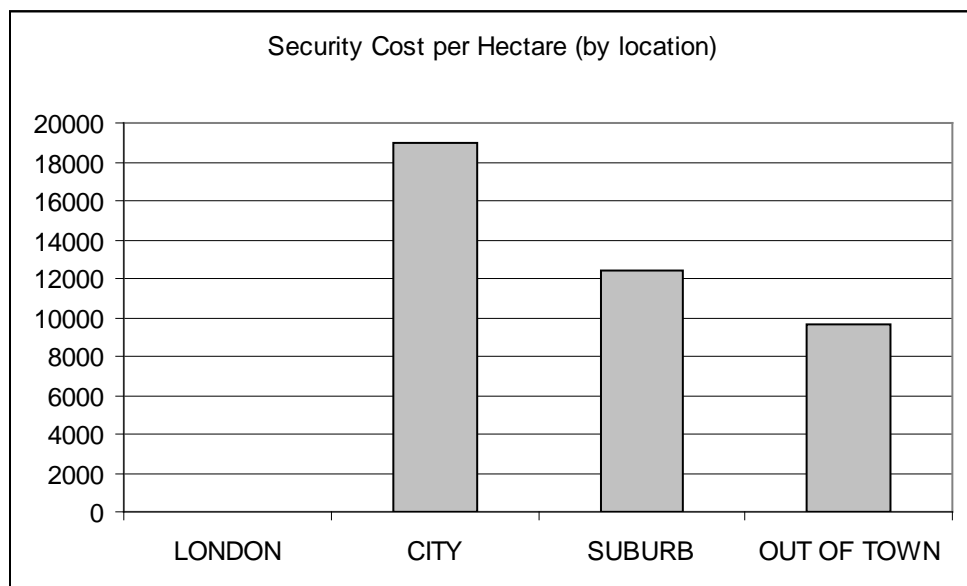
available from EMS, the benchmark is constructed using the total of the Grounds Area (D9) and the Playing fields area (D10). Neither of these measures includes the footprint of buildings. If we were to use the Site Area measure (D8) this would not include the residential estate of the institution. A more rounded measure of size can be found in section 9.1.2.3.

Uses: This PI should be used to compare institutions whose geographical context is similar; for example campus universities like Reading, Loughborough, Exeter and UEA. Those institutions whose area is taken up mainly by buildings or who have public highways between university buildings would provide another group (London based universities, Luton, Plymouth etc.).

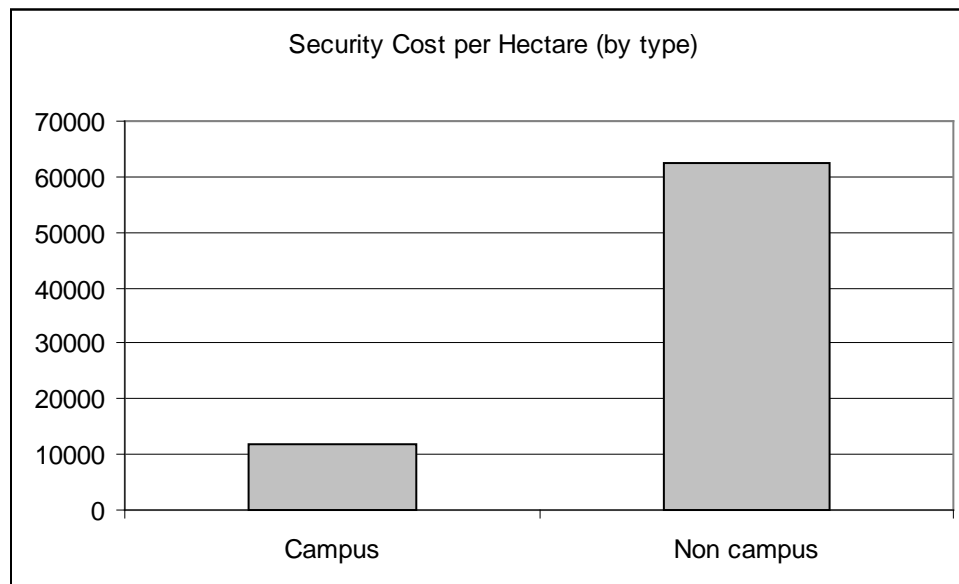
The following charts look at the pattern of Security Cost per Customer FTE by model, location and type.



This chart shows that there is no significant difference between the security costs per hectare by model. The outlier is the mixed model; this is due to a small amount of land for Kings College and distorts the measure.



This chart shows that there is a significant difference between the costs of securing university property with those institutions in city areas costing more than those in out of town areas. Note that London universities did not supply data for grounds and LSE and Kings have been excluded since they would distort the measure.



This chart shows that the cost of securing campus universities is less than that for securing non campus universities. This corresponds to the above chart since most campus institutions are based out of town or in the suburbs.

Institutional level information is available in Supplement Section C.

9.1.2.2 Security Cost per m² Building Space per Year

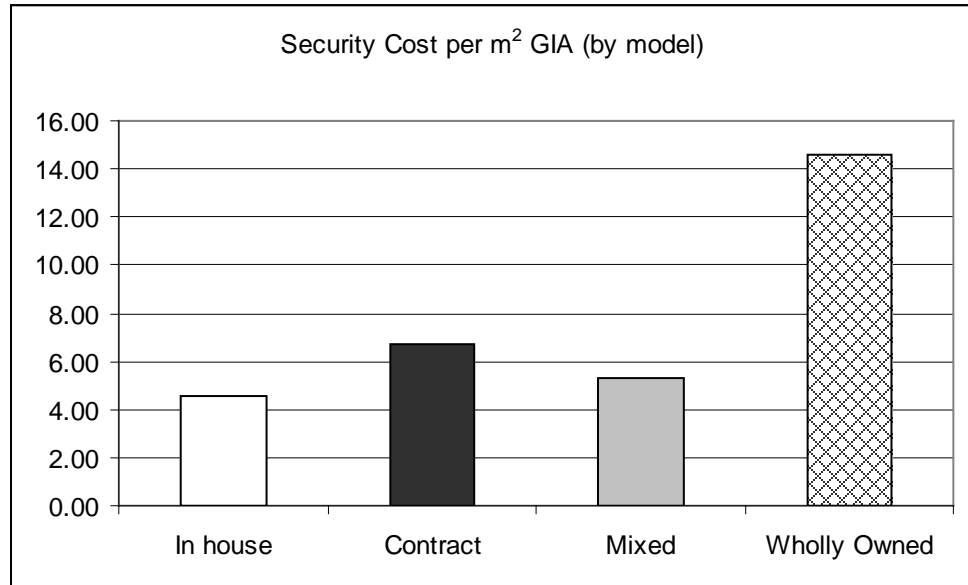
Definition: This is defined to be the expenditure of the security department in 2004-05 divided by the total floor space of the university in that year. The total floor space is taken from the gross internal area (GIA) measure calculated by EMS.

