Risk management in higher education and research in the Netherlands

Helsloot, I.; Jong, W

published in
Journal of Contingencies and Crisis Management
2006

DOI (link to publisher)
10.1111/j.1468-5973.2006.00490.x

document version
Publisher's PDF, also known as Version of record

Risk Management in Higher Education and Research in the Netherlands

I. Helsloot and W. Jong

This study examines risk in higher education and research on the basis of a classification into three domains. The practical utility of this division into three domains is that it makes it easier to see what risks are unique to higher education (custodianship of knowledge), what risks are dependent on developments in society (microcosm of society) and what risks faced by an educational establishment are no different from those facing any other organization (education as an organization). The results of a survey of the field (through questionnaires, meetings and interviews) show that higher education institutions still do not routinely have an integrated policy on safety, security and crisis management. Within individual institutions, there is little communication between the three. Institutions, staff and students have limited awareness of the range of risks to which they and their environment are exposed. At the same time, establishments tend not to share their experiences in this field with others. Even within individual institutions, there is often little involvement of staff and students in safety and security policy and its implementation.

1. Introduction

Higher education and research is largely faced with the same 'new' and the same 'conventional' safety and security risks as other sectors in society. In other sectors, e.g. commerce and industry, these risks may present a direct threat to the quality and continuity of a company's operations. In the educational sector, they may have a direct influence on the continuity of higher education and research.

One example of the problem of security in higher education is the vulnerability of information systems in the virtual learning environment (leading to problems of the authenticity, manipulation and theft of information). Another is the vulnerability of the expanding physical infrastructure of higher education (with problems of theft, increasingly complex health and safety conditions, fire). Possibly the most well known example of recent times in the Netherlands was the fire in the computing centre at Twente University of Technology. This was a 'conventional' disaster which, due to the location of the fire, was immediately linked to the 'new' problem of safety and security: protecting information, and temporarily replacing and subsequently restarting an ICT system that is essential to the university's research and teaching.

> On 20 November 2002 a fire was deliberately started in the university complex. It devastated the university's computing centre and reduced to ashes the rooms of dozens of members of staff belonging to three faculties. The damage was put at forty to fifty million euros. This is apart from the loss of data collected in years of experiments which were stored by individual members of staff in their rooms. For the country's insurers, the fire was the signal to review policies throughout the Netherlands and scrutinize the risk assessments of universities, colleges and research establishments.

This example illustrates the need for both risk management and crisis management.[1] Educational and research institutions simply cannot abdicate from involvement in developments in and around themselves, the concomitant safety and security issues, and the logical consequence which is the wish for policy and accountability. Responsibility for all this lies in the Netherlands with the institutions themselves.

The purpose of the present study is to contribute to the development of insights and tools for the benefit of safety, security and crisis management in higher education and science. Key concepts in the study are anticipating risks, being realistic in preparing for them, and understanding the context of higher education and research institutions. The research for it was based on an integrated approach which ties in with existing structures and starting-points for policy such as the autonomy of educational and research establishments.

The research was carried out in four phases.

Phase 1. Getting started

Phase 1 of the research consisted of designing a project plan in which the design and substance of

This study has been funded by the higher education directorate of the Ministry of Education, Culture & Science (OCW) of the Netherlands

the research were further elaborated on the basis of a preliminary survey. In particular, the preliminary survey gave us a framework for the performance of the risk survey in the next phase.

The preliminary survey covered the whole of higher education and research. In it, we used:

- Extensive desk research: international academic literature, research reports, policy papers, legislation and regulation, and the Internet.
- Face-to-face interviews with key informants from the Ministry of Education, Culture & Science and other ministries, educational institutions, research establishments, ancillary services and external experts.
- A telephone survey of selected institutions in order to gather practical information about the current state of affairs in safety and security management in the widest sense.

Phase 2. Nationwide survey

Phase 2 consisted of conducting a nationwide survey to reveal what risks are already being recognised in higher education, in addition to showing what structures and methods (e.g. best practice) are already in place for their management. When compared with the results of the initial survey the risk survey revealed the gaps in current safety and security management in the Netherlands, but at the same time it produced some best practices which are worth sharing.

The risk survey used a structured questionnaire. This was differentiated according to institution, risk type and responsibilities within individual institutions. Following testing in a number of trial interviews the questionnaire was sent to all higher education institutions in the Netherlands. The complete results of the questionnaire are available as Appendix 1 of the online article (please see link on page 159).

