

## Cost effective security management

In December 2003, the Secretary of State for Health launched a new strategy developed by the NHS Security Management Service (NHS SMS) whereby each NHS body was provided with a Local Security Management Specialist (LSMS). Steve Garton, director at Advent IM, discusses the challenges facing a LSMS, and suggests ways in which security can be made more manageable, in the most cost effective manner in tackling security management issues

The hospital environment carries multiple assets not only in the form of physical pieces of equipment, but also in the patients and staff it caters for. As the economic belt tightens, the LSMS is now faced with the challenge of addressing security on a lower budget, locking down equipment, data and ensuring all patients, visitors and staff are physically safe. More often than not, the person in this position has limited resources in-house to support their efforts. As such, we have been increasingly called in to offer expertise and guidance when addressing both the physical security and information assurance of hospitals and care centres alike. This has been further encouraged by theft and data leaks on the rise. As this continues to be the case, senior level staff are raising security on the corporate agenda, as their position ultimately makes them 'accountable' for how secure the hospital buildings and public spaces actually are.



Steve Garton,  
director Advent IM

So, how can the LSMS take on this responsibility in reality and what processes and procedures should they be looking to implement as a way to tackle threats on a hospital'?

Having worked with a number of hospitals, producing a 'security health check' as a clear breakdown of areas for focus, we have become all too familiar with the common concerns and threats within and around the healthcare environment. We have conducted numerous assessments and made recommendations as to how hospitals can streamline their security methods, which in some cases have been approached well but in many others, not so effectively. Poor planning and disjointed strategy tends to conic as a result al' low expertise or ill-advice from a security product provider, looking to sell more units, such as CCTV cameras, unnecessarily.

Security needs to be addressed not only from the designated LSMS, but also at CEO level, as they stand ultimately 'accountable'. If the team of staff see it of importance at board level and noted as everyone's responsibility, then those at the operational end really start to see the value and make decisions based on this wider outlook rather than relying on their own reasoning or instinct, which often can be misled. In one case we saw a CEO of a hospital drafting an entry on the hospital bldg, outlining the importance of security in the building and outer grounds. This one-liner in corporate materials or policies can really assist in getting the buy-in from staff in creating the best environment for providing optimum healthcare for patients. As senior management disseminate the message down, they can lead by example so the LSMS can look to take appropriate and effective action for security on their behalf.



For those in the 'responsible' LSMS position, the task to lock down a hospital can seem extremely intimidating. There are, however, some simple steps one can take to make a hospital a safer place. Foresight is key to assess the true threats on a building and its contents, rather than playing catch-up after a threat has taken a hold. When this happens, it can be detrimental to the hospital brand and long-term reputation. In many cases we have seen hospitals only realise an item is missing when they come to use it for a certain procedure. An effective way to combat this is to simply list all pieces of equipment within each department or ward that are deemed 'essential', i.e. create an asset register. An inventory that purely lists those high priority items will be more succinct and manageable, rather than listing everything from MRI scanners to pens in the stationery cupboard. In addition to physical equipment, I have known hospitals to also log patients and more specifically, babies, to ensure they are kept safe

from harm's way. Additionally, each time a new worthy item is brought into that department it must be added to keep an updated register of all assets within that specified area. Only then can management understand what they are protecting and then make best plans as to how to do just that.

From here it is all about finding ways to safeguard those assets. In some cases, it is deemed fit to electronically tag pieces of apparatus or patients to keep a real-time snapshot of where all are situated. This is a useful means to monitor assets; however it is a costly process and should be considered strategically before being fully implemented. As with all high-level decisions, any pieces of technology must be considered as part of the wider security strategy; solutions do not work solely on their own, but as part of a 'layered' approach. For example you can install CCTV cameras throughout a department but if they are not orientated properly to capture relevant footage, or the doors to that particular space are left unlocked, then the effectiveness is somewhat reduced.



Once all assets are established and recorded, I would recommend that the LSMS or similar, conduct a threat analysis whereby they truly understand the environment they are working in, who requires access to certain parts of the building and why they need to have access. This helps to address the 'opportunist' threat, whose modus operandi might be harder to fathom - an independent view often pays dividends. By establishing points of entry and areas of particular concern - including theatres where expensive equipment or drugs might be stored, offices with high level data filed or patients in critical states - those responsible can look for measures to complement technology solutions they might see fit for adoption. The layout of furniture and walkways can be manufactured so that the traffic of people is directed a certain way, slowed down for CCTV filming purposes or via a reception desk to ensure that visitors are guided a certain way to suit the wider strategy.

In the past we have worked with hospitals to produce a crime reporting process. This is a simple process but is often shied away from as it can highlight serious issues within the institute. However, unless a problem is exposed, it will not be recognised and therefore not addressed. This information can also be used when considering the installation of additional precautions brought on board to lower future risk. It also provides the LSMS with evidence for the board, where threats have been distinguished and mitigated through their security strategy. By working such a process into a mandatory security policy that all staff must sign and adhere to, the LSMS can ensure that all employees are educated about the part they play in the security procedures as well as highlighting actions that are acceptable and those that are not, remembering that security is the responsibility of all.

Unfortunately threats can come in all shapes and sizes, from inside and out, but by really understanding an environment and identifying true threats, the LSMS can best manage the procedures and processes that need to be implemented to safeguard all that resides in the hospital.

For further information, call Steve Garton at Advent IM on 0121 559 6699, email [bestpractice@advent-im.co.uk](mailto:bestpractice@advent-im.co.uk) or visit [www.advent-im.co.uk](http://www.advent-im.co.uk).