

SECURITY IN THE BIOSCIENCE INDUSTRY

Richard Connelly, Screening Manager, Agenda Security Services

Public and private sector companies and organisations working within the bioscience industry have for many years been acutely aware of the need for appropriate security measures to be in place for the benefit of their staff, stakeholders, and not least the general public. Security measures differ from company to company, site to site and in many cases from building to building and even within buildings. This requires a detailed review to ensure the security measures adopted are fit for the purpose and proportionate to the requirements.

When looking to review your security requirements remember two things:

- Do not rely totally on technology alone to provide your security requirements
- Ensure your staff receive appropriate security awareness training

SECURITY AND BIOSCIENCE

The requirements for the highest levels of security to be applied are a necessity with the use of containment laboratories that tackle existing and emergent infectious diseases. Reports in the media are constantly reminding us that we live in dangerous times. We are constantly reminded of the daily threats from terrorist activity, threats from the environment, and threats from horrible diseases that may kill us all off. If we were led to believe these exaggerated musings from the media, we would be unable to lead our normal lives; but sensational stories do sell newspapers and make great headlines – especially on breakfast TV news programmes as it's early in the day when people are at their most gullible!

There is a serious threat from infectious and other organisms to society which can be a local issue or on a global scale. The perceived and real threats need to be subject to meticulous laboratory investigations within secure and controlled environments.

The specific methods taken to ensure both safety and safe working practices contribute and safeguard members of the public and also the laboratory personnel working with these dangerous agents.

It is very important that any organisation embarking on a building project with the ultimate aim of containment of infectious agents needs to be entirely sure of its plans and objectives for progressing the proposed programme at a very early stage of planning and development.

One issue must that not be disregarded as unimportant is the issue of security. Of all the items to be considered, this is perhaps the most important, security of the facility itself to prevent access by unauthorised personnel, and security of the staff working within the facility. However, most important is the secure containment of infectious or other agents being used for the research programmes taking place within the bio-containment areas.

Therefore security needs to be a requirement at all levels and failing to meet basic standards could lead to a complete breakdown. For example, the use of electronic access controls with barriers, guards, CCTV etc will be negated by poor security awareness training being provided to all staff.

Not too long ago I requested to undertake a 'Social Engineering' test with a client and upon arrival I was allowed to enter a research building by merely knocking on a door and asking to be let in! This company has the above measures in place yet I had not been invited, had no pass, and was allowed to wander unescorted in and out of offices unchallenged. My 'tour' was only interrupted when I was spotted by a member of staff who knew me. Social Engineering is a constant threat that is frequently either misunderstood or ignored. Do so at your peril!

Security should be considered from the start particularly when new builds are under consideration. It is essential that external experts are consulted at this early stage in order to gain their knowledge and experience, and to verify that what is being proposed is attainable. The cost of these ventures is considerable, and all involved in the build or construction of biological containment facilities are under no illusion as to how expensive and specialised these structures need to be, and the detailed specifications that are required to ensure that all requirements are met.

Bio-containment facilities need to be designed by specialised architects who have experience and knowledge, together with practical skills, for the development of these unique buildings.

An essential pre-requisite is to search for, and retain, the services of a competent and experienced building contractor who is able to provide a portfolio containing recent successful projects similar to what is being proposed. Visits to these projects should be made and questions asked. Wherever possible, visits to different containment facilities at an early planning stage will contribute greatly to the proposed project at later stages – and perhaps save a considerable amount of time and effort.

Recent reports have highlighted various areas of security within the industry for review including:

- clarity of responsibility for bio-security especially on sites with mixed ownership,
- single unified framework for human and animal pathogens based on risk assessment,
- resourcing in all areas including training,
- funding for projects and continuing development, and
- secure vetting of staff

Your Local Counter Terrorism Security Advisor should be your first and main point of contact who will provide all necessary help and assistance.

REFERENCES & LEGISLATION

The report from the House of Commons Innovation, Universities and Skills Select Committee on Biosecurity in UK research laboratories provides an excellent reference. A copy of the report can be obtained

from:<http://www.publications.parliament.uk/pa/cm200708/cmselect/cmdius/360/360i.pdf>

An independent review of containment facilities by Professor George Griffin provides a detailed review and a copy can be obtained

from:<http://www.publications.parliament.uk/pa/cm200708/cmselect/cmdius/360/360i.pdf>

London First has produced a brief document named Chemical, Biological and Radiological Threats, Good Practice for Businesses. A copy can be obtained

from:http://www.londonfirst.co.uk/documents/CBR_good_practice_notes_FINAL-1.pdf.