Phase 3. Qualitatively validating and interpreting the results

On the basis of the results from phases 1 and 2 a draft report was written which then served as input for two working conferences on safety, security and crisis management in higher education and research. The first of these conferences concentrated on operational responsibilities within individual institutions. The draft report was discussed, as were the general areas in which solutions might be sought for the risks identified by the COT. The second conference focused on administrative responsibilities.

During the working conferences the draft report was taken as the basis for identifying and further discussing the 'blank spots' in current safety, security and crisis management policy. The report of the administrative working conference is available as Appendix 2 of the online article (please see link on page 159). Comments arising have been incorporated into this report as and where appropriate.

This article presents the result of the first three phases of the research.

Phase 4. Developing a Higher Education Safety and Security Audit

The research framework for the risk survey was further refined to create an audit or self-audit framework for periodically determining the state of affairs in respect of safety and security management; this in turn led to the Higher Education Safety and Security Audit, which is available as Appendix 3 of the online article (please see link on page 159).

2. Risks

Starting from the natural understanding of the term 'risk', the well known fact that there is no single, unambiguous definition of the term 'risk' that has the unalloyed support of all experts in the field of 'safety and security' still is surprising. In the literature we find all sorts of definitions of the term. Gratt (1993), for example, presented 14 different definitions of risk, while Vlek (1990) had earlier done comparable work in which he distilled 20 definitions from the literature.

Risk implies both insecurity or uncertainty and undesirability. In the words of a Dutch governmental advising body: risk is the possibility, with a certain degree of probability, of damage to human health, to the environment and to property, combined with the nature and extent of that damage (Gezondheidsraad, 1995).

If we wish to compare risks objectively, however, in order perhaps to arrive at a priority ranking of safety and security measures, we would naturally prefer to have a solid measure with which we can determine the nature and magnitude of a risk. The insurance world has long had just such a measure: the simple formula 'risk equals probability times damage', the result being expressed (in the Netherlands at least) in euros. For its target group, this is an eminently convenient formula. The abstracted version of this formula is widely accepted among safety and security experts: risk is probability times effect. The impossibility of comparing 'apples and pears' means that in the actuality of administration this formula is of little practical value. Of course, even for insurers there is still the problem of finding significant data on the basis of which it will be possible to calculate the probability of a particular type of accident occurring and causing a given financial loss.

As soon as we try to apply this formula more widely than insurance policy holders and the financial loss arising out of accidents caused by or befalling them, we are immediately faced with the problem of how to quantify probability and effect. Disagreements on the subject of risk management can often be traced back to choices made regarding the definition of the limits of the system to be examined. (RIVM, 2003: 19) The discussion is then often about what constitutes a risk-bearing activity, what constitutes damage or loss, how to define the causal link that has to be proved, and within what period the effects have to become apparent.

One of the problems in the case of higher education and research is that it is difficult to calculate the probability of laboratory accidents or to quantify the effect of, say, damage to public image or reputation. It is therefore predictably impossible to arrive at a uniform hard and fast yardstick against which risks in higher education and research can be measured.

Some researchers take the stand that 'all risk is perception', i.e. that there is no usable distinction between an objectified risk and a perception of a risk. 'A risk is a social construct: it is constructed by actors. Objective data may play a part, but this need not be the case. Often there are no reliable data, assumptions on which the calculations are based are often debatable, and in any case a risk, by definition, contains an element of unpredictability' (De Bruin, 1999: 125).

If all risk is a matter of perception, then the question for those who have to assess risks is what aspects of a given risk play an important part in that perception. One of the first systematic attempts to investigate when, in the public perception, the advantages of an activity or technology outweigh the safety risks associated with it was carried out by Starr (1969: 1232–1238). In 1969 he concluded that the acceptance of risks taken freely (such as driving a car or smoking) is roughly a thousand times that of imposed risks. Later research, principally by Slovic and Fischoff in the United States (for an overview: Slovic, 2000) and Vlek and Stallen in the Netherlands (Vlek & Stallen, 1996: 9–31), points to the perception of a risk being determined by a number of important and sometimes interconnected aspects. However, we have not yet reached the stage of being able to produce consistent modelling of the above factors in a way that has any practical predictive value (Sjöberg, 2002: 665–669).

A classification of risks in higher education and research

In the present study the risks that occur or have the potential of occurring in higher education are described on the basis of a classification into three domains. This classification is designed to reflect the diversity of elements that play a part in safety and security in higher education.

