

# Management of security services in higher education

## Case studies and cameos

The UK Value for Money Steering Group

© 2002 HEFCE/SHEFC/HEFCW/DEL

# Management of security services in higher education: Case studies and cameos

## Contents

	<b>Page</b>
Introduction	2
<b>Case studies</b>	<b>3</b>
1. Assessing security risks	3
2. Developing a security strategy	7
3. Training for security staff	11
4. Balancing technology and other security measures	14
5. Evaluating in-house and contracted-out security provision	18
<b>Cameos</b>	<b>23</b>
Security environment (2.1)	25
Legislation, quality and standards (2.2)	26
Insurance, assessment and management of security risks (2.3)	27
Security strategy (2.4)	27
Security management structures and links with other services (2.5)	29
Raising awareness of crime, and crime prevention (2.6)	30
Procurement (2.7)	34
Staff training and development (2.8)	35
Balancing technology with other security measures and resources (2.9)	38
Funding and service performance (2.10)	41
List of abbreviations	43

## **Introduction**

As part of the study of security management in higher education by the UK Value for Money Steering Group, higher education institutions (HEIs) provided many instances of good practice, and examples of solutions to security problems. So that other institutions can learn from their experiences, these are presented here as a series of case studies and cameos. This is one of three outputs of the study. The *National report* (HEFCE 2002/30, June 2002) identifies the key management issues for governors, senior managers and heads of security in developing and reviewing security services, to ensure that they are effective and provide value for money. A *Security toolchest* and these *Case studies and cameos* contain practical guidance and ideas to help institutions identify and implement their own management solutions. Both are available on the web at [www.aucso.org.uk](http://www.aucso.org.uk).

### **Case studies**

The case studies focus on five key areas, and draw on the experiences of several institutions. Clearly there is no single correct approach. There are constraints on resources and management time, and often a successful outcome will depend on gaining the support of staff and students. However, the case studies – and the accompanying self-assessment questions – aim to highlight the issues, and to help institutions identify effective solutions.

### **Cameos**

The cameos describe how individual institutions have approached specific problems in managing security. They are grouped under the 10 main elements discussed in the *Security toolchest*.

# Case study 1: Assessing security risks

**National and local crime rates were rising, and crime-related activities were affecting the institution's premises. These crime-related activities included thefts and vandalism.**

## Issues and considerations

The institution has always had a good relationship with the police and other local authority and emergency service organisations.

Installation by the local authority of more closed circuit television (CCTV) systems in the city centre was causing a 'ripple' of crime to be displaced on to the institution's campuses/precincts. The subsequent criminal activities and vandalism were increasingly affecting the institution.

The senior management team was advised of the situation by the head of security. The head of security reported an increasing level of security incidents, as recorded by his security staff. In his view, local criminals regarded the institution's buildings as 'open house'. In some instances, the people involved were well known to both the security staff and the police.

Expensive audio-video equipment and computers were being targeted. Academic staff were not always reporting some of these losses. Claims against the insurers were not dealt with by security but by another department. No exchange of information regarding incidents and subsequent claims took place between the two departments. Equally, the replacement cost of stolen items had not always been correctly accounted for in the institution's asset registers and financial records, but were 'written off' to revenue as consumable items.

## Options and solutions

The institution decided to carry out an 'assessment of risk' survey for each building and the campus. Although this seemed a daunting task, there were some similarities between groups of buildings, and once a thorough risk assessment had been made of one typical building, the remaining buildings in the group were deemed to have similar characteristics.

There are many risk analysis models. The one used by the institution was developed by the Chartered Institution of Building Services Engineers (CIBSE). Insurance surveyors, chartered architects and structural engineers have created other risk models.

The survey took the following matters into account:

- who should undertake the assessment
- definition of risk criteria and priorities
- review arrangements
- links with other contingency planning arrangements.

It identified the following matters to be considered:

*People*

- a. Authorised users.
- b. Access permissions.
- c. Permissions for other users, eg taxis, deliveries, contractors.

*Buildings*

- a. Location.
- b. Nature of site.
- c. Building construction and design.
- d. Day by day management of the building.
- e. Building function and activities.
- f. Details of past security record.
- g. Value of contents of building.
- h. Security measures in place.
- i. Insurance arrangements.

*Equipment*

- a. Asset registers.
- b. Inventories.
- c. Acquisition and disposal of equipment.
- d. Storage.
- e. Maintenance of equipment.
- f. University regulations and procedures.

*Specific security measures and arrangements*

- a. Alarms and key management.
- b. Barriers.
- c. CCTV.
- d. Landscaping.
- e. Lighting.
- f. Manned patrols and static posts.
- g. Other security measures and controls.

*Specific security issues*

- a. Lone working.
- b. Car parking.
- c. Emergency arrangements and procedures.

The criteria used were as follows:

- building location surroundings: general location, character of neighbourhood, level of occupation of adjacent premises during risk periods, landscaping, 'surveillance' view offered to passers-by, level of lighting

- building and structural strength: ease of access and movement, type of structure, type of door and window frames, quality of door and window security fittings
- building contents: visibility, value, transportability, disposability
- supervision: hours of occupation, numbers and level of supervision of visitors
- consequences of loss: sensitivity, inconvenience
- history of loss: level of previous loss for building and for occupier
- existing security measures: intruder alarms, security guards, CCTV and observation
- recommended level of protection: factor ratings were applied to each of the above criteria to assess the level of risk from very low (no special measures) to very high (physical and extensive electronic measures).

The outcomes of the overall security risk assessment, for the entire campus, were compared to an earlier CCTV survey that had identified the vulnerable areas of each building/campus area. The head of security was also a member of the institution's insurance panel and periodically consulted the institution's insurers regarding specific risks identified during security and insurance company surveys. The head of security and his staff undertook the assessment, and retained the risk analysis documentation for future reference.

The institution decided that it was important to co-ordinate business continuity plans with the assessment of security risk. In developing this approach, the institution set up a task group (which reported to a risk management group) to identify the most important risks faced by the institution. A management plan was drawn up to address these risks. The plan covered security (such as computer theft), health issues (eg an outbreak of meningitis), and major emergencies, such as fire, explosions, floods, and acts of terrorism. The head of security is a member of the institution's risk management team. The head of security has delegated management responsibility for implementing key arrangements in the event of a major emergency, as part of the management plan.

All departments were involved in drawing up the implementation plans. It was the responsibility of the head of security, on behalf of the risk management group, to confirm that all departments had implemented the plans. The management plans implemented to date cover halls of residence, IT services and security.

The plan includes training for all key staff, including security staff, and it is periodically tested with local emergency services (both as a paper exercise and/or real life scenarios). The head of security has established a call-off contract for security staff. These additional back-up staff have received induction training, to maximise their effectiveness on campus in the event of a major incident.

The institution's management plans and risk assessment strategies are regularly updated and reviewed by the risk management group. An operations manual details the procedural arrangements carried out by the institution's security services; modern security systems are in place to deal with all reported

matters, including major emergencies. There is a separate procedural manual for major emergencies, which has been published and circulated within the institution and to its local community partners (the local authority, police and emergency services). It has the approval of the City-Centre Emergencies Co-ordination Committee and was successfully tested as a paper exercise.

All security incidents notified to security staff are recorded. The data are used to develop management statistics, which are reported to the senior management team and others. The institution is a member of a security performance group, which consists of two other HEIs and one further education college (FEC). Management data are exchanged between members to support continuous improvements in the delivery of their security arrangements. The institutions concerned have collaborated previously on a number of issues; they have a similar management approach and are of comparable size.

### **Self-assessment questions**

1. What consultation and partnership arrangements are in place regarding crime awareness, prevention and deterrence? How effective are these? What else can be done?
2. How effective are the relationships with the police and local emergency services?
3. What are the areas of concern? What actions have been taken to discuss and resolve them?
4. What is the nature of crime on campus? What actions have been taken – either by the institution, or in partnership with others?
5. How do the institution's rates of crime and security incidents compare with local crime rates?
6. How are these reported within the institution?
7. How are insurance losses reported and accounted for? Is the head of security advised?
8. How often are insurance reviews undertaken by the institution's insurers? Who is involved? Does this include the head of security? Is there a two-way exchange between finance and security about insurance reporting?
9. How does the institution assess security risks? Is there a formal method for risk assessment?
10. How is the senior management team involved in assessing/evaluating risk priorities?
11. When was the last risk assessment undertaken?
12. Has the institution set up a risk management group? Does it cover major emergencies?
13. What review procedures are in place? What training is offered?
14. What systems are in place for security and insurance incident reporting and monitoring? Can these be co-ordinated/integrated?

## **Case study 2: Developing a security strategy**

**The institution wanted to maintain a balance between an open campus policy and adequate protection for both people and property.**

### **Issues and considerations**

The institution's objective was to create a reasonably protected workplace for its students and staff, within an open campus. However, the issues linked to these considerations had not been drawn together. Neither had the institution mapped out how it would deal with security matters in the future.