Advantages: This PI will give us an indication of how much each institution spends relative to its size. This PI will give us a more objective measure for those campuses that have varying amounts of green space.

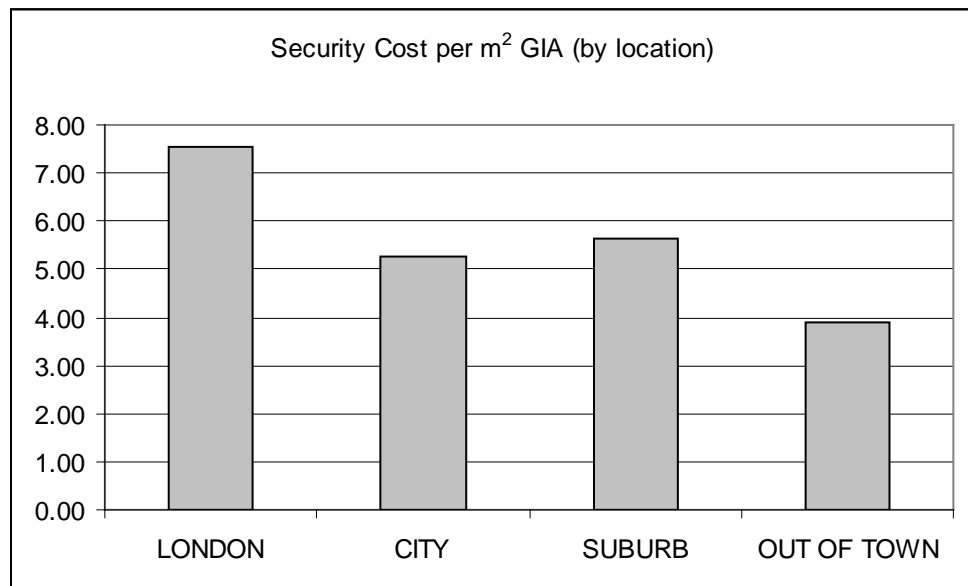
Disadvantages: It has been difficult to compare expenditure items where different institutions use different cost centres and budgets vary in complexity. In order to simplify this measure we have excluded capital expenditure (this will be measured but not as a PI). Other issues include the fact that some universities will include unused building space in their building space measure. There is also no way of knowing which areas are secured.

Uses: This PI is more objective than 9.1.2.1 and could be used to compare all institutions although caveats on non-secured areas may be required.

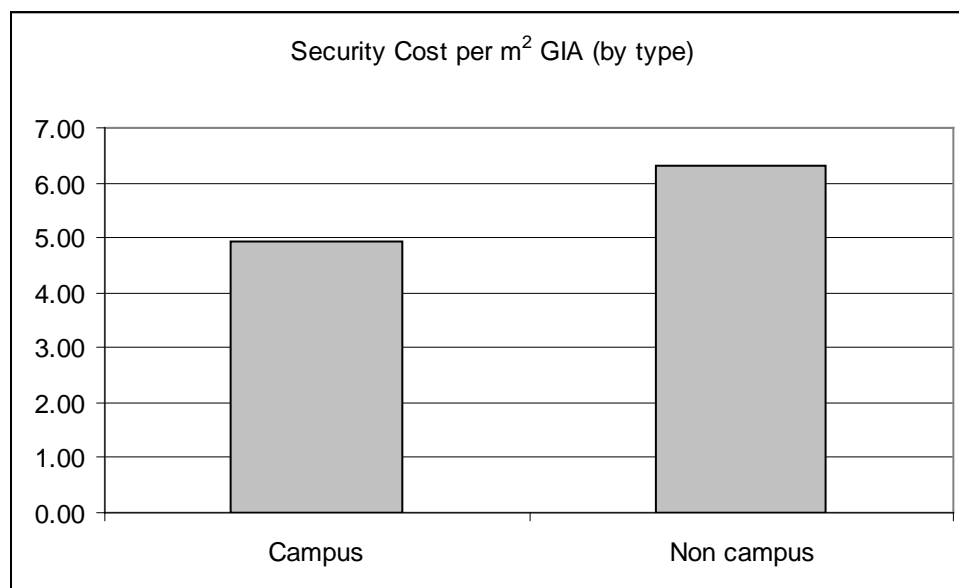
The following charts look at the pattern of Security Cost per m² GIA by model, location and type.



This chart shows that there is a small difference between the costs per m² GIA for contract and in-house models.



This chart shows that in general it costs nearly twice as much to secure institutional property in London than it does in out of town areas.



This chart shows that there is relatively little difference between the cost of securing building space on a campus institution vs. a non campus institution.

Institutional level information is available in Supplement Section C.

9.1.2.3 Security Cost per m² Total Area per Year

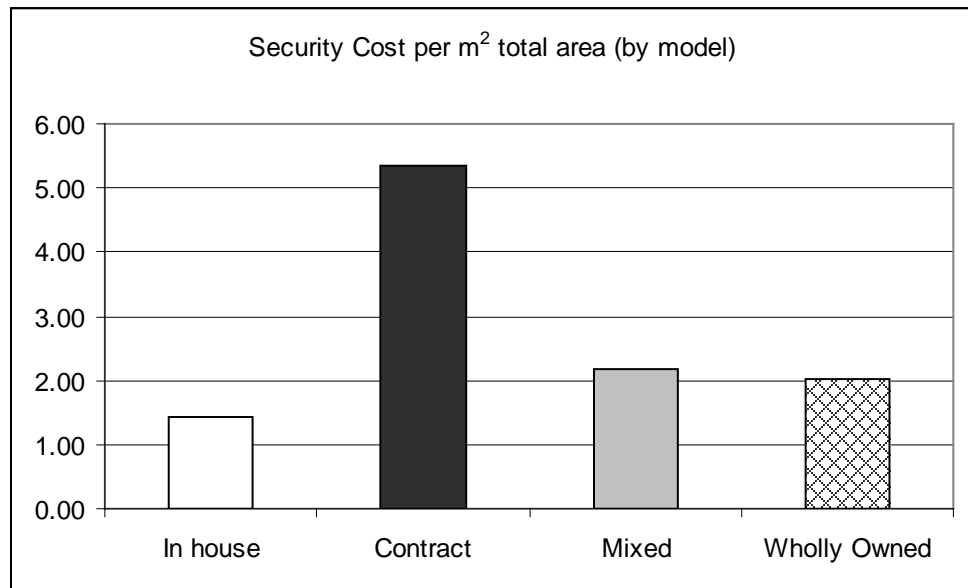
Definition: This is defined to be the expenditure of the security department in 2004-05 divided by the sum of the total floor space and the grounds area of the university in that year.