Another essential element is compliance with current legislation and regulations. There are several Acts of Parliament which need to be consulted including:

- <http://www.defra.gov.uk/corporate/regulat/forms/Ahealth/path1.pdf>
- <http://www.opsi.gov.uk/si/si2002/20022677.htm>
- <http://www.opsi.gov.uk/si/si2002/20020063.htm>
- http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010024_en_1

A CASE STUDY

Of course, security does not just apply to containment laboratories; the need for proportionate security measures throughout the bioscience industry is also a necessity. Take the development of a new research laboratory as an example:-

The client had decided to implement a building programme to increase current capacity by nearly fifty percent. This required extensive planning including working with the local authority, architects, builders and numerous other groups. Normally this would be difficult enough but as the building was to be used for medical research involving animals, the security stakes were pushed much higher.

Previous developments of this nature have been subjected to extensive and sustained attacks from animal extremist groups, resulting in serious and expensive delays to the project and, in some cases, cancellation. This type of extremist activity has, no doubt, caused some organisations to postpone research projects and even move them to other countries.

The old saying 'failing to plan is planning to fail' illustrates the need for a professional and dedicated team to be identified and involved from the start as an essential element of such a project.

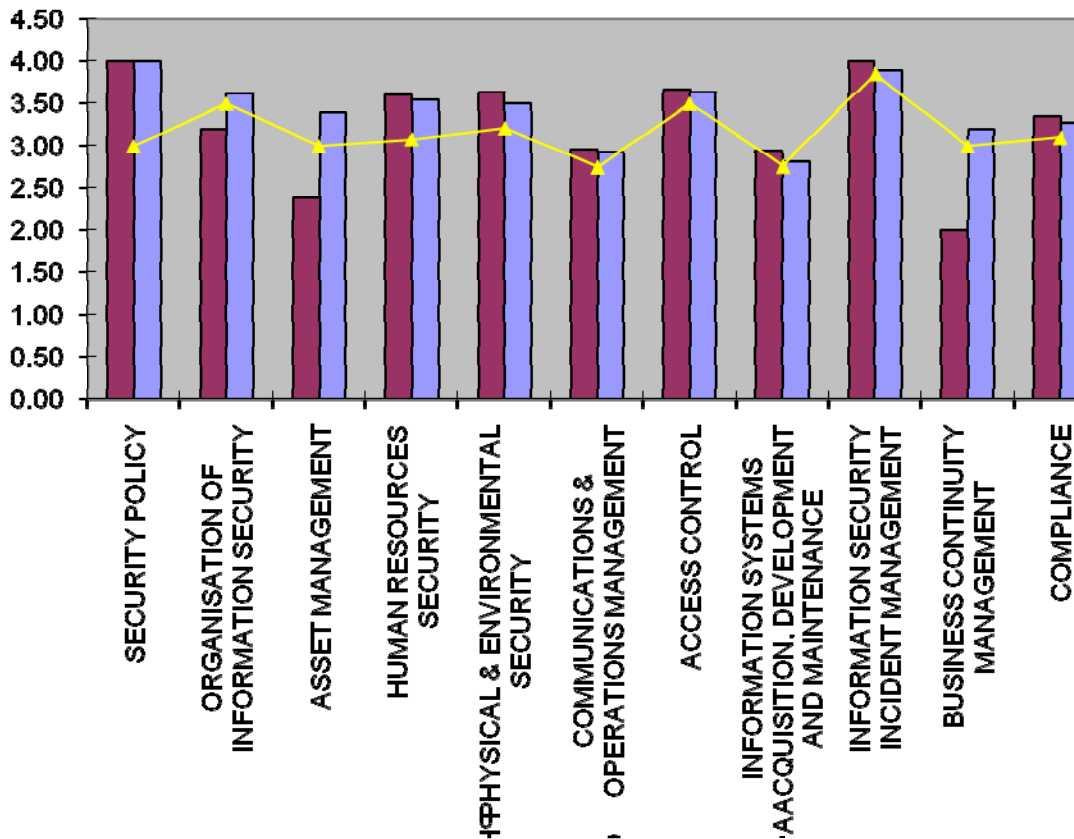
The business case had been created, the Directors were all in agreement, the money was made available and the time had arrived to commence the project. The projected costs for the new build were calculated in eight figures, a significant sum and delays could not be afforded, not least because it would hold up potentially lifesaving research projects. More importantly, activity from extremist groups could cause a significant rise in costs which were not acceptable. Liaison with the local National Counter Terrorism Security Advisor, The National Extremism Tactical Coordination Unit and other professional bodies provided extremely beneficial advice and assistance to identify some of the primary security measures that would be critical to the success of the project

Working with the Home Office, the local authority, the police and other interested parties is essential to create a valuable resource of intelligence, advice and guidance to avoid all possible issues having a potential for disruption. This expertise is also then available to assist in the event of any concerns that might arise throughout the life of the project because the personal contacts have been made, regular meetings held and all parties have a good understanding of the project requirements and scope.