On appointment, the new head of security found that the institution had no strategy for implementing security initiatives over the next five years. Nor was there any documentation on how the institution would respond to legislation concerning data protection, crime and disorder, and human rights. The head of security was aware that there was a substantial volume of good practice within the HE sector and guidance from the security industry, the British Standards Institute and others. However, he was not clear to what extent the institution wished to incorporate this guidance within its security operations and procedures.

The senior management were under the impression that there was or had been a security strategy in place, even if this was 'not formalised'. The new head of security felt that any such strategy resided solely 'in the head' of his predecessor. On further research, he found that there were some 'policy' documents, but these related to specific security measures and had never been put together to form a coherent strategy. The head of security believed it would be difficult to gain the support of the senior management team for future initiatives if such a policy was not documented. Initiatives could be jeopardised if they were implemented piecemeal or were regarded as being ad hoc.

Different options could be considered as part of developing a strategy, resulting in a more effective integration of measures and a better use of finite resources. There was also some security equipment that would come to the end of its operational life within two to three years. A plan would be needed for replacing the equipment and how this was to be financed.

There was a further concern for the head of security. He wanted to adopt a risk management approach in providing the institution's future security services. This would take account of the threats and risks identified by security staff, and form part of the institution's wider approach to risk management. There was a need, therefore, to formalise these arrangements and enable the institution to address the risks effectively.

### **Options and solutions**

The head of security met with members of the senior management team (SMT) to discuss his concerns and suggest a way forward. However, at the conclusion of the meeting, the head of security felt that although the SMT was largely supportive, it was committed to other issues. Senior managers had little time to debate some of the security matters raised; and equally, they felt unable to participate more actively in developing the strategy because of a lack of knowledge and/or involvement in the

past. Some felt that the validity and effectiveness of previous security actions taken by the institution ‘spoke for themselves’.

The head of security, in consultation with other senior managers, prepared a draft report for consideration by the SMT group. The final report formed the basis of the institution’s security policy and strategy. The head of security drafted the strategy, again following further consultation within the institution. It was subsequently approved and adopted by the institution. The SMT agreed that the approval and adoption of the strategy would result in the implementation of some specific security initiatives.

Initial actions included the introduction of agreed security initiatives across the institution (based on recommendations by the head of security) and obtaining funding from external agencies where appropriate. All heads of departments were required to ensure that the security strategy was implemented within their own departments. The institution’s risk management group and insurers also approved the strategy, which will be reviewed annually.

The institution’s combined security policy and strategy encompasses the following:

- mission statement – security policy and service aims
- key security objectives – for the next five years
- statements of security management and personal responsibilities for key staff and others (these were closely aligned to those given in the institution’s health and safety policy, to provide an integrated approach to personal safety and the assessment of all threats and risks)
- implementation arrangements for the security policy and strategy
- resources to be allocated
- staff training/advice – for security staff and others
- links between security services and other services within the institution and key players
- service level standards/agreements for in-house and contracted services
- review arrangements for the security policy and strategy – timing and mechanisms.

Annexed documents cover the following:

- assessment of security threats and risks (as part of an overall risk management approach/procedures adopted by the institution)
- buildings protection
- student residences – on campus and with private landlords
- access arrangements on campus for taxis, maintenance contractors, deliveries, and so on
- personal property – staff and security
- implementation of specific security measures and initiatives, for example, security and customer surveys, ID cards, alarms, lighting, and keys and locks

- organisational arrangements
- codes of practice for security staff
- contracted security arrangements
- implementation of initiatives in response to issues such as: out of hours working, car park security, advice and liaison with students and staff regarding personal safety and crime awareness, security costs borne by academic and administrative departments as part of devolved budgets
- the HEI's financial regulations and procedures.

The policy would support the overall duty of care to students and staff. The security procedures would enable security staff to take appropriate action in undertaking this duty.

### **Self-assessment questions**

1. How does the institution define 'open campus access'? What are the restrictions? Are these effective/required?
2. What arrangements are in place regarding the protection of property belonging to the institution, its staff and students? Are there defined levels of cover to be provided?
3. How does the institution map out/project its future requirements for security provision?
4. What does the institution regard as the skills required by the head of security? These can include career background, role in context of the institution, implementation of policy and security strategy.
5. How does the institution ensure that security concerns are raised and addressed at the highest level?
6. Does the institution have a personal safety policy and security strategy? Are these linked to health and safety and integrated within risk management arrangements?
7. Has the institution defined its objectives and aims regarding security?
8. How does the institution ensure that existing and future security measures are not ad hoc/piecemeal?
9. What arrangements does the institution have to evaluate different security options?
10. Do the institution's risk management arrangements include security risks? How are these prioritised?
11. Is the head of security a member of the institution's risk management group/insurance panel/major emergencies group?

12. Does the head of security have access to a senior manager who has executive responsibility for security?
13. How does the institution ensure that the head of security:
  - a. Has access to budgets?
  - b. Is advised of insurance losses?
  - c. Publishes security management statistics?
14. Are the institution's security measures subject to regular reviews? Are results retained? How is the strategy updated following such a review?
15. How is the draft strategy considered to ensure relevancy and effectiveness? Does it have the support of the SMT?
16. Is the policy integrated with health and safety plans and other strategic documents?
17. Does the strategy have a forward vision for security initiatives?

## **Case study 3: Training for security staff**

**The head of security had a number of management concerns regarding the delivery of a professional security service. They included a persistent level of absenteeism among some security staff; inflexibility within shift working and cover arrangements for holidays and training; an anti-training culture among some of the older security staff; and problems attracting suitable staff.**

### **Issues and considerations**

Within the last three years, a merger with a smaller HEI had taken place. There had been some changes in the management team. For example, a new head of personnel had been appointed. The head of security had been in post for a number of years and had some good staff. But there were also concerns about some of the staff, who had been there much longer. The head of security felt isolated and had received little support from the senior management team. It was for this reason that some of his concerns had not been addressed earlier.

The head of personnel and the head of security identified the following joint concerns:

- persistent absenteeism among some security staff
- inflexibility within shift working/cover for holidays and training
- anti-training culture among some older security staff
- difficulty in attracting new, suitable security staff (in part linked to local employment conditions)
- increasing responsibilities for security staff linked to legislation
- poor working relations within the existing mixed in-house and contracted security provision.

They agreed that some issues could be resolved by identifying appropriate training for each member of the security staff.

The head of security welcomed the changes proposed, but there remained two major concerns. One was that some security staff might not accept the changes, whereas others had a genuine desire to offer a better level of service. The head of security also recognised that some academic and administrative staff would continue to regard security staff – at least in the short term – as being solely concerned with ‘locks and bolts’.

The other concern was the merger with another institution, where an externally provided security contract was in place. The head of security wanted all security staff to become more flexible and to accept changes in shift working, to cover leave of absence, training and special duties required at different locations, as necessary. However, in-house staff resented the presence of the contract security staff.

### **Options and solutions**

The institution had a training programme for its security staff. However, the training did not cover the matters identified by the head of personnel and head of security. Continuing reductions in the budget were a constant frustration to the head of security, who was also under pressure to introduce service

level statements; and there were not enough security officers to provide cover for those undergoing training.

The institution therefore reviewed the pay scales of its security staff and provided a clearer career structure to attract new staff and to aid retention. All new security staff are appointed on a six-month probationary period, during which they are supervised and required to record the training received and the duties undertaken. The shift system was also reviewed in discussion with staff unions. Arrangements are being considered whereby shift teams could be rotated/mixed. Some training events will be held to break down 'them and us' cultures.

Shift supervisors have been appointed and received training in coaching and overseeing security staff. After each period of absence, the security officer concerned is interviewed either by the head of security and/or a shift supervisor. The head of personnel may also be involved in such meetings, when appropriate.

The institution also reviewed its training arrangements for all security staff and introduced a four-day induction programme, devised by the head of security. The time was allocated equally between a session on 'this is the university', covering the campus and local environment; and another on 'this is security', covering professional issues. All security officers receive guidance on their responsibilities under criminal law (covering issues such as lawful and unlawful arrest, and civil actions against the institution). The institution introduced as part of its structured training programme records of 'how a security officer is performing'. The latter is an on-going process, linked to an annual appraisal scheme.

A security operations manual has been introduced, which documents the arrangements involving security staff, for example managing major emergencies. As such it outlines the roles and responsibilities of security staff and the standards to which these are to be performed.

The training arrangements sought to develop the institution's in-house expertise in delivering the training. Security staff are able to attend training events covering, for example, dealing with aggression, stress management, and report writing. They are also offered courses provided by the Security Industry Training Organisation (SITO), and security officers are encouraged to support regional events run by the Association of University Chief Security Officers (AUCSO).

The institution also decided that it was important that the training offered covered not only security-related training, but also general career/management development. The head of security, for example, wanted to update his awareness of British Standards, quality management and Investors in People. In the mid- to longer-term the institution is considering Investors in People and other benchmarks, such as National Standard Training, ISO9000 and Chartermark.

### **Self-assessment questions**

1. How does the institution ensure that security incidents are reported, addressed and considered at the highest level of management?
2. Has the institution reviewed the line management responsibility for security?