Risks are assigned to the following three domains:

a. Higher education as a microcosm of society (social safety and security)
b. Higher education and research as an organisation (organisational safety and security)
c. Higher education and research as a custodian of knowledge (security of knowledge)

Naturally it will always be important to take account of the fact that risks do not really lend themselves to classification into strictly bounded categories: the risks of fire is regarded as a primary risk to physical safety, but there can be no denying that it has points of contact with social safety and security. For example, neglect increases the risk of fire and arson. The vulnerability of ICT is a risk faced by all organisations, but in higher education and research it is an essential risk to the security of knowledge.

The risks falling under the domain of higher education as a microcosm of society are the risks that face society at large and are therefore automatically reflected in higher education with its public function. This means that the risks involved are mainly threats to the safety and security of society.

The risks falling under the domain of higher education as an organisation are the same risks that face every organisation and hence also face the education sector. This is a diverse group of risks which includes fraud, theft and fire. However, because it is very much more than a matter of mere physical safety, we have elected here to use the term 'organisational safety and security'.

The risks that fall under the domain of higher education as a custodian of knowledge are risks connected with the vulnerability of the primary process of education: acquiring, managing and disseminating knowledge. There are several ways in which knowledge can be lost or accidentally disseminated. One important risk in this domain is associated with the vulnerability of the ICT structure within educational and research establishments. The loss of information can pose a threat to academic, scientific, commercial and social interests.

The practical utility of this division into three domains is that it makes it easier to see what risks are unique to higher education (custodianship of knowledge), what risks are dependent on developments in society (microcosm of society) and what risks faced by an educational establishment are no different from those facing any other organisation (education as an organisation).

In order to further subdivide the domains of social safety and security, physical safety and security and the security of knowledge, we use

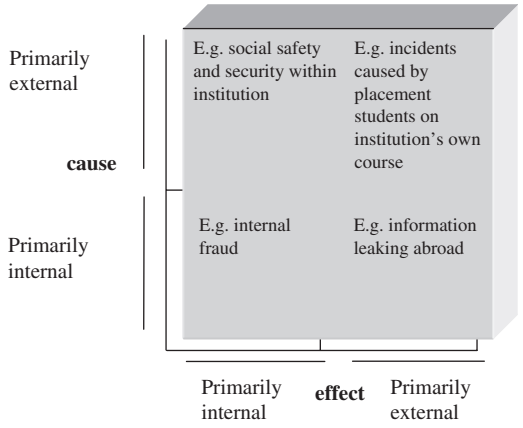
two dimensions: a) the reasons for a risk, and b) the consequences that arise if the risk materializes.

Risks may be the result of two sources: an internal cause (within the institution or an external cause (outside the institution).

This division into two domains gives the institution a handle on safety, security and crisis management, because it makes it possible to see to what extent the institution itself can affect the occurrence of the risk. A risk that is the result of external causes is less amenable to control than a risk that arises outside the walls of the institution concerned.

As a second distinction, risks can be divided according to the impact they have, which may be an internal impact or an external impact.

In the case of an internal impact the institution is the primary owner of the problem and thus has primary responsibility for tackling the situation. In the case of an external impact the institution is probably not the primary owner of the problem. Tackling the problem will in any event entail consultation with external partners such as the local authority, police and psychosocial services.



Using this distinction it is also possible to take a conscious look at the effect of macro and micro trends:

– Macro trends are developments in society that affect the nature and magnitude of both new and existing risks. Macro trends are thus of particularly direct relevance to risks in higher education with a primarily external cause. (Rosenthal, 2001)
– Micro trends are developments within the institution that affect the nature and magnitude of risks. Micro trends thus have a direct effect principally on risks in higher education that have a primarily internal cause.

Trends in the development of risk

To gain sufficient insight into the development of risks within higher education and research institutions it is necessary to have careful monitoring of both macro and micro trends.