The planning team used the international standard ISO 27001:2005 as a benchmarking tool to assist in the consideration of the many security factors. It provided the team with a detailed Information Security Management System (ISMS) from which all areas of the business plan were to be tested.

The ISO 27001 security model utilised a traffic light system to identify areas of concern, those that required improvement and those that already met the requirements. The results were superimposed onto a graph (see Schedule I) which provided an instant analysis.

Schedule I



The graph clearly identifies two areas of concern, asset management and business continuity, and these were quickly addressed.

Although the standard was able to provide an excellent guide for the development of the ISMS, the project required additional security measures to protect the confidentiality and integrity of all information and stakeholders' details. Projects like this had failed solely on the lack of confidentiality of the data, for example, where animal rights extremist group had identified the builder and contractors and targeted them directly.

Identification of ALL stakeholders was required and regular meetings conducted to brief people and highlight potential issues, but before this could be achieved all external stakeholders had to be subject to thorough due diligence checks before being invited to tender. Those failing to meet very high security standards failed to make it to this first stage and were not privy to the full details of the build programme.

Due diligence screening provides an effective method to identify those companies (and their personnel) who may not be suitable for working on such a project and those companies that have appropriate security measures in place, including business continuity plans, particularly to ensure the supply chain is maintained during the build.

This initial scoping process proved to be extremely effective and lay the ground rules for those companies who were successful to follow.

The issue surrounding lost laptop computers, disks and documents is well known. A careless e-mail with drawings attached showing animal testing rooms, processes and names of clients and locations ending up in the wrong hands, was not an option.

Initial drawings did not contain any of the above details and each copy was numbered and circulated to an approved list. The use of removable media was not approved and all laptops encrypted.

These were just some of the basic security arrangements put into place during the planning process. With regards to the actual design work it is imperative that some members of the planning team have an understanding of the requirements for good security design. The 'Secured by Design' model is a useful template, but there are many other useful sources that offer advice such as the Centre for the Protection of National Infrastructure. In any case, the team must make rational decisions at the design stage to ensure that security is designed in during the build process in addition to the completed facility. It is very difficult to retro-fit effective security and simple ideas like ensuring that the enclosed loading bay can accommodate an articulated lorry for secure deliveries is an example which may be impossible to secure after the building has been completed. Access routes and controls are easier to design in rather than trying to retrofit and so need to be fully considered. There are many other considerations but the point is that they need to be considered at the design stage not when it is too late.

Finally, the project design team must also consider the requirements of the Health and Safety Executive and the Home Office with particular reference to the animal facilities. Business Continuity are buzz words but it applies to all research facilities in ensuring the safe and effective operation of the animal unit in compliance with the relevant legislation and animal welfare policies. At the design stage contingencies can be built in to assure supplies of water, power, heating and ventilation – backup power can be planned in or space made and working put in place for the delivery of backup generators. Store rooms and availability of supplies of consumables and animal feed for example can be considered to ensure sufficient space and supplies to enable the facility to operate when there is breakdown in supply or severe weather delivery issues for example. It is much easier at this planning stage to consider many of the issues that the completed facility might face and develop sensible plans rather than having to deal with a crisis without a plan. Can rooms be isolated to contain a

disease outbreak? This is another example, which is difficult to retrofit although the design element might be to use IVC caging.

It is easy to see why so many research facilities have flaws which the people working there have to put up with because of the lack of a well thought out plan that went beyond the simple facility design process and built in contingencies and security at the design stage! Our role in this case study was to offer independent security on facility design advice. Having design facilities and carried out hundreds of audits, our input considered best practice within the constraints of the budget and allocated building footprint, and resulted in a delighted client who will benefit from learning not only how to do it but also how not to do it. If you have any questions regarding this article please do not hesitate to contact Richard@agenda-security.co.uk.

ADDITIONAL USEFUL REFERENCES

<http://www.netcu.org.uk/default.jsp>

<http://www.nactso.gov.uk/>

<http://www.bsi-global.com/>

<http://www.securedbydesign.com>

<http://www.cpni.gov.uk/>