3. Does this include a review of the head of security's role and responsibilities?
4. Has the institution reviewed its training arrangements for security staff?
5. Does the institution have a training policy and programme for security staff?
6. How are the training policy and programme applied to internal and externally delivered courses?
7. Do the training policy and programme cover all security staff?
8. Do new security staff, whether in-house or external, receive induction training?
9. Are training objectives and outcomes agreed with each security member of staff in advance of training received?
10. Do the training arrangements include security-specific and more general personal development/management elements?
11. Do the training arrangements cover the following:
  - a. Service improvement.
  - b. Customer care.
  - c. Legislation.
  - d. Risk assessment of security-related incidents.
  - e. Health and safety, fire, first aid and other emergency responsibilities.
  - f. Management information and data collection and dissemination.
  - g. Budgets and tactical plans – setting and reporting.
  - h. Staff training, management and supervision.
  - i. Team building.
  - j. Sickness, leave management and reporting.
  - k. Community liaison.
  - l. Strategic plans.
  - m. Staff recruitment and retention.
12. Are the training arrangements for security staff included in the institution's security strategy?
13. Are security staff members of AUCSO? Is the institution a member of AUCSO?
14. Do security staff attend AUCSO events?

## **Case study 4: Balancing technology and other security measures**

**The institution did not want to incur excessive expenditure by over-reacting to individual security-related incidents; yet at the same time it wanted to make all students, staff and visitors feel safe and to protect their property.**

### **Issues and considerations**

The institution had previously made some investment in CCTV cameras. Some years ago, it had also installed an auto-dialling system linked back to its main control room. The security services section had recently set up an incident recording system. It wanted to develop a link between the incident reporting system and its records for tape management of CCTV cameras for recording security incidents.

There were a number of operational problems with the institution's existing night security arrangements. These were largely related to recruitment of security staff, the rotation of security staff within shifts, and the provision of cover for staff training and absences. The institution was therefore considering contracting out these arrangements to an external provider.

Next to its main campus was a science, research and business development park, on which the institution had a number of departments. There was no CCTV provision on this site, and the institution was considering extending its CCTV coverage, linked to its main security control room.

Matters of increasing concern to the head of security were that the security staff and the porters carried out two separate security operations, working to diverse patterns, which gave no overlap with the security management during the day. The security staff operated a day and a night shift. At the end of each shift, there were no arrangements to pass on information to the next shift, nor to the security supervisors and head of security.

In addition, some communication equipment was outdated. Radio systems were on different network frequencies and staff could not speak to each other. Alarm systems, both intruder and fire, were not integrated; different suppliers had installed a variety of systems over the years. Security staff had a casual attitude to responding to alarm incidents because of the age and unreliability of the existing equipment, resulting in frequent call-outs and high maintenance charges.

Elsewhere on campus there were computer clusters, available to students outside normal lecturing/teaching hours. Facilities such as libraries required much better access control systems. Within these areas, the institution had also installed a significant number of computer terminals. In addition, the institution conducted research under licence by the Home Office.

Security, safety and health policy issues were debated by several committees within the institution. Although the campus safety committee and the safety policy committee received regular reports on incidents, recommendations to amend security provision were not always linked to security trends and an assessment of risks.

## Options and solutions

The situation created a number of challenges for the head of security. Further investment in security technology, such as CCTV, could be expensive to install; decisions would have to be made regarding its operation and the monitoring of the tape output; some retraining of staff to use the new equipment would also be needed.

As another option, additional security staff could be recruited to provide a more flexible response to any security incidents. On campus, staff could quickly attend to most incidents. However, off-campus security (which included the development park and some other buildings) was dealt with by other service providers that were not managed by the institution. Confidential, commercial research was also undertaken off-campus.

Some years ago, the institution had established a risk management group. In addition to a pro vice-chancellor and the head of security, this included representatives drawn from across the institution. The initial actions identified by this group combined a review of its existing security arrangements with an assessment of risk. An assessment was undertaken of different levels of security for each building and for the campus as a whole. As part of its risk analysis, the institution identified the main risks, and how to isolate the problems and then assign a priority.

This review and records of past incidents enabled the institution to identify areas of weakness on campus. In determining a cost-effective approach, it looked at a number of scenarios, such as 'what if no capital investment in equipment was made?' and 'what would be the impact on revenue costs following the recruitment of additional staff?' For the development park, it evaluated the technical considerations of installing CCTV cabling that was linked back to its main control room; the maintenance costs of new equipment; and the costs of monitoring the tape and data output of CCTV.

The head of security realised that any solution must ensure that all no-cost or low-cost primary security measures had been identified. The latter included crime awareness material, locks and barriers. The cost of integrated security alarm equipment could be very high, partly because of the need to ensure that all security systems fed back to the main control room. Where processes involved automation, such as auto-dialling, telephone numbers needed to be regularly checked and updated.

To assist the future assessment of risk, the head of security prepared a schedule of appropriate security measures and where these should be installed. This was important to avoid a proliferation of alarms, locks and barriers. The following measures were considered: door and window locks; bar shutters and grilles; locks, chains and barriers; access control, ID cards and intruder alarms; adequate lighting; landscaping; and so on.

The programme for the installation of CCTV will need to be updated and adjusted where necessary, in the context of the full range of security measures proposed. The CCTV system will not be fully monitored by security staff. Initially, only the 'key and trouble spot' areas will be monitored during the day, with different areas monitored at night, based on the results of the security survey and the history of reported incidents. These arrangements are subject to periodic review, to maximise cost-effectiveness. Improvements in data management were also introduced in the light of recent Data

Protection Act requirements. Appropriate training for security staff regarding CCTV data management and other legislation were identified.

The head of security introduced incident reporting logs for each shift, and shift patterns were overlapped to allow incidents to be drawn to the attention of the incoming staff. Every morning, the shift supervisor discussed with the head of security any incidents recorded in the logs.

The security duties of porters were reassigned to the security staff. However, general campus crime awareness and liaison duties were identified for porters and all staff, to support the actions of the security staff.

The committee and management structure was reviewed in the light of the statement of responsibility (contained in the institution's security policy). The senior pro vice-chancellor was given executive responsibilities for the institution's security arrangements. He is also a member of the institution's risk management group, so all security risks impacting on the institution's business arrangements can be co-ordinated with other risks identified by the group.

Other elements within its security policy, to support the statements of responsibility and the implementation and operation of its security arrangements, covered the following people: director of support services, the head of security, heads of department, staff and students.

The institution now has a purpose-built security control centre, housing the most up-to-date security technology (which also covers fire and intruder alarm systems and CCTV). The CCTV cameras are controlled from the dedicated control room.

The institution's security personnel perform a wide range of duties over each 24-hour period, 365 days per year. A continuous shift system for security officers provides very visible campus patrols; receptionists are located in some buildings, with porters in others. In these buildings, badges were introduced to control access by visitors. Visible enthusiasm from all security staff, along with more helpful attitudes, has produced much higher satisfaction from the local community.

There is a procedural manual for security operations, and modern security systems are in place to deal with all reported matters, including major emergencies. The security staff turnover has been reduced; staff have job security which is pensionable, and there are opportunities for further promotion and training. The perception now is that the average yearly crime rate is reducing.

### **Self-assessment questions**

1. Does the institution have a security strategy?
2. Does the institution have a risk management group? Is the head of security a member?
3. Does the head of security undertake periodic reviews of security risks?
4. What arrangements are in place for risk assessment and are documents retained for future reviews?

5. Does the institution have a computerised security incident log/reporting system?
6. Are incident logs kept and reviewed by the head of security?
7. What management data are reported to the SMT regarding security?
8. Is induction training undertaken for contracted security staff?
9. Has the institution introduced a security procedures manual?
10. Has the institution identified appropriate security-related duties for porters, caretakers, and cleaners?
11. Are contracts for security staff subject to review?
12. What arrangements does the institution have for the investment appraisal of security initiatives?
13. Do these include repair and replacement decisions concerning security equipment?
14. Has the institution identified and implemented no-cost and low-cost security measures?
15. Does it periodically review its CCTV monitoring policy?
16. Are checks undertaken periodically regarding compliance with the Data Protection Act 1998?
17. Are notices displayed on the campus regarding CCTV cover?
18. What back-up arrangements does it have for CCTV tapes?
19. How often does the institution replace CCTV tapes?

## **Case study 5: Evaluating in-house and contracted-out security provision**

**The institution has had its own in-house security services for some years. It recognised the need to review its support services from time to time, as part of wanting to continually improve. Both academic activities and support services were subject to such reviews.**

### **Issues and considerations**

Within the last year, there had been a merger with a smaller FE institution, located outside the city centre. As a result, there was a need to rationalise the security service arrangements and to consider reassigning some of the duties undertaken by security staff, such as mail delivery.

The institution reviewed its academic activities and support services from time to time. The review panels comprised representatives from across the institution. An external assessor, from a similarly sized HEI, was also part of the panel. The reviews undertaken were structured, and in the past had identified a number of opportunities to improve the contribution made by its support services.