Advantages: This PI will give us an indication of how much each institution spends relative to its size. This PI will give us a more objective measure for those campuses that have varying amounts of green space.

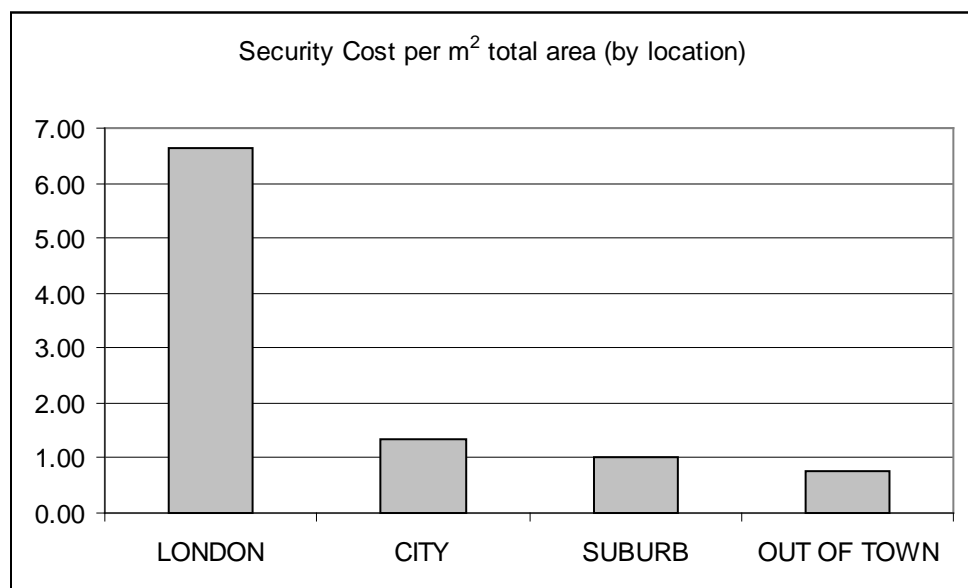
Disadvantages: It has been difficult to compare expenditure items where different institutions use different cost centres and budgets vary in complexity. In order to simplify this measure we have excluded capital expenditure (this will be measured but not as a PI). Other issues include the fact that some universities will include unused building space in their building space measure. There is also no way of knowing which areas are secured.

Uses: This PI is more objective than 9.1.2.1 and could be used to compare all institutions although caveats on non-secured areas may be required.

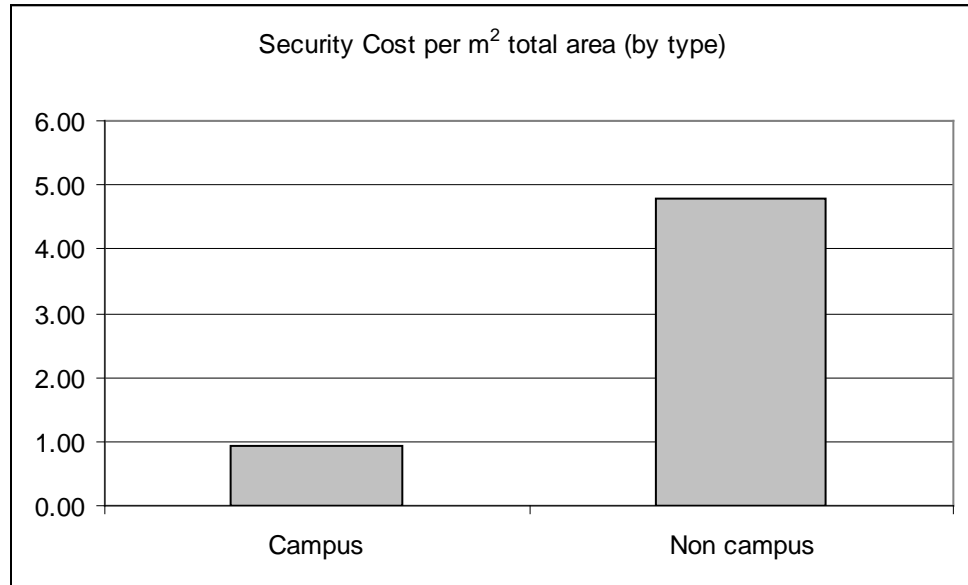
The following charts look at the pattern of Security Cost per m² total area by model, location and type.



This chart shows that securing institutional grounds and building space costs more for those institutions with a contract model of security.



This chart shows that securing institutional grounds and building space costs more for those institutions in London. Institutions outside of London which have more grounds area have significantly lower costs per m².



This chart shows that it costs more to secure land and property of those non campus institutions. This corresponds with the above charts since the London institutions are non campus.

Institutional level information is available in Supplement Section C.

9.1.2.4 Security Cost per Customer per Year

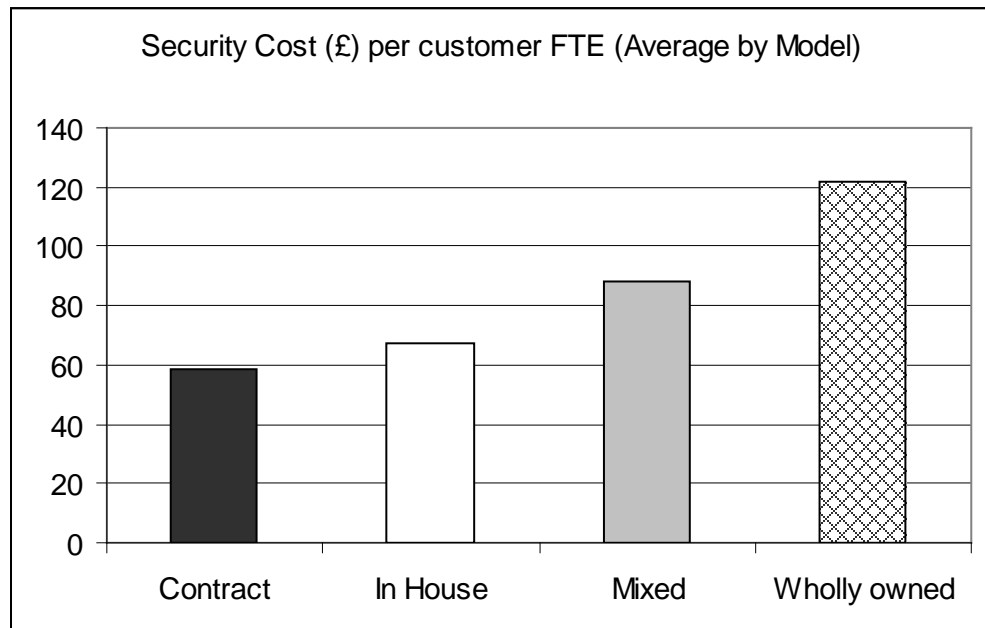
Definition: This PI is defined to be the expenditure of the security department over 2004-05 divided by the total number of customers of the security department, where the customers are students and staff and FTE numbers are used rather than headcount.

