

# What are the top ten security threats facing the research sector?



**Our perception of security is often developed from our environment and the media. We are all aware of the need for security but our interest is heavily dependent upon how relevant the security issue or threat is to us.**

The biomedical research community operates in an environment where it often faces the usual threats to organisations such as theft and fire but has additional major concerns over animal rights extremists and infiltrations. Add to these concerns over data security and intellectual property rights threats, it is not surprising that the industry is concerned about security. This article discusses some of those concerns and uses a security survey to show the primary concerns of three research stakeholder groups.

Our perception of security is often developed from our environment and the media. We are all aware of the need for security but our interest is heavily dependent upon how relevant the security issue or threat is to us. We all understand the importance of locking the house as we leave home and not letting people see our PIN number, but other security threats pass us by. Animal rights extremist tactics are designed to frighten research workers but we can become complacent because the activity is against another research facility. In the UK the police and prosecution services have done an excellent job in controlling the worst of the extremists; however this success could lead to us thinking that the threat has gone. Unfortunately the animal rights threat is unlikely ever to go away completely and the success in the UK in controlling the animal rights extremists is not yet matched in Europe or the USA where we are seeing an escalation in both activity and the seriousness of the attacks. Those of us work within the research industry or have an association as a supplier,

shareholder or client need to remain vigilant without being paranoid.

Good security practices make common sense. Systems put in place to protect against social engineering by animal rights activists are also very effective against fraudsters, thieves and scam merchants. Protecting and managing your data and information also reduces the risk of ID fraud, major breaches and data losses. There have been numerous examples in recent times of lost DVDs and laptops containing sensitive information and so consideration of the whole information chain is required. The Information Commissioner has prosecuted those who do not comply with the requirements of the Data Protection Act and so having robust controls and processes can assist in avoiding costly fines and bad publicity. Standards such as IS27001 are very effective in assisting organisations to manage their information and consider in advance the “what ifs” to enable the development of contingency plans and business continuity processes. These are much easier to develop proactively rather than in the midst of a crisis.

## **Developing the Security Survey**

Because we all view security differently it was decided to develop a survey to review how different groups within the research sector viewed security. There are many free resources to assess your risks, these are often generic but can be applied very easily to the research environment. A review was conducted to establish the top ten threats for the survey using information from the Centre for the Protection of National Infrastructure, MI5 guidelines, Special

Branch advice, the ISO27001 Information Management Security Standard and the Secured by Design Police accreditation. From the review a list of ten security concerns was developed and a survey generated. In no order of priority the ten primary threats were identified as:

## Top Ten Security Threats

### 1 Own Staff/Agencies

Own Staff/Agencies. How confident are we that we are hiring bona fide people; do we carry out pre-employment screening? Do our suppliers and agencies carry out screening too? Who has access to our facilities?

### 2 Data/Information Loss

How much of a concern are data breaches? Are we confident that our data and our data held by third parties are secure? Are our systems secure and who has access?

### 3 Extremism/Terrorism

How concerned are we by the terrorist or extremist threats? Are we complacent or have we carried out a reasonable assessment of the threats?

### 4 Contingency/Business Continuity Planning

Have we got in place contingency plans? Have we considered business continuity scenarios and communicated the plans?

### 5 Physical Security/Access

How confident are we that our access controls and physical security measures are robust? Do they prevent social engineering and/or break ins?

### 6 Theft/Fraud

Theft and fraud can cause institutions major problems, are we confident that we have preventative measures in place and processes to deal with events?

### 7 Lack of Security Awareness

Are employees security aware? Do they change passwords, lock doors, report issues or do we lack awareness?

### 8 Data/Information Storage and Disposal

Are we confident that access to sensitive data is controlled? Is secure storage available and actually used? Do we destroy confidential waste to BS8470 guidelines?

### 9 Lack of Training/Competency

Are we sure that our staff know what to do? Have they been trained in emergency procedures? Do they not give information away?

### 10 Regulatory Compliance

Breaches of the Data Protection Act are increasing, but what about employing illegal workers or the investigation following an infiltration or allegations?

Whilst not exhaustive, the list was restricted to the ten security concerns to enable delegates at three scientific conferences to complete the survey easily. The three groups were the Scientific Archivist Group (SAG) meeting held in Berlin, Germany in April 2008, the Tecniplast 8th International Scientific Symposium held in Buguggiate, Italy in June 2008 and the United Kingdom Science Park Association - Labs of the Future conference held in Nottingham in July 2008. The sample numbers surveyed are relatively small but the groups represent their stakeholder interests very well:

- Scientific Archivist Group – Research Institution Archivists (47 Respondents)
- Tecniplast Symposium – Research Facility Managers (69 Respondents)
- UKSPA – Researchers and Science Park Research Tenants (26 Respondents)



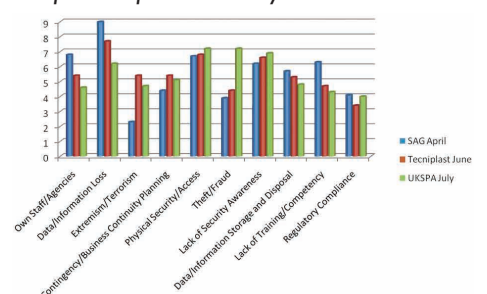
In each case the survey exercise was conducted as a part of a presentation entitled “Delaying Research Facility Security” which looked at the seven layers of security affecting research facilities. The diagram below shows the issues that were presented. The ten security threats outlined above were used to show how any of the ten issues could have an impact on the seven different layers of security identified.