The institution had first reviewed its security services five years previously. Since then, a new head of security had been appointed. As part of the second review, the head of security summarised the existing in-house security arrangements as follows.

#### Strengths/merits:

- part of the institution
- predominantly loyal staff
- flexible in adapting to the demands of the institution
- supported the strategic plan and objectives
- good training arrangements for its security staff
- security staff were good at dealing with students and staff
- security staff knew the institution's campus intimately, which was an advantage in responding to incidents
- security staff had a pastoral role in handling student-related problems.

#### Concerns/difficulties:

- both revenue and capital costs have risen steadily, and in some years sharply, in meeting security service needs (for example in responding to changes in legislation and technology, and following a review of pay and pensions)
- a number of security staff were increasingly subject to long-term sickness, self-certificated sickness and other periods of 'time off', often preceding/following annual leave and changes in shift working rotas.

## **Options and solutions**

The options identified by the review were as follows:

- retain in-house staff, and approach local police authorities to appoint trained police officers as university 'bobbies' (both non-funded and funded arrangements)
- supplement in part the in-house security arrangements with contracted arrangements
- contract out completely the security services to an external provider
- establish a wholly owned, subsidiary company of the institution for its security services, including extra resources for staffing and equipment.

The options were evaluated by the head of security, who reported to members of the institution's senior management team.

### **Retain in-house staff**

The following strengths and concerns were identified.

#### Strengths/merits:

- commitment, motivation and morale of the security staff
- a sense of ownership of the institution
- technical understanding of security equipment
- interaction with the emergency services (mutual trust with the local police)
- increasing efficiency of staff using technology.

#### Concerns/difficulties:

- problems when in-house staff were asked to work with contracted security staff.

### **Part or wholly contracted arrangements**

#### Strengths/merits:

- supply of personnel
- supervisor supervising a contract, not people
- makes sure company doing what it should do
- reports back to the company, problems sorted out (usually)
- pensions, sick pay, training, equipment and other costs borne by the provider.

#### Concerns/difficulties:

- okay at first until .....
- staff turnover, among management as well as on the ground
- good service depends on a good manager
- buying the service at a cost
- contract includes VAT, but no pension or sick pay

- expensive, due to VAT costs and the Transfer of Undertakings (Protection of Employment) Regulations –TUPE
- in-house staff taken on but probably laid off after a year and replaced by poorer quality and lower paid staff
- gut feeling that standards would drop in line with the reduction in staff
- limited commitment, motivation and morale of the security staff
- no understanding of the institution’s overall plans and strategy.

### **Establishment of a subsidiary company**

#### Strengths/merits:

- retains existing key security staff
- opportunity to develop stronger security management skills
- generation of external income from local schools/colleges and other organisations
- VAT savings
- staff employed by the subsidiary understand the management culture and ethos of the institution (however, there was some consideration as to whether it was appropriate for the institution to generate income by offering security services to external bodies).

#### Concerns/difficulties:

- incorporation issues and costs
- accountability and legislative requirements
- future changes in taxation.

Following the review, the institution decided to retain its in-house staff for the city-centre based campus, but contract out its security arrangements for a satellite campus (the former small FE institution).

The option of establishing a subsidiary company to deal with all its security arrangements was initially considered attractive, but the institution decided that some costs regarding setting up the company, transferring staff (TUPE), and VAT considerations could not be determined clearly enough to proceed further. It decided to review these arrangements in four years’ time.

### **Self-assessment questions**

#### **Strategic**

1. Has the institution identified the strategic, tactical and operational requirements for its security services?
2. How does the institution ensure that its security services support its corporate strategic plan?
3. What arrangements does the institution have for security services as part of its procurement strategy?

## **Tactical**

4. Has the institution identified the stakeholders for its security services and the arrangements for determining their service needs?
5. Does the institution have arrangements to determine how its security services – both internal and external – are to be provided? These may be part of its arrangements for facilities management.
6. Does the institution have explicit procurement procedures for its security services and supplies, whether provided internally or externally?
7. Are security services subject to service level agreements or statements, and do service plans indicate the required strategic, tactical and operational objectives?
8. Has the institution established service standards for internal and external providers of security services?
9. Does the institution have up-to-date specifications for security services, whether provided internally or externally?
10. Does the institution undertake periodic reviews of its security service arrangements, both internal and external, involving one or more of the following processes:
  - market testing (formal and soft)?
  - departmental (faculty/school) reviews?
  - stakeholder service reviews?
  - contract reviews with service providers?

## **Operational**

11. Does the institution formally consult stakeholders on their current and future security service needs?
12. Does the institution consider the following issues for security services, whether provided internally or externally (both individually and on a group basis):
  - provision/availability of closely-related services?
  - existing/potential areas of overlap in security services provision?
  - co-ordination with other support services?
  - evaluation of stakeholders' perceptions of value for money regarding its security services (which may be as part of its facilities management arrangements)?
13. Has the institution appointed a dedicated security manager? If other arrangements apply, what are they, and does the manager responsible have the appropriate professional skills and time to act effectively in managing the security services?
14. Are some management responsibilities for security delegated to other service providers? How are the overall arrangements for security services co-ordinated?

15. What actions have been taken by security staff regarding liaison with customer departments, the dissemination of management information, and so on?
16. Has the institution formed partnerships and co-operative relationships with its security service providers?
17. Does the institution review service level standards/agreements with its security service providers and stakeholders?
18. How often are the security contract terms and costs reviewed?
19. Who provides advice to the institution on purchasing and contracting matters for security services and supplies?

# Cameos

Cameos provided by individual HEIs are given in the following sections, which relate to the 10 main elements of the *Security toolchest*.

## 2.1 Security environment

- Security by design
- Access smart cards
- Traffic management

## 2.2 Legislation, quality and standards

- Compliance with legislation

## 2.3 Insurance, assessment and management of security risks

- Management plans for major emergencies
- Reducing false fire alarms

## 2.4 Security strategy

- Reviewing the security strategy
- Policies and procedures put into practice
- Management responsibility for security services
- Total reorganisation – introduction of dedicated security staff

## 2.5 Security management structures and links with other services

- Security audits
- Incident management
- Combined security and postal services
- Rotation of security staff roles
- Liaison with other departments

## 2.6 Raising awareness of crime, and crime prevention

- Establishing communication and partnership
- Links with the local police
- Rapport with local communities and local councils
- Multi-agency approach
- Emergency response teams
- Campus watch schemes
- Local early warning systems
- Student security groups – students and staff
- Emergency telephone numbers
- Crime prevention publications
- Personal safety
- Student surveys
- Security services web pages

2.7 Procurement

Combined in-house and contracted security services  
In-house security staff  
Community safety partnerships  
Funded police officers  
Relations with policy

2.8 Staff training and development

Induction training and personal development courses  
Investing in continuing professional development  
Dedicated in-house programme  
Comprehensive training and development programme  
Instruction manual for security staff

2.9 Balancing technology with other security measures and resources

Linked CCTV and card access systems  
Individual intruder alarms linked by auto-dialling to control room  
Personal safety and security measures  
Window grilles and alarm contacts on doors  
Campus patrols – security duties for non-dedicated security staff  
Monitoring security patrols  
Manned and dog patrols  
Use of security vehicles  
Operational procedures manual

2.10 Funding and service performance

Monitoring crime statistics to target resources  
Allowing 10 per cent of property value to provide effective security measures  
Devolving security budgets to the head of security  
Income generation: extending security services to local businesses

## **2.1 Security environment**

### **Security by design**

At a number of institutions, there is close consultation between security services and the estates department, regarding the security implications for major refurbishments and the provision of built-in (security by design) facilities in new buildings. This can avoid costly changes at a later date.

One institution believes that its approach to security by design is unique. It employs fully qualified architectural liaison, crime reduction and specialist IT personnel within its estates department. This saves consultancy costs, as well as police time. It also ensures that a consistent approach is adopted within the institution for all security issues. The crime prevention and architectural liaison officer is Home Office trained; the crime reduction officer has police and local government community safety experience; and the dedicated IT specialist is responsible for the extensive and complex access control systems and for other technical support staff.

Benefits of this approach include a rapid internal response to technical questions from engineers and maintenance staff; a streamlined approach to crime reduction initiatives, such as the installation of CCTV and alarms; and the early consideration and implementation of 'security by design' solutions in all new-build projects. The security staff provide an advisory service for all heads of department, who are financially responsible for security within their buildings. They are respected by other staff because they provide credible, professional and timely advice, based upon qualifications and experience.

Advice can be obtained from the police, but often there is a delay, which can increase the costs of a project. Some institutions use consultants, for example for CCTV, but they will need to understand the institution's detailed requirements so this too can be costly.

At another institution, the security staff are always consulted during the initial stages of developing the institution's estate. The consultation also involves the local police architectural liaison officer. This approach ensures that the institution's security service is aware of, and is able to contribute effectively to, the strategic planning of the institution's estate, by serving to 'design out crime'.