Advantages:

Disadvantages: Note the above issues with using expenditure within a PI. Customer numbers can also be skewed; it is easy to come by an FTE number for staff and students since institutions have been supplying this number to HESA for sometime now. However this does not take into account visitor numbers, conference guests and the impact of headcount work which security departments are responsible for (permit issues, inductions etc.). This also does not take into account the level of service offered by security. There may be hidden costs where levels of service are low from security (in general from contract models) and those services are supplied by other departments.

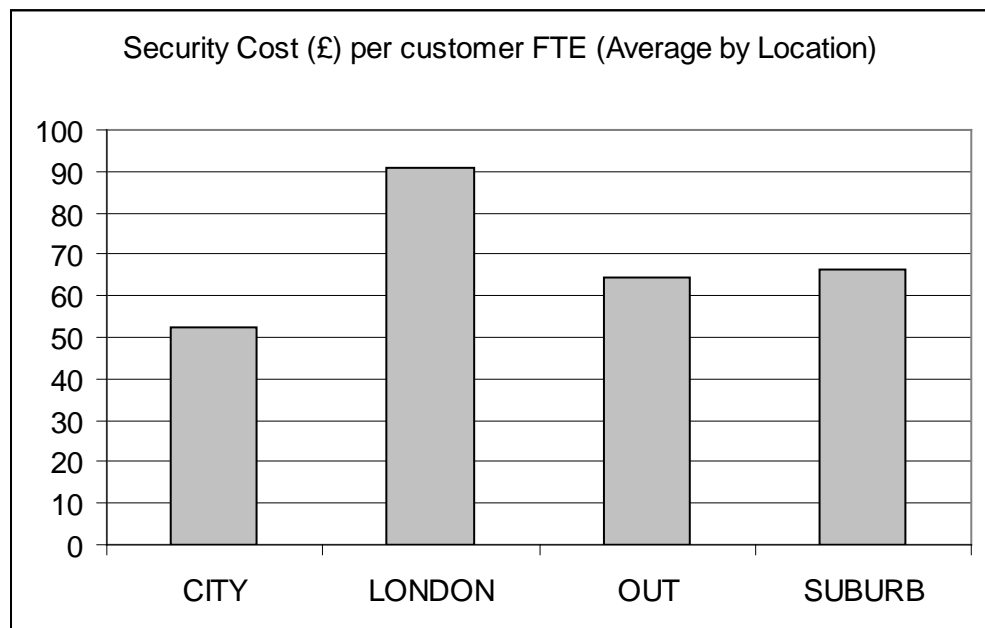
Uses: This PI could be used to compare universities as a broad benchmark. Understanding of the underlying context would ensure that numbers were used appropriately.

The following charts look at the pattern of Security Cost per Customer FTE by model, location and type.

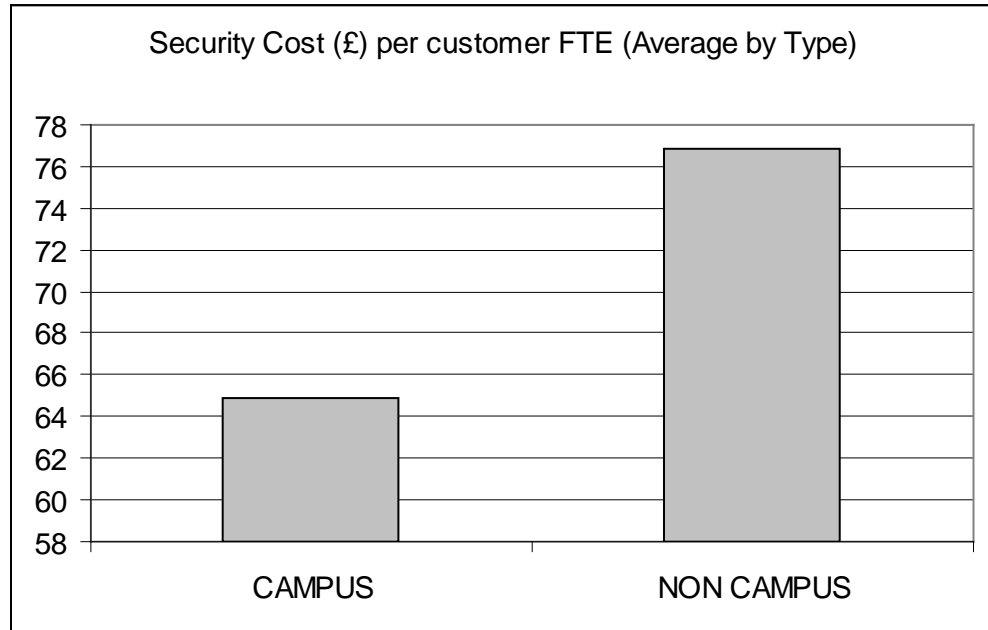


From this chart it appears that contract security costs less per customer than in-house security. It is important to note here the relationship between model and services offered as seen in section 7.5.2.

This relationship is explored further in Supplement Section M at an institutional level.



From this chart, it costs more to supply security in London than other locations. It is interesting that those universities which were based in city centres other than London had a lower cost per customer FTE than those institutions based in suburban or out of town locations.



From the above chart there is a small difference in the Security cost per customer FTE between campus and non campus.

Institutional level information is available in Supplement Section C.

9.1.2.5 Cost of Implementing new Legislation

Definition: This PI is defined to be the FEC of implementing new legislation including the cost of training, covering shifts for training, qualifications, licensing and re-licensing etc.

Advantages: This PI will show institutions how much resource (time/money) is required to implement new legislation.

Disadvantages: Few universities could identify the cost of implementing new legislation; therefore there is no valid comparison to be made at this stage.

Uses: This PI could be used to compare universities. Its main use however would be in understanding uncontrollable costs. Another use could be within decision making concerning the value of implementing new legislation.

There is no chart for this indicator since the quantity of responses was very low.

