Getting Security off the waiting list

Security provisions for hospitals don't have to be expensive or cumbersome – but they must follow a thorough risk assessment. After a series of hospital security scares, Alex Chambers outlines steps even cash-strapped NHS facilities managers can take.

Stories of violence, rape and kidnap on hospital wards around the country are back in the news again, and many hospitals are being asked to review their security provisions. In 1993 hospital security was under the microscope following a number of high profile and extremely distressing cases. However it seems 10 years on, we still have much to learn.

So why do incidents still occur? One of the most frequently used explanations is because of the need to balance security with patient care. It is often felt that heightened security measures restrict the ability to react to the sorts of emergencies hospitals face, and prevent timely treatment of patients. Hospital managers often argue that distressed or fragile patients are intimidated by physical security measures such as CCTV, access control, alarms and buzzers and that hospitals need to be seen as open, friendly and comfortable places. Alongside this must be the age-old election issue of cost cutting within the NHS and, as with most businesses in times of hardship, security is invariably the first area to see its budget slashed.

SENSIBLE AND INEXPENSIVE MEASURES

One of the first points to make is that security provisions do not have to be expensive or cumbersome. There are some sensible and inexpensive ways to instantly improve security without blowing the budget. Some of them can be as simple as changing the way you do things; for example: ' No staff allowed on the wards unless they are wearing their ID badges'; or 'All mothers to be discharged in wheelchairs with their newborns'. Policies such as these will help to spot the rogue staff member intent on theft or the abductor walking out with someone else's baby.

The second point is that security can be designed to serve a multitude of functions. If you want to discourage criminal activities then signage, barriers, locks, cameras, and the presence of security officers can make the message clear. If it's a discreet approach you're after, then a change in policies, hidden cameras and patient tagging may all improve security without increasing patient fears.

The third point is that staff, patients, and visitors alike must all be made to see the benefits of security and buy in to the policies and provisions put in place. Medical staff are already becoming aware of the need for tighter security measures as the numbers of reported acts of violence and verbal abuse toward hospital staff rises. Regular consultation meetings with all the operating groups help focus security needs as well as aiding the buy-in process. With recent surveys showing that as many as one in three nurses have been attacked in the last year, 'the NHS launched its 'Zero Tolerance' campaign, in which hospitals have the right to refuse care to patients who abuse staff. Sadly, however, incidents of violence in hospitals continue to increase.

EXCUSES, BUDGETS AND WASTE

This said, the phrase commonly cited after an incident occurs at a hospital is: 'This is a hospital, not a fortress.'

Excuses are made that tighter controls are not necessary, that they would be difficult to manage and would impose severe restrictions on visitors and patients.

The other most common excuse is that there isn't the money to spend on security in the overstretched NHS. In today's culture of litigation, with companies eager to help people claim compensation for any accidents or incidents (that are not their fault), surely the question should not be 'can we afford not to?'

In many cases, the problem is not a lack of funds, but funds being wasted on ill-advised or unnecessary measures. It takes an expert to recommend the right solutions for any given situation. Deciding what you are aiming to achieve with your security provisions is an important first step. Are you simply aiming to deter offenders or do you wish to prevent criminal activities, protect staff, patients and visitors and possibly prosecute those with criminal intentions?

MONEY WELL SPENT?

A hospital spent £70,000 on CCTV cameras and extra lighting in their car park areas. Six months later, when a drug-addict broke into a parked vehicle and threatened a doctor with a screwdriver, the police commented that it would be unlikely that they could use any of the CCTV footage to help identify the offender or prosecute.

DEVELOPING A SECURITY STRATEGY

The next step is to identify the likely targets and the threats that each faces. This enables the development of a security strategy and a plan to mitigate risk. The security plan must be part of the overall operational strategy of the establishment and must recognise that the hospital's primary function is healthcare. The security strategy should therefore support the activities of the hospital with the least possible negative impact: inevitably some threats/risks might remain only partially mitigated.

The process of threat and risk identification should include an evaluation of the effects each would have on the hospital and its visitors. This will help to highlight areas of concern and prioritise which areas to address and how.

Very few places have as many different types of risks and threats associated with them as a hospital, making the task very complex. Not only do hospitals provide care for patients, teaching and research facilities for medical staff, catering and administration facilities, recreational and relaxation areas, but it also open to the public, making it harder to secure.