### **Access smart cards**

One institution has a university card system (an integrated ID, library, registration and access card), which provides better control of access to campus buildings.

### **Traffic management**

At one institution parking permits are issued with a unique number to each student, staff member and visitor as required. This allows the security staff to quickly identify vehicles in the institution's car parks whose owners are not 'on university business'.

At another institution, following extensive market testing and consultation with staff, the institution awarded a five-year contract to an external contractor to provide security and car parking management

services, under the direction of the estates department. The contract took over the roles and responsibilities of six in-house staff (who were re-deployed elsewhere within the institution), and the contract night time and weekend security officers. The contract included the provision of capital equipment (parking barriers and control mechanisms) and a car parking administration system (permits and so on). More importantly, it allowed for staffing at double the pre-contract levels.

The award of the contract coincided with the introduction of charges for parking at the institution. The initial cost for staff and students was extremely modest – 50p per day, £5 per month (deducted from salary) or £50 per year. A business plan was developed which, if delivered, would result in the contract being self-financing over the five-year term (it has already exceeded expectations for year one). After the first full year of the contract, the following benefits are evident:

- increased manpower, providing better and more visible security
- increased control over car parking, providing a safer environment for the ‘university community’
- improved ‘customer care’ facilities, including a security escort service for women, a ‘get-you-home’ service for all staff and students, and a flat battery starter service
- reduced car crime. The institution has traditionally suffered a relatively low level of car crime, particularly since the introduction of CCTV in 1995. The level of car crime in the first year of the contract has been reduced to nil
- a self-financing contract.

One institution, realising that it sends several thousand students each year into the local community, felt that it had some responsibility to ease some of the problems entailed. The main concern was students parking their vehicles on the surrounding streets, thereby denying parking space to local residents. The institution’s regulations tell students that they must not park in the surrounding streets. The institution wrote to the residents and issued identity tags so the security staff could identify the residents’ vehicles. They then placed notices on all other cars, which were mainly owned by students. This strategy not only reduced the number of students parking their vehicles on the streets, but also improved relations with the neighbours. All these initiatives had the support of the student union.

## **2.2 Legislation, quality and standards**

### **Compliance with legislation**

One institution recognised that legislation concerning the work of security must be fully complied with, and all departments that can advise on current legislation should be consulted as soon as possible. The institution has identified the relevant legislation and is considering the cost implications. This includes the Private Security Industry Act 2001, which may affect the way ‘in-house’ security is managed, not least for car parking and clamping; the Data Protection Act 1998; the EU Directive 2000, concerning the use of CCTV; the Human Rights Act 1998; and the EU Working Time Directive 2000.

## **2.3 Insurance, assessment and management of security risks**

### **Management plans for major emergencies**

At one institution, a major emergencies plan has been implemented. It is supported by a procedural manual for all reported matters, including major emergencies, and has been published and circulated within the institution. Both the plan and the manual have the approval of the regional emergencies co-ordination committee, and they were successfully 'tested' in a table exercise two years ago.

### **Reducing false fire alarms**

One institution recently joined the local fire services in an awareness campaign to reduce the number of false fire alarms. This initiative is introduced at the start of each academic session when the institution feels it will be most effective. The institution works closely with the local fire services and for many years has had a system whereby it meets the emergency services at the campus site entrance whenever an alarm has been raised, so that they reach the right place with the minimal amount of delay.

## **2.4 Security strategy**

### **Reviewing the security strategy**

At one institution, the security policy statement and procedures cover every aspect of its security service provision: crime prevention, access control, asset protection, and personal safety and security. Both the policy and the procedures are regularly reviewed and amended as circumstances change, to take account of crime trends and the expansion of the institution. The institution feels that it is essential for the policy and procedures to be communicated widely, through printed copies and electronically.

Another institution supports continuous improvement by ensuring that the institution's internal auditors audit all areas of security at least once every three years.

### **Policies and procedures put into practice**

Security operations at one institution are governed by an operational procedures manual. Systems are in place to deal with all reported security matters, including major emergencies. The institution's security policies and procedures are well communicated.

### **Management responsibility for security services**

At one institution, the head of security is part of a management structure for resources. The resources division consists of finance, estates, personnel, residential services, trading activities including conferences, strategic purchasing and project management. The heads of each department form the resources management team, which meets twice monthly. This structure allows security concerns to be addressed regularly; and related departments – such as estates and residential services – to be considered together. The resources division is led by a director, who is a member of the vice-

chancellor's management group. Alternate meetings of the resources team are agenda driven, so that there is the opportunity to table contentious issues with supporting papers. The head of security has a positive view of this structure, not least because a number of the key players in the institution are aware of his problems and can discuss them to achieve mutual understanding.

### **Total reorganisation - introduction of dedicated security staff**

In 1998, one institution decided to create a completely new, professional security operation, capable of providing the 24-hour, 7-day cover, which the growing university community was coming to demand. The institution is city-centred, with academic buildings and student residences all within a mile (or so) of each other. The installation of CCTV in the city-centre was causing a 'crime ripple', by pushing crime out, so that the institution became the target of criminal activity. The university community (approximately 20,000 students, staff and visitors) required a higher level of personal safety.

At that time the institution was served by about 60 porters, whose duties meant that they could not be responsible for 'door-keeping' while they were delivering goods internally. Their basic salaries were the lowest in the organisation, and overtime had become essential in order to create a reasonable standard of living, but overtime was balanced by high levels of sickness absence. There were also two separate security operations involving 30 staff in total. These worked on diverse patterns, which gave no overlap with managers during the day. They had radio systems that could not speak to each other, and their attitude to responding to alarms was based on the belief that most were false, and the wiring was probably at fault. The institution was also clear that much better access control systems were needed to reduce the incidence of its libraries being used as refuges for the bewildered.

Today, the institution has a continuous shift-based, security operation of 64 staff, who provide very visible campus patrols. This operation includes receptionists located in some buildings, porters in others; and a CCTV networked system of approximately 60 cameras controlled from a suite where the wiring does actually work. There is also a visible enthusiasm from all, a helpful attitude, and much higher satisfaction from the community. Even the neighbours can ring a hotline to complain of noisy students. Liaison with the police involves joint walkabout patrols of the streets, and in most months security staff assist in a handful of detentions or arrests.

Crucially, the operation is managed and supervised by professional security staff. Salary levels are all higher than the national basic; turnover of security staff is minimal; and the security patrol officers are recognised for their 'pastoral' role, especially on the residential sites in the early hours of the morning when they are busier than at mid-day. The transformation costs were significant, in that voluntary severance was accepted by numbers of porters who did not want to join the new operation. The 'capital' costs were imminent anyway, and the running costs, thanks to the elimination of overtime, are justified by the enhancement to the service.

Another institution started with a garden hut and a handful of men some 25 years ago. It now has two purpose-built security control centres, housing the most up-to-date security technology (fire and intruder alarm systems and CCTV). It also has 48 security personnel, performing duties over each 24-hour period (shift rotation system), 365 days per year. It has an average yearly crime rate of

approximately 150 incidents, of which about 100 involve petty theft. Crime does not disrupt the education or research activities at the institution.

## **2.5 Security management structures and links with other services**

### **Security audits**

At one institution, the head of security offers an inspection service to departments so that potential problems can be explored and solutions proposed. A form has been developed to capture key information about systems and procedures relating to cash collection and storage, key issue and recovery, locking and unlocking procedures, awareness of risks, and personal safety. This information forms the basis for discussion and advice on procedures and improvements. The process does not seek to supplant the responsibility of each head of department for security issues within their area, but rather to 'head off' trouble while recognising that the department also has to function effectively. Absolute security within an institution is rarely possible, but acknowledging this fact does not mean that there are no gains to be made. This approach also prevents ad-hoc solutions being developed across the site, and ensures a consistent approach. It also establishes a bridge between security services and other staff.

### **Incident management**

Many and varied incidents may occur within the boundaries of a large institution, and it would not be feasible to involve the police in all of them. Because of this, one institution provides its own patrol and response service, reflecting the community warden approach favoured by government. The local police are only contacted in the event of serious offences. This does not replace the police officers on the campus, rather it encourages them. Patrolling in the knowledge that there is a direct link between the police radios and the security control room improves confidence and working relationships on both sides. Other benefits include a better exchange of information and a partnership approach to crime and disorder.

### **Combined security and postal services**

At one institution the postal and security services have been combined. Postal and security staff have the same uniforms, so that during normal working hours additional support in extraordinary circumstances is available from the post room. Furthermore, delivering the post in and around campus buildings also becomes a security patrol: sometimes the sight of a uniform is sufficient to deter any would-be criminal.

### **Rotation of security staff roles**

Security staff in one institution change roles throughout a shift to keep energy, motivation and morale high. Providing employees with meaningful work, such as investigating a theft or visiting victims, helps improve morale, and reduces absenteeism and staff turnover.

At another institution, total flexibility in managing staff – such as having them change shifts at short notice, change sites and even grades – cuts down on overtime and enables the institution to ensure continuity in service cover, in times of need, but at no extra expense.