9.1.3 Staff

9.1.3.1 % Turnover

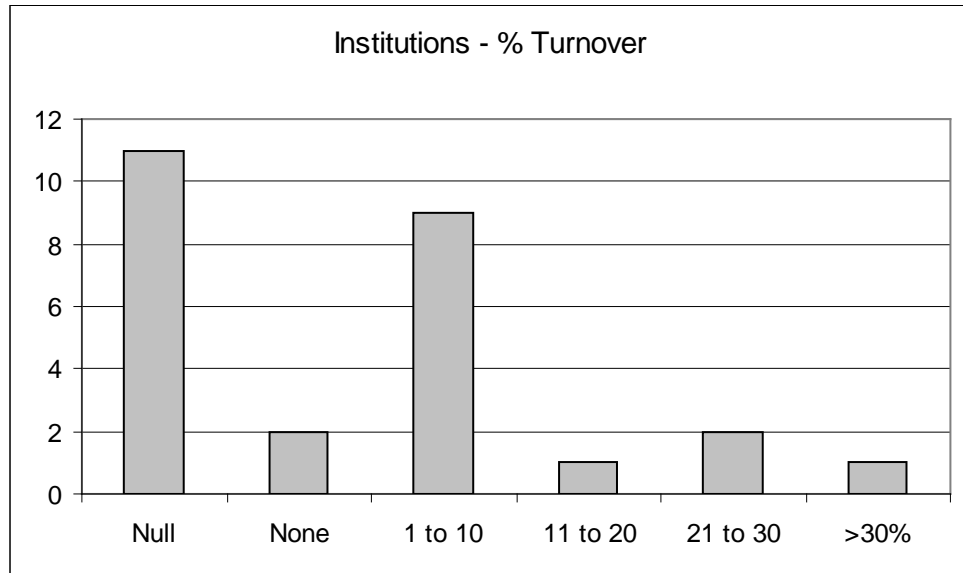
Definition: This is defined to be the number of staff who have left the department as a percentage of the size of the department.

Advantages: We expect turnover to be non-zero but a high turnover is indicative of either issues within the department or a significant restructuring project. Turnover of staff impacts on the department in terms of knowledge and experience of the institution but also on the costs of filling roles temporarily with contract staff as well as increased on-boarding costs.

Disadvantages: Since a high turnover can either indicate issues with the department or a restructuring project, some contextual information is required to draw conclusions from turnover figures.

Uses: This PI should be used within the department to monitor issues with staff as well as results of exeunt interviews. Universities can be compared on this measure.

The following chart shows the pattern of turnover.



Institutional level information is available in Supplement Section C.

9.1.3.2 Ratio Non-Operational : Operational Staff (FTE)

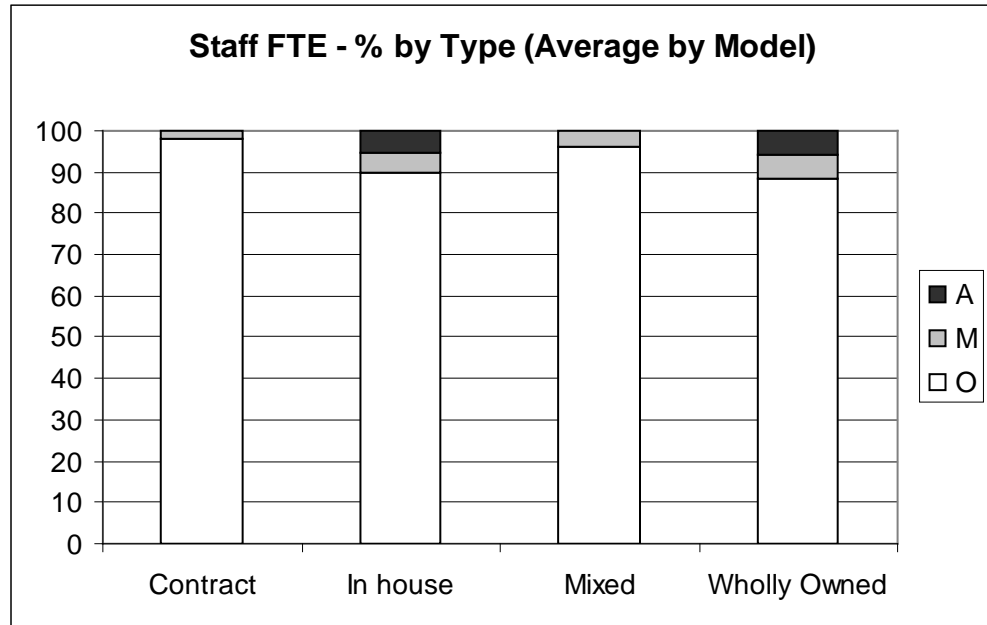
Definition: This PI is defined to be the percentage of Non-operational staff to the percentage of operational staff calculated based on FTE numbers where non-operational staff are managers and administrators and operational staff are security officers, supervisors etc.

Advantages: This PI will give an indication of the relative support available to the security department. Further investigation could show issues with under resourcing of the department at either management or administrative levels.

Disadvantages: Context information will be required to draw conclusions from these numbers. Some institutions will include parking in their staffing numbers and the administration required may sit within security or within estates.

Uses: This PI should be used to compare institutions. It could also be used within institutions to compare support services against each other to see if there are any administrative outages or management overloads etc.

The following chart shows the ratio of FTE Security Staff by model.



* Where administrative (A), management (M) and operational (O) staff.

Institutional level information is available in Supplement Section C.

9.1.4 Coverage

9.1.4.1 Ratio Customers: Security Staff

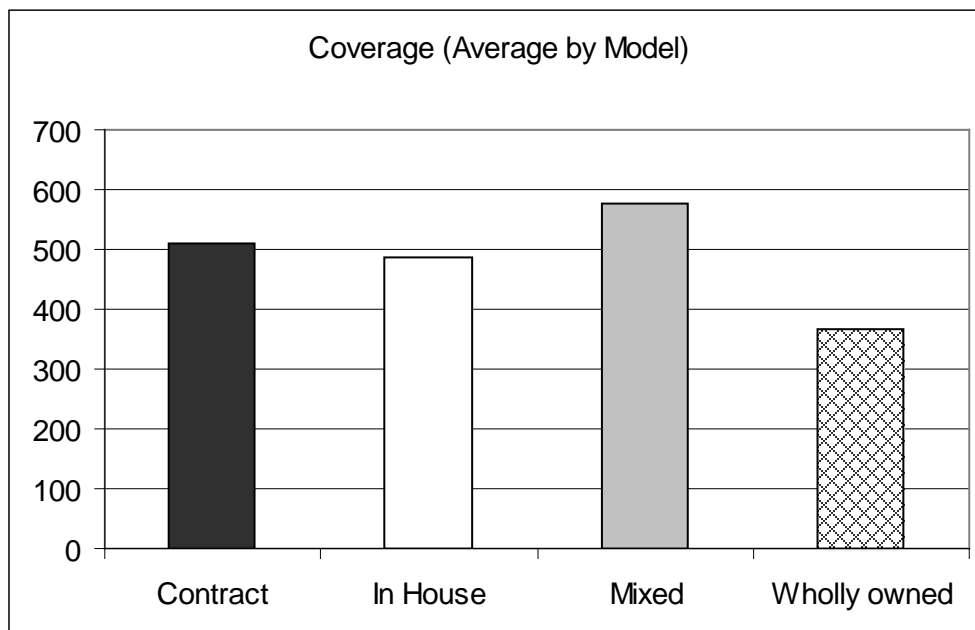
Definition: This PI is defined to be the number of customers per member of operational security staff, calculated on FTE.