Diagram 1: Delaying Research Facility Security



The delegates were asked to rank the ten threats indicated by giving a score of 10 to the highest threat, 9 for the next and so one until finally giving 1 for the least concerning threat. The results are shown in the following graph:

Graph 1: Top Ten Security Threats Results



### The Archivist Results (SAG)

The primary concern for the archivists was data and information loss which scored very highly. The archivists' next concerns revolved around four key issues; the first was physical security/access, the second was concerns over their own staff/agencies, the third was lack of security training/competency and the fourth was lack of security awareness. All other scores were relatively low with extremism/terrorism being scored as the lowest concern.

### The Facility Manager Results (Tecniplast)

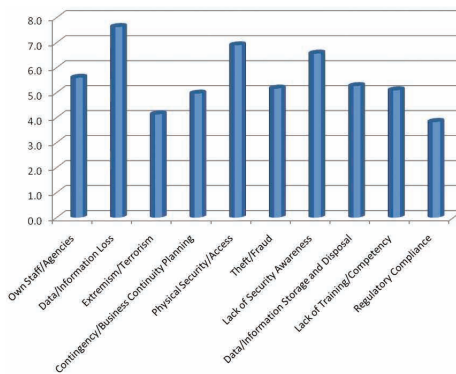
Data and information loss was also the main concern for the facility managers although they did not score it as highly as the archivists. Physical security/access and lack of security awareness were ranked the next two highest for this group overall with the next four highest concerns being own staff/agencies, extremism/terrorism, contingency planning/business continuity planning and data/information storage and disposal. The lowest scoring threat was regulatory compliance.

### The Science Park Results (UKSPA)

There were two main concerns for the science parks with physical security/access and theft/fraud joint highest with lack of security awareness also scoring highly. The next two highest concerns were the lack of security awareness and data/information loss. The next four highest were contingency/business continuity planning, data/information storage and disposal, extremism/terrorism and own staff/agencies. The lowest concern was regulatory compliance.

The results indicate that some of the primary concerns are similar across all three groups and the graph below shows the mean results.

Graph 2: Top Ten Security Threats Means



From graph 2 we can see that the primary concern overall is data/information loss, followed by physical security/access, lack of security awareness and own staff/agencies. The lowest concerns overall were regulatory compliance and extremism/terrorism.

### Conclusions

All three groups work within the research sector and from the individual scores it is clear that they have different perspectives in security. Clearly data security is a primary concern for all groups and the use of a standard such as ISO27001 would assist in the evaluation of the risks and development of processes and contingencies. It would also assist with resolving potential issues in the data/information storage and disposal and regulatory compliance categories. Secured by Design is a good format for considering physical security/access concerns along with the use of a detailed security audit. Self audit tools are available on some of the links below. The issues around the lack of security awareness and concerns over own staff/agencies require further consideration. Training programmes can be developed to raise awareness and even basic housekeeping like clean desk policies and locking things away would help. With regards to staff it is important that we employ people who have our best interests at heart and avoid the costly fines that can result from hiring or using an illegal worker. Prevention of infiltration and industrial espionage is also a factor but having a robust pre-employment screening process and insisting that suppliers also comply with your standards is important and makes good business sense. For example, a major pharmaceutical organisation reported a

reduction in petty theft and crime of over 40% in the four years since implementing a more robust screening process.

It is concerning that extremism/terrorism and regulatory breaches feature so low on the means. Complacency is dangerous and whilst research organisations cannot operate in a steel box we need to remain vigilant to these threats. The Government's baseline screening standard is aimed at having a more robust pre-employment screening process but it is also heavily slanted towards preventing terrorist sympathisers from infiltrating Government institutions indicating that they continue to take the threats seriously.

It might be useful within your own institution to carry out the security survey to see how the various threats are perceived amongst your own employees. At very least it might get your employees thinking about security and when used in conjunction with the limited but representative results reported here, you could benchmark your organisation and set priorities to resolve the highlighted concerns.

A list of useful web resources is listed below:

- [www.securedbydesign.com](http://www.securedbydesign.com)
- [www.mi5.gov.uk](http://www.mi5.gov.uk)
- [www.cpni.gov.uk](http://www.cpni.gov.uk)
- [www.berr.gov.uk](http://www.berr.gov.uk)
- [www.ico.gov.uk/](http://www.ico.gov.uk/)
- [www.bsi-uk.com/InformationSecurity](http://www.bsi-uk.com/InformationSecurity)
- [www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)
- [www.londonprepared.gov.uk](http://www.londonprepared.gov.uk)
- [businesscontinuity/assessingyourrisk/](http://businesscontinuity/assessingyourrisk/)

If you would like any more information about this article please do not hesitate to contact the author, Norman Mortell BA (Hons), Director of Operations, Agenda Security Services, [norman@agenda-security.co.uk](mailto:norman@agenda-security.co.uk) or visit our web site [www.agenda-security.co.uk](http://www.agenda-security.co.uk).