### **Liaison with other departments**

One institution found that security principles and procedures were more easily implemented by regularly communicating with line managers and staff.

At another institution, the security services involve and consult with the health and safety officer on all issues where there are areas of common interest.

## **2.6 Raising awareness of crime, and crime prevention**

### **Establishing communication and partnerships**

One institution places strong emphasis on working positively with local partnerships, such as the local coalition on crime committee which provides information on current crime trends and crime prevention seminars. In addition, the institution is a member of the local crime prevention panel. Panel members represent local retailers, hospitals and so on, and work with the police to promote a safe and secure environment. The flow of information between members promotes greater awareness of current criminal activity; the panel is also a platform for local initiatives to combat crime.

### **Links with the local police**

At one institution, a web page is used to provide information on crime prevention from the institution and the police, and a channel for the police to ask for information on crimes. The number of hits on the site is monitored, to show whether or not information is reaching a wide audience.

### **Rapport with local communities and local councils**

One institution has established links with the local community, local councillors and council officers to represent staff and students with regard to improving security and personal safety in the local area. Several established forums exist to discuss inner-city regeneration, transport, crime and personal safety. Attendees at these meetings include police, the British Transport Police, Rail Track and local authority traffic and transport advisers. The institution also places strong emphasis on working positively with local traders, and is a partner on the local coalition on crime committee.

### **Multi-agency approach**

Another institution has adopted a multi-agency approach based on a security strategy. It produced a report describing the approach, and a full review of its activities over the year is given in the estates annual report.

## **Emergency response teams**

Several years ago, one institution realised that the response from emergency services was becoming more erratic, owing to their increasing workloads and reduced resources. Consequently, criminals felt that they had ample time to commit offences and stroll away. Furthermore, keeping the peace with limited police support was becoming more difficult; and the sensitive smoke detection systems required by law in halls of residence and other buildings were creating more and more false alarms. In addition, the institution needed efficient 24-hour first-aid cover and safety support to allow it to operate both business and social functions outside core hours.

It decided to introduce in-house emergency response teams, capable of performing the initial basic functions of the emergency services. The response team – a minimum of six on-duty security officers – provides the initial response to any incident within the institution. The security officers assess the situation, take what action is necessary, including calling the emergency services if required, and contain the incident until the relevant service(s) arrive. This initiative has been applauded by all the emergency services, as they now know that if they do receive a call for assistance from the institution, it will be of a reasonably serious nature.

The emergency response team is tested by the fire authority. This gives the institution a certain amount of leeway regarding the evacuation of premises. The team investigates all fire alarms before calling the fire service so buildings are no longer evacuated in response to false and malicious alarms.

The emergency response teams have made the institution a safer place and have reduced crime, particularly outside core hours. They have not only filled the gaps left by the under-resourcing of emergency services, they also allow all departments to operate outside core hours knowing that the requirement for first-aiders and safety support is satisfied. Finally, this approach has fostered good relationships with the emergency services, created a more varied and satisfying career for the security staff, and placed a new importance on proper training and the achievement of high professional standards, all of which provide security staff with a greater sense of purpose.

## **Campus watch schemes**

The campus watch scheme at one institution has security staff, student support services, the students' union and police adopting a unified approach. It recognises the value in proclaiming the same crime prevention and personal safety messages. Unusually, the scheme is co-ordinated by the head of security, although some data are also provided by the police. General advice on trends is provided on a monthly basis, as well as being posted on the web-site.

The police support the initiatives by having a campus police officer and by providing free crime prevention and personal safety advice at the start of each academic year. Support from the students' union comes in the form of campaigns and publicity throughout the academic year. Student representatives attend the police talks and contribute to the content. In particular, the 'Swag' campaign – whereby union officers attempt to get into unsecured kitchens – raises awareness each year of 'sneak-in thefts'. Information provided by students as a result of warnings being put out by campus watch is patchy, but on average it amounts to over 100 contacts, with five or six people being apprehended annually. These arrests are directly attributed to the quality of the information flow.

## **Local early warning systems**

At one institution an 'early warning' system was set up with local partners. A student security group had been formed with the police, students' union, campus and residential staff. Regular meetings are held and the group works to everyone's advantage. The institution has a number of CCTV surveillance cameras on campus. In collaboration with the local authority, the scheme was extended to cover the local area, to help reduce crime. As a result of this extended coverage, a partnership was created with neighbouring businesses, the local FE college, the local authority parks department and the police to share information about immediate security problems such as car thieves and vandals. The system uses a 'hotline' telephone to disseminate information, and potential criminals are tracked on CCTV.

## **Student security groups - students and staff**

Involvement and close consultation with the students' union and all student support services ensures a free flow of information at one institution, particularly with regard to personal safety and welfare issues. Security services are very much valued for their 'caring' role when there is no one else left on campus. The student security group was established in 1999 in response to students' and the institution's concerns about security and safety on and off campus.

The group consists of officers from the students' union, estate department managers with a security responsibility, staff from accommodation services and the police. Its aims are to monitor trends (through regular local crime statistics published by the police); address perceptions of crime (from student surveys); and implement measures to reduce crime levels and increase safety awareness. This has been achieved through various means such as:

- police crime prevention advice being available during 'freshers week'
- the publication of leaflets, and the availability of advice at student advice centres
- collaboration between the police and the institution's security officers, and the sharing of intelligence
- the sourcing of funding to install CCTV, improve lighting, and provide window and door locks, property marker pens and so on.

The group meets regularly and provides a useful forum for the exchange of information and ideas between a wide range of organisations that have a direct concern with security.

## **Emergency telephone numbers**

At one institution students and staff did not know who to contact in an emergency, or how to do so. The '888' system was introduced throughout the institution, and is similar in practice to the emergency services '999' system. The 888 telephone line is available to all staff and students (for both internal and external calls). The institution's security service responds to calls by providing a 24-hour, mobile cover (with occasional support provided by two mobile units) for the main campus, satellite campuses and halls of residences.

Little cost was involved in installing a dedicated telephone line in the institution's security control room. The control room staff ensure that all 888 calls are given priority in terms of being answered, and serious incidents are responded to immediately. The system is particularly well received and actively used by students living in the halls of residence. Staff and students are encouraged to use the 888 service in preference to 999, since a more rapid response can be given.

### **Crime prevention publications**

One institution has a useful series of leaflets. One is aimed at staff, students and visitors, and is entitled 'Security: a matter for us all'. It was designed by the institution's security review working party and covers the CCTV code of practice, car park controls and general security advice. This complements a leaflet produced by the student welfare department entitled 'Women alone', which lists the precautions to take when out alone, or baby-sitting, or travelling in a car or by public transport. Both leaflets are issued to new members of staff and all new intakes of students. Another booklet for staff and students gives hints on keeping safe while working alone, walking home in the dark, using public car parks and so on. The institution has also joined forces with the local council and the police to have an accreditation scheme for accommodation owned by private landlords.

### **Personal safety**

An evaluation of practices and procedures concerning personal safety of the campus community is an ongoing programme at one institution. It publishes a safety booklet each year with useful information on reducing the possibility of becoming a victim of a crime. First year students receive a talk on crime prevention from the head of security or the local crime prevention officer. And there is a bus service for students leaving the campus late in the evening.

In addition the institution encourages departments to inform the security service of staff working late within a particular building. This not only gives comfort to the individual member of staff, but also alerts security staff about who is in the building if an emergency arises. The institution has found that installing a personal attack alarm at a person's workstation has substantially reduced people's concerns about their own safety.

### **Student surveys**

Each year one institution, as a student project, carries out a survey of students and local residents (many of whom are students living in privately rented accommodation), to identify their concerns about safety and security on and around the campus. The survey covers the extent to which respondents have been affected by crime, the security of premises, and respondents' fears about crime and their personal safety. The results are posted on the institution's intranet and reported to the student safety group.

## **Security services web pages**

At one institution the security web page contains advice, reports, current initiatives, trends in crime, links to comparable organisations and a summary of the security policy and procedures within the institution.

## **2.7 Procurement**

### **Combined in-house and contracted security services**

One institution has found that 24-hour cover from in-house security staff, plus contract security, works well. The institution supports these arrangements with CCTV cameras. Campus staff are on duty generally between 6.30 am and 11.45 pm each day (Monday to Saturday). In order to provide an immediate response to security incidents, and random patrols, a contract security company is employed to provide a mobile (van-based) and highly visible deterrent, 24 hours a day. This has led to a significant decrease in crime. The same company is able to offer competitive rates (as they also provide static post security staff when the campus staff are not on duty). The arrangement is a working partnership: both the mobile patrol and the static post security staff are managed by the institution.

### **In-house security staff**

One institution provides 24-hour cover, two response vehicles and over 50 patrolmen for its premises, working closely with the local police.

### **Community safety partnerships**

One institution has concluded that it can no longer rely on other local agencies for support and solutions to crime-related problems. It believes that community safety partnerships are to be encouraged, rather than seeing attendance at partnership meetings as onerous. As the second biggest employer and major stakeholder in its area, the institution has become a committed member of its local action group and a partner under the terms of the crime and disorder legislation. It regularly holds local meetings with the police and local authorities, chaired by a member of the security management team.