Advantages: This PI will give us an indication of the relationship between number of customers and operational security staff. By using an FTE number we should get comparable numbers for those universities which have a large number of part time students or staff.

Disadvantages: There is no input in this measure as to how much those FTE Security staff work. On average non-contract staff work for 39 hours per week and contract staff work on average 56 hours per week. Thus the figures could give a distorted view with contract security models showing much lower levels than in-house models.

Uses: This PI can be used to compare institutions but could also be used within institutions to compare buildings or residences and be part of a service level agreement to set minimum staffing levels.

The following chart shows the coverage as defined above by model.



There is no significant pattern in coverage by model. The highest level of coverage (with the lowest number) is just over 200 customers per security staff FTE at Roehampton and the lowest is Cambridge with over 950 customer per security staff FTE. Cambridge could not supply security staff numbers for colleges so a low level of coverage could be expected. KCL did not supply a full set of staff information so is not included in these numbers.

Institutional level information is available in Supplement Section C.

9.1.4.2 Minutes per Customer

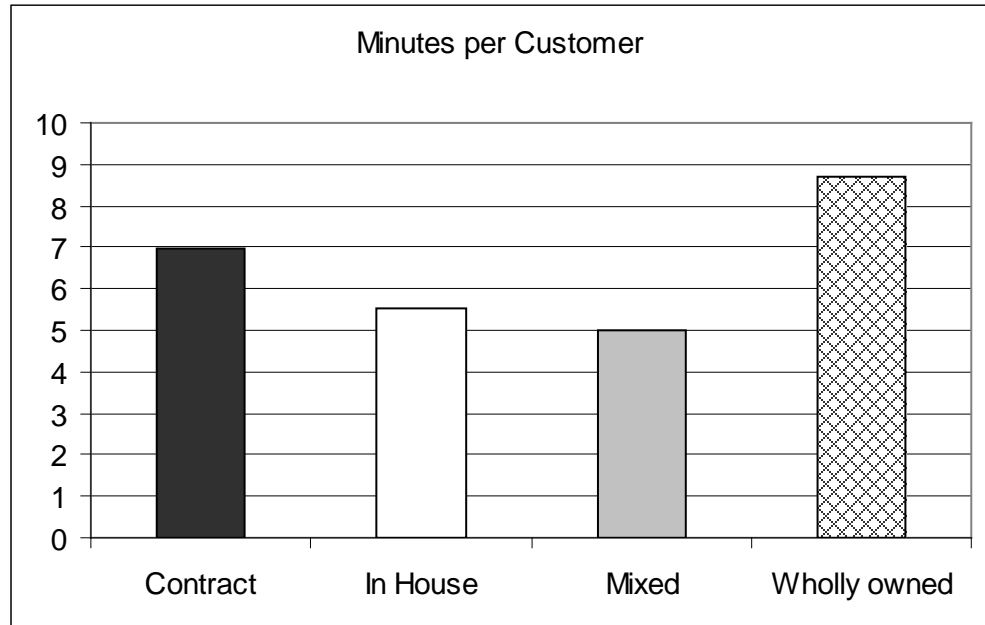
Definition: This PI is defined to be the number of minutes of operational security time per customer per week.

Advantages: This PI will give us a more objective idea of the amount of operational security time available since some FTE work 35 hours and some work 56 hours on average.

Disadvantages: This number is based on average working week figures as given in the study. It is dependent on the shift pattern as to exactly how many security hours are available each week. Comparison of these figures depends on institutions having broadly similar working patterns.

Uses: This PI can be used to compare institutions but could also be used within institutions to compare buildings or residences.

The following chart shows minutes per customer as defined above by model.



This chart shows that contract models appear to offer more operational time per customer than in-house models. The mixed model and wholly owned model only represent one institution. KCL was removed from this analysis since it did not supply enough staffing data.

Institutional level information is available in Supplement Section C.

9.1.5 Stakeholder Focus

9.1.5.1 % of New Customers Proactively Contacted by Security (Raising Awareness)

Definition: This PI is defined to be the percentage (by headcount) of customers seen in their first year at the institution.

Advantages: This PI will show how much awareness is generated by the security department of the work that they do and the services that they offer.

Disadvantages: It is difficult to define a proactive contact and is not something we have been able to track in this study.

Uses: Information to measure this PI is not captured in this study. We have not captured how many customers access the website and how many students and staff attend inductions. Measures for this PI could be taken internally and a target set for awareness within the university population.

Response: We have been able to collect yes/no data based on a series of proactive steps that security departments could have taken to generate awareness amongst students and staff at their institution. This will be analysed to provide a checklist for each institution of the type of steps that they could take to improve awareness at their institution.

There is no chart included here since the study did not collect this data.

9.1.5.2 Community Satisfaction – Decrease in Complaints

Definition: This PI is defined to be the decrease in complaints between one year and the next and is specifically those complaints from the community external to the institution.

Advantages: *This PI will show how well the institution is managing the impact of activities of students and staff on the wider community.*

Disadvantages: *This PI will depend on the communication patterns and how proactive Security is in getting community feedback. This PI may not be valid in more rural areas where the university impact may be lower.*

Uses: *This PI should be used where institutions have particular issues with their local communities. It should not be compared across institutions as contexts are too different. The use of this PI within security will also depend on the institutional policy on student/community relations.*

Response: *Universities should capture complaint numbers over the course of the year and chart the trend. External complaints should be followed up as internal complaints within a certain number of days and actions taken as appropriate.*

There is no chart included here since the study did not collect this data.

9.1.5.3 Customer Compliments, Complaints

Definition: *This PI is defined to be the ratio of customer compliments to complaints.*

Advantages: *This PI will show levels of awareness of security activities (whether good or bad) within the institution.*

Disadvantages: *The results of this PI will be determined by whether the institution has a generally accepted feedback culture or whether feedback is only made where issues have been found.*

Uses: *This PI should be used internally. Complaints should be responded to within a set amount of time and compliments should be posted internally.*

There is no chart included here since the quality and breadth of the data collected from the study was not high enough.