Ian Johnson Associates Limited - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

Continued from page 1

Typical areas of special risk are:

- A&E department
- Paediatrics and maternity units – including special care baby units
- Staff safety in and around hospitals – unpopulated wards or corridors, pharmacy departments, pathology, car parks and residential blocks
- Areas that contain items of value – including ward drug storage units, IT and office areas, surgical rooms and radiation departments

Visiting hour, the use of agency staff, emergencies and budgets pose problems to the usual security systems and policies. These issues may undermine the secure nature of a hospital site, and so the incentives for criminals increase. Items such as computers, expensive medical equipment and drugs make hospitals a prime target for thieves. Coupled with this is the need to safeguard those items which are of potential danger to the public, such as hazardous and toxic chemicals, surgical or radiation equipment.

Ask the questions before others ask questions of you! Why have an access control system to a ward if patients are forced to leave the safety of the ward to visit the toilet and risk being vulnerable to attack? Why go to the expense of installing as sophisticated CCTV system if the quality of the recordings is unacceptable in a court of law? Risking the reputation of the hospital by failing to provide 'a duty of care' is no longer acceptable, especially as the risks are only too well documented.

As violence towards staff and patients in hospitals is on the increase, disposing of security officers completely is not recommended as they often provide a much-needed support during an incident. However, it usually proves beneficial to use a mixture of physical and electronic security measures. Spending some of the budget on access control systems will show cost benefits in the longer term, and may free up some of the time of the guards to spend elsewhere e.g. patrolling the car parks or dealing with aggressors etc.

BALANCING SECURITY AND EFFICIENCY

Providing effective security in a hospital is never an easy task, with so many different and varied risk issues to address. The key is to strike a balance between providing a safe and secure environment and an efficient healthcare facility.

To be accepted, security must make sense and be seen to work effectively. All too often insufficient attention is paid to the detail when security measures are being considered. Invariably this is because of poor planning, not allowing enough time and lack of knowledge. It is the panic purchase mentality: something has to go wrong before security is even considered, and then the pressure is on to introduce new equipment or a new procedure as quickly as possible. Hospital security must be the subject of regular reviews to assess and evaluate any changes in risk and potential weaknesses and vulnerabilities in the security planning.

TRANSPARENCY

It is not an easy task to provide adequate security when your budget is constantly under review, however the task is that much harder if one cannot visibly show the benefits of security. One of the greatest mistakes made by those in charge of the security budget is not providing some sort of reporting facility. How can you argue the case for money towards security personnel, training or systems, if you cannot show the value they would or do currently add. For example, perhaps the installation of access control would reduce the number of thefts from staff, patients, and visitors, and so the time taken in reporting, investigating and responding to incidents.

A SECURITY CHECKLIST

Identify who is at risk
- All staff, patients and accompanying visitors

What risks do they face?
- Violence
- Stress, emotionally related
- Medication reaction
- Substance abuse
- Confrontation
- Verbal abuse or intimidation
- Sexual attack
- Robbery and theft of personal property
- Damage to property
- Abduction

When and where might they be at risk?
- Car parks and access routes
- Public areas (e.g. toilets, canteens, waiting rooms)
- Corridors (especially during quiet periods)
- A&E Departments
- Unsecured or low-staff wards
- Private or screened wards, rooms and cubicles
- Areas containing items of value

What assets are at risk?
- Medication
- Medical and surgical equipment
- IT and other portable, saleable assets
- Patient and staff personal property
- Private personal or medical information
- Consumables

If you can do this then you should be able to show that a little money spent on security makes a greater direct cost saving to the hospital as a whole.

It is no easy task to provide tomorrow's security provisions with yesterday's budget but there are still many ways to improve the hospitals security measures - however, proper planning is key. When working within a tight budget, it is even more crucial to plan for the longer term and many integrated systems will allow for you to introduce features stage by stage, as and when money becomes available. If you begin by making some simple changes and working towards demonstrating the benefits to the board, you should find that money allocated to the security budget provides real cost-savings on the whole, which can be plowed back into the hospital and it's security.

If you would like further advice on conducting a security review of your working environment and would like to speak to an advisor, call our consultants on 01252 782664 or alternatively email: info@ija.co.uk

An abridged version of this article appeared in Facilities Management Magazine.

Ian Johnson Associates Limited - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 F: (+44) (0)1252 782818. E: info@ija.co.uk W: www.ija.co.uk