As well as the marketing benefits, involvement also provides opportunities such as sponsoring institution-based crime reduction initiatives, and consultation with local landlords, neighbourhood watches, local businesses and so on. With the Human Rights Act now referring to functions that benefit local communities as public authorities, the implications for security departments in city-based institutions are clear. Equally, by becoming involved in local action groups, the aims and intentions of the institution are more clearly defined to the community itself.

### **Funded police officers**

One institution has gone to considerable lengths and expense to provide adequate security measures to protect its assets and the community, but still suffers from crime and unwanted intrusions on the

campus and at its halls of residence. For some time the institution and the regional area police commander have been in discussions concerning the local crime rate and how best to meet this growing threat to the institution's community.

Following the successful installation of a funded police officer at a local NHS hospital trust in 1999, the institution entered into a contract with the regional police force to provide an officer dedicated to the institution's premises. The officer is based on the main campus and works closely with the head of security and the team of security patrollers. He carries out the duties on a mixed shift system, bringing to bear the necessary police and local intelligence experience to combat crime in the area.

At another institution, discussions were held with the local police with a view to creating a specialist post for a university (or higher education) liaison officer within the police force. Prior to the appointment of the liaison officer, the police had difficulty in creating a 'focus' for particular problems as they are continually changing their work patterns. A dedicated officer now takes ownership of the institution's crime-related problems. The institution has found it very productive and of great value.

### **Relations with police**

One institution has established close links with the local regional police. The divisional commander, a chief superintendent, is a member of the institution's council and estates committees. The police provide a uniformed officer to oversee policing issues on the campus. He has an office in a prime ground floor reception area, and has full access to the institution's security control room. In addition to numerous day to day informal communications between the police and the institution's security staff, the institution also has a more formal mechanism in the police liaison group.

The group is chaired by a pro vice-chancellor and meets several times a year to discuss security and policing issues. The group consists of police officers; staff who deal with student accommodation, estates and security; plus representatives from the students' union. Relevant items from the police liaison group are reported to the security committee, a sub-committee of the institution's services committee that reports to the institution's council. The management arrangements also ensure continual and up-to-date communications with the police on a formal and informal basis.

## **2.8 Staff training and development**

### **Induction training and personal development courses**

Security staff at HEIs can come from a wide range of backgrounds and some, due to a change in career direction, have no previous security experience. One institution believes that security staff need training in all the areas that they are likely to come into contact with, and this includes all types of crime, first aid, safety issues and fire training, as well as personal development and 'on the job training.' Opportunities for training in the HE sector come in several distinct areas.

The institution has developed a four-day initial training course for all new recruits. It covers administrative issues such as the completion and submission of documents relevant to the security service, radio voice procedure, crime prevention, safety, completion of pocket notebooks and powers of arrest, statement and report writing, and animal rights issues. All the criminal offences likely to be

encountered by officers on campus are covered in detail. At the end of the four days, a multiple-choice test is given to ascertain what each participant has learned. The test also gives the opportunity to go over any ground that appears to have been generally misunderstood.

All aspects of each assignment area are identified and included in a training manual that each recruit carries with them in the initial weeks of service. Both the shift supervisor and a mentor or experienced officer support the recruit during the 'on the job' training phase. During the initial accompanied patrols, the recruit keeps a record in the training manual of all points of each assignment that are covered. The mentor or supervisor then initials this entry to confirm this fact. It is then a simple matter to identify and address any gaps in a recruit's training.

Security officers are encouraged to attend personal development courses run by the university on, for example, assertiveness training and dealing with aggression, as well as training in computer skills. Officers also attend outside training courses on specialised equipment. National vocational qualifications have so far not been used: they often seem to fall below the standard the institution seeks to achieve, and are quite non-specific in some areas. Much more use is being made of the supervisory management courses at Birmingham and Aston Universities, and all supervisors and acting supervisors attend these courses. A recent feature here is that the course has been recognised by NEBS (the awarding body for management qualifications).

### **Investing in continuing professional development**

One university believes that investing each year in progressive training of security staff is essential. Any failure on the part of the security personnel resulting from lack of training may make the institution liable for the consequences of their actions. The standard and type of training vary, although in-house training on health and safety regulations is part of any programme. There is specialist input from outside bodies, such as a recognised national training organisation. Training opportunities are non-discriminatory and, where appropriate, are designed to meet national standards.

At the institution, there are three main types of training undertaken:

- all employees receive general induction training provided by the staff development department
- all new employees are expected to complete a probationary period. During this period they receive probationary training which will involve assimilating and completing certain tasks essential to their employment. Such training is supervised and a written record kept of their performance
- the final element of staff training is continuation training/continuous professional education (CPE) and may involve practical workplace training, internal and external courses. It may be used to enhance existing skills, knowledge and performance; to train staff in using new technology, new practices or procedures; and to ensure compliance with any statutory regulations.

## **Dedicated in-house training**

Recent mergers with other HEIs have meant that one institution has increased considerably in size, gaining several new campuses. As a result the security department has expanded dramatically in numbers of operational staff and in the extent and complexity of its responsibilities. In order to provide a consistent, high quality service in support of the institution's mission, a programme of training for all staff was required.

Commercial packages were investigated, but although they covered general security duties, they were found to be lacking in areas of importance to officers working within an HEI. Furthermore, they were expensive for the numbers of officers involved, reduced the availability of operational staff to unacceptable levels, and were not compatible with employees' shift patterns. The decision was therefore taken to introduce an in-house training team, in the form of a fire training officer, a first-aid training officer and a security training officer, and to adopt the Security Industry Training Organisation (SITO) syllabus, supplemented with material specific to the institution.

The training commences at the start of employment and continues throughout an individual's service. It thus reinforces the knowledge and experience an individual gains on duty and provides a foundation for more advanced training for those seeking promotion or wishing to specialise. The system also allows for staff to train as teams in practical subjects, such as emergency responses, and for practical, one-to-one, on the job training to be undertaken with officers when necessary.

There has been a marked improvement in the professionalism of the security department as a whole, with supervisory grades able to accept more responsibility for the management of their teams and individuals. One-to-one training has also helped those who are slower to learn and overall there has been a great improvement in individual morale, team spirit and effectiveness in dealing with emergency situations. In addition, a reduction in course failures and a general rise in work practice standards have reduced counselling and disciplinary proceedings involving senior management. Overall, the flexibility and professionalism of the security department has improved, with officers receiving nationally recognised qualifications and better job and promotion prospects. The cost has been substantially less than that of outsourcing training and there has been no reduction in the number of officers available for operational duties or shift work.

## **Comprehensive training and development programme**

At one institution all staff, whether in-house or contract, have the opportunity for continued development (lifelong learning). All in-house staff also have an annual appraisal, identifying and exploring personal objectives and development opportunities. Developmental opportunities and objectives are in line with the department objectives, as per the departmental business plans. Both the divisional and personal objectives are specific, measurable, achievable, realistic and time-related (SMART). A training programme, comprising training and development requirements of individuals and the specific training requirements of the security department, is published annually. Each member of staff receives an individual copy.

An effective communication strategy is a requirement for the Investors in People (IiP) award. All departments within the institution are encouraged to achieve this award. To aid communication

throughout the security department, monthly ‘team talks/briefs’ are included as part of a cascade of information, initiated by a ‘core brief’ at the highest level within the institution.

### **Instruction manual for security staff**

A security instruction manual is an important tool for one institution to set out guidelines and strict codes of practice for all its security staff. The manual covers such things as:

- code of conduct
- legal guidelines
- health and safety regulations
- guidelines for dealing with incidents
- contingency planning
- customer care
- CCTV code of practice and guidelines
- intruder alarms and responding to activations.

## **2.9 Balancing technology with other security measures**

### **Linked CCTV and card access systems**

Some years ago, one institution integrated its CCTV system with a card access control system on the main campus to enable the movement of personnel to be monitored. A slave monitor was located in the control room. This enables security staff to check on the movements of patrols, and shows if any of the doors to buildings have been forced, which in turn enables a security response to be made.

More recently a comprehensive external CCTV system was introduced which enables the visual monitoring of people who come onto the main campus. The scheme was paid for with money from car parking charges. The scheme is proving to be highly successful, not only in observing and tracking would-be thieves, but also in monitoring such matters as disorderly behaviour by students, and traffic management. Although some limited concern was initially expressed by staff about the ‘big brother’ approach, by operating to strict guidelines it was quickly recognised that the cameras in fact benefited staff and students by helping to prevent crime and improve personal safety.

### **Individual intruder alarms linked by auto-dialling to control room**

Following a spate of burglaries on the main campus, where computers and similar equipment were being targeted, the security department of one institution, in conjunction with recommendations by the institution’s insurers, installed intruder alarms at various vulnerable locations, including the computer suites. These operated on an auto-dialling system whereby activation is automatically received within the institution’s control room. Security staff can then arrange an immediate response, either by one of the patrolling security officers or by the mobile cover.