9.1.6 Insurance

9.1.6.1 UMAL Rating

Definition: *This PI is defined to be the rating of the institution for their insurance from UMAL.*

Advantages: *This rating would imply the level of risk the insurance industry estimated for the institution and as such represents an external comparable PI.*

Disadvantages: *This data is not available in the form of a rating. Few institutions worked with their insurance officers in this way.*

Response: *A better PI would be the excess which an institution faced for a specific claim e.g. personal laptop theft. Comparing this would show which institutions were considered low risk and which had worked with insurance companies/officers to decrease their excess by appropriate security and appropriate awareness and prevention campaigns.*

9.2 Strategic Qualitative PIs

9.2.1 Stakeholder Focus

9.2.1.1 Customer Satisfaction – “Feel Safe” & Awareness Measures

Definition: *This PI is the result of internal surveys within the institution and provides an indicator of how safe customers feel within the institution.*

Advantages: *This PI is customer related and is comparable to the national levels shown in the University Lifestyle Survey from Sodexo.*

Disadvantages: *There appears to be some difficulty in running surveys on a regular basis. As customers complete more surveys, quality of returns tends to decrease.*

Uses: *This PI should be used internally to increase awareness of security offerings and to increase buy in from customers. It can be used to highlight particular areas of concern.*

9.2.2 Focus

9.2.2.1 Right Levels Management

Definition: *This PI should be in the form of a check list indicating who has executive responsibility, line management, operational management etc.*

Advantages: *This PI will show whether the security department has the right levels of executive responsibility and line management above it and appropriate operational management within it.*

Disadvantages: *With the various different naming conventions and structures within the institutions this PI may not be valuable.*

Uses: *This PI should be used to ensure that appropriate management levels are in place.*

A table of management levels is in section 7.2.

Institutional level information is available in Supplement Section C and Supplement Section H.

9.2.2.2 100% documents published (strategic plan, vision & SLA/SLS)

Definition: *This PI should be in the form of a check list.*

Advantages: *This PI will show those security departments who have the above documentation in place and reviewed on a regular basis.*

Disadvantages:

Uses: *This PI should be used to ensure that departments have the correct documentation in place as a result of good communications with stakeholders and within the department.*

A chart of document availability by model is in 7.1.4

A chart of documentation availability by institution is in Supplement Section C.

9.2.3 Policies

9.2.3.1 Security Plan Aligned to Other Relevant Department Plans?

Definition: *This PI should be a qualitative judgement on whether the Security Strategic plans and policies are aligned to other relevant department plans.*

Advantages: *This PI will show us whether security has good communication practices with other departments and has consulted them as stakeholders in the formation of their documentation.*

Disadvantages:

Uses: *This PI should be used internally.*

There is no chart included here since the study did not collect this data.

9.2.3.2 Risk Assessment Complete and Actioned?

Definition: *This PI is defined to be the status of the institution with respect to Risk Assessment.*

Advantages: *This will show whether the security department has completed a risk assessment and whether they use the risk assessment as a basis for resource modelling or access control policies.*

Disadvantages:

Uses: *This PI should be used internally.*

A chart is included in section 7.6.2 giving information on involvement in risk assessment.

Institutional level information is available in Supplement Section C.

9.3 Operational Quantitative PIs

9.3.1 Incidents

9.3.1.1 Incident Numbers

Definition: *This PI is defined to be the number of incidents per month by type, site, date, time and cost of incident.*

Advantages: *This PI will show the security department when and where incidents are happening. This information can be used internally to identify hot spots and times of day when customers are most at risk. Appropriate use of high visibility security at these locations and times may deter crime and reassure students and staff. Other uses of the data may be to improve access control or positioning of CCTV cameras.*

Disadvantages: *This level of information is not always available within the incident reporting system.*

Uses: *This PI should be used internally.*

There is no chart included here since the study did not collect this data.

9.3.1.2 Number Captured on CCTV

Definition: *This PI is defined to be the number of incidents captured on CCTV.*

Advantages: *This PI could be used to analyse the value of the CCTV system in either deterring crime on campus, allowing security to monitor areas and respond quickly or in the use of CCTV images to aid identification and conviction.*

Disadvantages: *This PI requires that extra information is captured on the incident reporting form (physical or electronic) and that footage is monitored closely.*

Uses: *This PI should be used internally. It is best used on a short term basis as a check against objectives for the CCTV system rather than an ongoing PI.*

There is no chart included here since the study did not collect this data.

9.3.1.3 Number of Alarms and Response Times

Definition: *This PI is defined to be the number of alarm responses the security service has made and the time it took to respond.*

Advantages: *This PI could be used to understand the resource implications of an alarm response service for security.*

Disadvantages: *This PI requires that security record each alarm response and the time taken to respond. Whilst this is the case in some institutions, it is not a widespread practice.*

Uses: *This PI should be used internally in discussion with stakeholders.*

There is no chart included here since the study did not collect this data.

9.3.1.4 *Response Times by Site, Time, Date, Incident Type*

Definition: *This PI is defined to be the time taken to respond to incident reports by time, site, date and incident type.*

Advantages: *The time taken to respond by security would be used during discussions with stakeholders to set realistic response times within service level agreements. Ongoing the PI would then be used to see whether those service level agreements were being met.*

Disadvantages:

Uses: *This PI should be used internally.*

There is no chart included here since the study did not collect this data.

9.3.2 Staff

9.3.2.1 *Average Shift Hours per Week*

Definition: *This PI is defined to be the average number of shift hours per week.*

Advantages: *This PI would be used to ensure that appropriate working conditions are being met and that overtime hours were at appropriate levels.*

Disadvantages:

Uses: *This PI should be used internally and externally to compare against industry and sector norms.*

A chart showing this data can be found in section 7.5.4

Institutional level information is available in Supplement Section C.

9.3.2.2 *Appropriate Staffing Presence Maintained... In the control room? On patrol?*

Definition: *This PI is defined to be the staffing levels of the security department on shifts across the various locations where security is required.*

Advantages: *This PI could be used within Service Level Agreements to define the minimum staffing levels expected.*

Disadvantages: *This PI requires this information to be captured in a systemic fashion and perhaps a Deister style patrol logging system to be put in place to prove that.*

Uses: *This PI should be used internally.*

There is no chart included here since the study did not collect this data.

9.3.3 Response

9.3.3.1 *Provide Response Within X Time Limit in Y% of Cases*

Definition: *This PI is defined to be the percentage of cases in which the response from security was made within the appropriate time frame.*

Advantages: *This PI would be used within service level agreements as discussed with stakeholders. If priorities were agreed on incident types, different levels of response would be appropriate.*

Disadvantages:

Uses: *This PI should be used internally and is a target which will help improve operational behaviour.*

There is no chart included here since the study did not collect this data.

9.3.3.2 *Provide Assistance in Emergency Calls Within X Time Limit in Y% of Cases*

Definition: This PI is defined to be the percentage of cases in which assistance from security was provided within the appropriate time frame.

Advantages: This PI would be used within service level agreements as discussed with stakeholders.

Disadvantages:

Uses: This PI should be used internally and is a target which will help improve operational behaviour.

There is no chart included here since the study did not collect this data.

9.3.3.3 *Acknowledge Within X Days Stakeholder Complaints, Resolve/report Findings with Y Days*

Definition: This PI is defined to be the response times to complaints/compliments received by the security department.

Advantages: This PI will improve securities communications patterns with the staff, students, visitors and community of the institution.