The initial cost of installation was of some concern to departments, generally in the region of £1,000 per system. The amount became more realistic and acceptable when broken down to a minimum life span of 10 years, which in real terms worked out at approximately £2 per week. As the system

dispensed with the need to go through the alarm companies' central station, considerable savings on the annual maintenance contract were made, with additional savings achieved by operating on an internal ex-directory telephone line. At the moment the institution has 100 separate systems relating either to a department or to a computer suite. In the light of its success and reliability, the institution is now expanding the scheme by modifying general off-site alarm systems in a similar way.

### **Personal safety and security measures**

At one institution, threats to staff or aggressive behaviour by students or staff sometimes occur. The institution's security staff visit the victim and talk to them, get an account of the incident and briefly report it in an 'occurrence book', with a description of the person accused of doing the threatening. Brief details are put on a white board in the control room (with the room number and internal telephone number of the victim), so that each successive shift is aware of the matter.

The institution always has available in the control room, small hand-held alarms (which emit a loud noise and bright flashes of light when activated). Security staff are encouraged to hand them out freely to anyone in the institution who might feel vulnerable during the evening or any student going home alone. The institution believes that the reassurance given to academics, staff and students is of greater value than the small cost in alarms (£4 each) and security staff time.

### **Window grilles and alarm contacts on doors**

The installation of grilles and other security measures is now a basic security strategy at one institution. Previously the institution had installed few alarms and little physical security for items such as computers. In the first instance passive infra-red detectors were installed with an alarm to the control room if anyone entered illegally. Where this was too expensive, the devices were locked down. The result of this approach was that secured computers were still being stolen, although not as often. In alarmed areas the institution still suffered thefts as many thieves realised that – providing they could get out of campus buildings within 10 minutes or so – there was little chance of anyone being able to respond to the alarm in that time.

The head of security realised that if it was possible to install an alarm that was activated whenever anyone entered a room illegally, and that there was a security device to lock down the property to withstand a 10-minute attack, then the thief would be reluctant to attempt the crime. The institution therefore installed grilles on the inside of windows and alarm contacts on doors. If a window is broken an alarm will activate, but the thief still has to overcome the grille, which is unlikely to be achieved in 10 minutes. Similarly if the thief enters through a door, they have to break a lock on the equipment itself, which takes at least 10 minutes, giving the security staff time to arrive.

### **Campus patrols - security duties for non-dedicated security staff**

The head of security at one institution is responsible for approximately 2,000 car parking spaces and traffic management at the institution. The tasks of security officers and car parking attendants have been merged to create a 'campus patrol'. The campus patrol officers have become multi-skilled: in addition to protecting cars and managing traffic and car parking, they patrol the campus and assist in the locking and security of buildings.

## **Monitoring security patrols**

At one institution a computerised database was installed in March 1998 to record the time and date when security officers check various locations within their patrols. The security officers carry a clocking device that they pass over a clocking station fixed to the building. The officers may decide in which order they patrol, as long as each area is visited. If points are missed, usually as a result of being involved with a crime-related incident or fire alarm, the reason is given in the officer's written report. The data are downloaded from the clocks and can be saved on disk for future reference. The information can also be perused to reveal any areas that may have been missed.

The benefit of this system is that, if there is an incident, the exact time and date that the security officer was present in the area can be established. This helps to pinpoint the time of the crime and demonstrates to the staff and students that the building is being patrolled. Initially it was introduced into one patrol area and evaluated over a four-week period. This proved successful and all patrol areas were then fitted with the clocking points. Clocking points and patrols can be altered if it appears beneficial to do so. Additional key stations are inexpensive and can be fitted within minutes. The system also helps the security officers, as no dispute can arise as to whether they visited a building during their patrol.

## **Manned and dog patrols**

During 1997 one institution was plagued with numerous burglaries and other security incidents (on average one burglary every seven days) at its five outlying halls of residence. These buildings had no on-site security staff and were in high risk crime areas, and the response time from the police was not satisfactory. Not surprisingly, there were many complaints from students and parents. The institution was on the point of inheriting a further three halls of residence through mergers with two other HEIs. These mergers would bring an additional four campuses with limited security cover.

The institution decided that the most cost-effective approach would be to introduce deterrent patrolling and emergency response to all of the poorly protected areas. For this solution to be effective and safe it required a two-officer team to be mobile at all times during the most critical hours. This would have entailed the use of 16 officers on a rotating shift pattern. However, following research into the use of guard dogs, the decision was taken to establish a unit employing eight officers and eight dogs, at a considerable saving.

As a result, burglaries have been reduced from one every seven days to five in three years. The system has proved such a good deterrent that the dog unit is now also used on the main campuses outside normal working hours. This has proved very popular, especially with female staff and students who felt vulnerable after dark before the dog patrols were introduced. The dog unit also heads up the emergency response teams, reacting to intruder alarms and breaches of the peace, and this has, to date, put a stop to violence by suspects, which was becoming a problem. The savings, based on this year's rates are some £163,000, the difference between employing eight officers with eight dogs for £220,000 in place of 16 officers for £383,000.

## **Use of security vehicles**

One institution is shortly to give a trial to an electric powered vehicle, which it hopes will give security staff an advantage in catching car thieves. The scenario is always the same: car thieves see the white security van with university insignia on both sides long before it arrives at the scene, and so stop what they are doing and run away. The institution hopes that the new quieter vehicle, unmarked and coloured green, will help to catch car thieves in the act and so deter car crime on the campus.

As the campus site is so open, the institution has also tried a new tactic in dealing with vehicles suspected of being there for criminal purposes. The security vehicle is parked at a central point to monitor arrivals. Visitors are then immediately challenged. Previously the security vehicle was kept on the move all night in the hope that this would act as a deterrent. As the institution has several car parks it was found to be ineffective.

This summer some of the institution's security staff on mountain bikes have been successful in keeping young cycle thieves off the campus, by intercepting them before they find a target. Previously the pedestrian areas were patrolled on foot, and the cyclists were able to make off before security staff arrived at the scene. The institution plans to expand the scheme over the next 12 months and especially during the next school summer holidays.

## **Operational procedures manual**

At several institutions, the security operations are governed by an operational procedures manual, and systems are in place to deal with all reported matters including major emergencies.

## **2.10 Funding and service performance**

### **Monitoring crime statistics to target resources**

One institution has found that monitoring crime through statistical analysis is an important part of the strategy to reduce crime and target its security resources. The security department already had a computerised system for crime management and crime pattern analysis. This had been updated over the years to take account of the size and layout of the campus. A continuing requirement was that it was capable of monitoring and analysing all crimes and incidents reported on campus. The institution consulted with the local police, to establish the data that should be recorded. It believes that the unique nature of each HEI means that the crime analysis needs to be tailored in order to:

- identify areas of concern
- raise the level of awareness and understanding of crime-related problems on the campus
- help develop appropriate actions in response to areas of concern.

As part of its overall crime reduction strategy, there is annual investment in security technology and projects to reduce crime and the fear of crime on campus.

### **Allowing 10 per cent of property value to provide effective security measures**

The head of security at one institution has identified that security measures amounting to 10 per cent of the value will secure any vulnerable item. So if the item is worth £500, £50 will buy a good security device; if it is valued at £6,000 then around £600 needs to be spent to provide good security. The head of security now tries to get schools and departments to build in 10 per cent for security costs. Where this advice has been followed, the institution has lost next to nothing.

### **Devolving security budgets to head of security**

At one institution the head of security is responsible for all security-related issues. The institution believes that reporting to the highest level is essential to ensure that crime and its effect on the organisation are given proper consideration. This also guarantees that decisions on high levels of funding are made without the requirement for protracted discussions. Wherever possible, control of budgets is devolved to the head of security – including the staffing budget, day to day operational costs, and an element for immediate expenditure – without recourse to higher authority.

### **Income generation: extending security services to local businesses**

One institution is offering security services to local organisations – including alarm monitoring, key holding, and security patrols – as part of a proactive approach to crime prevention. Staff and students are given crime prevention advice at every opportunity, particularly during induction periods, and are reminded of their responsibilities for security. This is done through presentations, security web pages, and the publication of reports on current initiatives and trends in crime. Close links with the local police and crime reduction agencies are encouraged, and the institution works in partnership to support crime prevention initiatives. Through such links, it is also possible to develop further business opportunities and potential income generation.

## List of abbreviations

AUCSO	Association of University Chief Security Officers
BSIA	British Security Industry Association
CCTV	Closed circuit television
CIBSE	Chartered Institution of Building Services Engineers
CPE	Continuous professional education
FE	Further education
FEC	Further education college
HE	Higher education
HEFCE	Higher Education Funding Council for England
HEI	Higher education institution
ID	Identity
IT	Information technology
JPPSG	Joint Procurement Policy and Strategy Group
NACOSS	National Approval Council for Security Systems
SITO	Security Industry Training Organisation
SLA	Service level agreement
SLS	Service level standards
SMT	Senior management team
TUPE	Transfer of Undertakings (Protection of Employment) Regulations