Disadvantages: This

Uses: This PI should be used internally.

There is no chart included here since the study did not collect this data.

9.4 Operational Qualitative PIs

9.4.1 Security Readiness

9.4.1.1 *Crisis/Contingency Plans in Place/practiced*

Definition: This PI is defined to be a check of whether the security department has crisis/contingency plans in place and regularly practiced.

Advantages: This PI will give an indication of security's readiness to respond in a crisis situation.

Disadvantages:

Uses: This PI should be used internally.

A chart showing this data can be found in section 7.6.1

Institutional level information is available in Supplement Section C.

9.4.1.2 *Ability to Supplement Staff nos. in Emergency Situations with Appropriately Trained Staff*

Definition: This PI is defined to be a check of whether the security department is able to supplement staff in times of need with appropriately trained replacements.

Advantages: This PI will give an indication of security's ability to react to changing situations.

Disadvantages:

Uses: This PI should be used internally.

Of the respondents seven use voluntary overtime to supplement staff numbers, five use contract relief, three use staff from other departments, seven use a mix of the above, one was unable to supplement and two did not supply information. A dependence on voluntary overtime can sometimes lead to outages and may impact on working time conditions. Supplementing staff should be taken into account when setting budgets since overtime budgets can vary considerably.

10. Contact list for participants

Institution	Contact Name	Job Title	Contact (Email)	Contact (Phone)
BATH	Brian Schofield, Richard Law	Head of Security Services	b.schofield@bath.ac.uk,	01225-386350
BBK	Elizabeth Whitehead	Facilities Manager	E.Whitehead@bbk.ac.uk	020 7631 6012
BRIS	Jerry Woods	Security Services Manager	Jerry.Woods@bristol.ac.uk	0117 331 1002
BRU	Chris Hoad	Security Manager	chris.hoad@brunel.ac.uk	01895 265337
CAM	Christopher Lewis	University Security Adviser	cdl30@admin.cam.ac.uk	01223 332839
CITY	BERNADETTE DUNCAN	HEAD OF SECURITY	b.a.duncan@city.ac.uk	020 7040 8041
ESS	Greg Dumbrell	Security manager	gregd@essex.ac.uk	01206 872361
EXE	ALLAN EDGCUMBE	HEAD OF SECURITY	A.C.Edgcumbe@ex.ac.uk	(01392)0263046
HERT	Frank Benton	Director of Estates	f.r.benton@herts.ac.uk	01707 286010
IOE	Anthony Tyrrell	Facilities Manager	a.tyrrell@ioe.ac.uk	020 7612 6110
KCL	Jennifer Briggs	Director of Facilities & Services	jennifer.briggs@kcl.ac.uk	0207 848 3310
KENT	Michael Epps	Security Manager	M.J.Epps@kent.ac.uk	01227 823829
LEI	Jim Shaw	Head of Security	jas43@le.ac.uk	(0116) 252 2522
LOU	Roger Kennedy	Security Manager	R.J.Kennedy@lboro.ac.uk	01509 222115
LSE	Bernard Taffs	Head of Security	b.taffs@lse.ac.uk	020 7955 6055
LTON	Geoff Hillman	Deputy head of Facilities	Geoff.Hillman@luton.ac.uk	01582 743835
OXBS	Mike McCluskey	Site Services Manager	mmclluskey@brookes.ac.uk	01865 483059
PLY	Wini Coles	Asst Director of Learning Facilities	w.coles@plymouth.ac.uk	01752 232263
REA	Maureen Mills	Security Services Manager	m.mills@rdg.ac.uk	0118 378 8046
RHUL	A Bathews/Jonathan Main	Security Manager/Asst Director Ops.FM	a.bathews@rhul.co.uk	01784 443069
ROE	Justin Cook	Deputy head of security	justin.cook@roehampton.ac.uk	0208-392-3108
SOAS	Deborah Rhys	Facilities Manager [Security and Cleaning]	dr@soas.ac.uk	0207 898 4904
STON	Gary Jackson	Chief Security Officer	G.K.Jackson@soton.ac.uk	0238 0593964
SUR	Barry Jakeman	Chief Security Officer	b.jakeman@surrey.ac.uk	01483 689937
SUX	DAVID LAMPER	HEAD OF SECURITY SERVICES	D.J.Lamper@sussex.ac.uk	01273 678233
UEA	Michael J. McCormack	Access and Security Manager	m.mccormack@uea.ac.uk	01603 592040

11. Acknowledgements

- 1) Members of the lead team for testing the questionnaire and helping to develop the performance indicators.
- 2) Individuals at each university for completing the questionnaire and taking time for a meeting at their institution.
- 3) HEFCE Report 02_30
- 4) HEFCE Tool chest
- 5) EMS for supplying estates data
- 6) HESA staff and student numbers

12. Contents Lists for the Supplement to Report 1010/06

- A. Foreword
- B. Proposed Key Performance Indicators developed by the Lead Team
- C. Performance Indicators
 1. Spending – Security Cost per hectare per year
 2. Spending – Security Cost per m2 building space per year
 3. Spending – Security Cost per m2 total area per year
 4. Spending – Security Cost per Customer FTE
 5. Staff – % Turnover
 6. Staff – Ratio Operational : Non operational staff FTE
 7. Coverage – customers per security staff FTE
 8. Coverage – minutes per customer
 9. Focus – Documentation Available
 10. Policies – Risk Assessment Complete and Actioned
 11. Staff – Average Shift hours per week
 12. Security Readiness
 13. Performance Indicators – Data Table
- D. Context
 1. Roles & Services
- E. Income Information
 1. Total Income by institution
 2. Income by Income Type
 3. Data for Security Income
- F. Expenditure Information
 1. Security Expenditure
 2. Expenditure by Expenditure Type
 3. Percentage of Security Expenditure Spent on Outsourcing
 4. Percentage of Security Expenditure Spent on Staffing
 5. Expenditure on Security as Percentage of Institutional Spending
 6. Data Table for Expenditure by type
- G. Incident Information
 1. Institution Incident Data
- H. Staffing Information
 1. Institution Incident Data
 2. Average staff costs per FTE
- I. Crime Statistics
- J. Estates Data
- K. Staff & Students numbers
- L. Sodexo National University Lifestyle Survey
- M. Combining Factors

©Southern Universities Management Services 2006

Copyright in this report is held by Southern Universities Management Services. The commissioning institution is free to copy or reproduce material in whole or in part, provided that the source is acknowledged and it is not used for commercial gain.

Subject to consent having been given to the distribution of the report to other members of Southern Universities Management Services consortium, members may copy or reproduce material for internal use, provided that the source is acknowledged.

The moral rights of the author should be respected in all instances.

This report has been produced for and reviewed by the commissioning institution. The statements and views expressed represent the understanding of the author and the institution arising through the approach described at the time of writing.