The macro trends that are relevant to the present study are:

- Rising levels of aggression and violence, often involving firearms, both in society in general and in schools, are necessitating careful consideration of the likelihood that this trend will also manifest itself in higher education.
- Cutbacks and efficiency operations (whether or not as part of privatization and encouraging competition) are tending to cream off the redundancy of staff and resources which helps prevent risks. This trend is also apparent in the institutions of higher education and research.
- The ongoing development and increasing use of ICT at the same time have the effect of increasing our dependency on it. Institutions are increasingly vulnerable to viruses, hackers, power outages and other electronic inconveniences.
- 'Tolerance is out': the trend is towards zero tolerance. This means that methods of enforcing rules and regulations are under constant development at both local and national level. This trend will clearly have the primary effect of reducing all sorts of risks, but it is also having a secondary effect in that it magnifies the impact of each incident, as it suggests that in the past there has been insufficient oversight and/or enforcement. Higher education establishments have to deal with this as applicants for licences etc., but at the same time they are expected to have their own vision of enforcement within their own institution.
- The multiculturalisation of society is increasing in the Netherlands. However, while it is widely seen as cultural enrichment, multiculturalisation must also be considered a potential source of tension. For example, the tensions between population groups of differing cultural backgrounds may be exacerbated by events elsewhere in the world.

By taking account of these macro trends, an institution can try to limit current risks through proactive action. In this way the University of Amsterdam, having identified the macro trend of multiculturalisation, responded proactively to the threat of war in Iraq in 2003 with a preventively scaled-up Crisis Management Team which assessed the social safety and security risks arising out of the tense situation.

A micro trend affects the probability of a risk materializing within the walls of a given institution. Identifying micro trends calls for the careful use of risk awareness, reporting procedures and incident analysis.

One important type of micro trend is sometimes known as *structural incidentalism*: the fre-

quent occurrence of minor incidents of a particular type often presages a major incident of the same type. One example is the risk of fire. If several waste-paper baskets are set on fire in a school within a short space of time, it is important to recognize that this is a coherent pattern: growing numbers of minor incidents of arson are a sign of a growing risk of a future possibly more serious fire.

Other examples of micro trends in higher education and research are graffiti, which indicate low social safety and security at the site, while racist slogans appearing at various sites in an establishment may be a sign of rising tension within it.

3. Crises

Risks materialize as incidents. Many incidents within the domain of higher education and research are dealt with, to varying degrees of success, at a decentralized level within the institution concerned, but some incidents develop to become a crisis requiring every possible effort if a resolution is to be achieved.

A crisis is defined here as a threat to the basic structures of higher education and research, such that critical decisions are needed which have to be taken quickly and with inadequate information (Rosenthal et al., 1989: 10).

On the theoretical and practical aspects of crisis management many articles have appeared in this journal. It is a matter of conjunction and study to see in what way exactly these are applicable in higher education and research. This article will focus on the risks which can be found in higher education and research.

To be able to manage incidents and crises it is necessary to have an insight into the general crisis trends identified in the literature. This will help not only in effectively managing a crisis but also in deciding in advance which risks need to be given more attention.

As was the case with risks, also for crisis trends can be distinguished (see for example: Rosenthal et al., 2001):

- *Politicisation*. In today's world a crisis is soon about more than the crisis per se. The functioning of the system concerned and indeed that of the individuals involved is almost immediately in the spotlight, and the demand for public accountability cannot be resisted. Independent investigation is often almost a primary requirement.
- *Mediatisation*. There has been a sharp rise in the attention the media pay to crises, to the extent that it now plays a major part in the politicisation of crises. The battle for the hearts and minds of the general public has thus become an important task, particularly for the administrators involved. However, it is important to be aware that the concept of media management is an illusion: the media cannot be managed. It is a matter of earning, rather than managing, public confidence.
- *Mobilization*. The modern citizen is a great deal more vocal than were citizens in the past. He mobilizes fellow victims, the media and the legal system in his efforts to gain 'justice'. There is no crisis without an interest group or lobby. In higher education, of course, the self-mobilizing student has been a familiar given since the nineteen-sixties.
- *Juridification*. Mobilization is closely related to the growing juridification of crises. In the first place it is possible to see rising activism in the criminal law, which is held by those involved to have considerable capacity for furnishing truth and retribution. More than in the past, then, there is a preliminary criminal investigation followed by criminal prosecution. The 'Americanisation of society' is another expression in the Netherlands that covers a great deal of ground. In practice, it often means mainly the growing litigiousness of our society, and the way those who are involved in crises are increasingly inclined to take those seen as their instigators to court.
- *Complexification*. Experience shows that each new crisis tends to involve more and more actors, each having or claiming their own role, responsibility or authority. To these actors, the trends outlined above mean that they cannot simply allow a crisis to run its course. This means that crisis management is increasingly a matter of involving the right players in the complex network of those involved. In preparing for a crisis, therefore, it is important to have knowledge of this network and the competence to operate within it.
- *Internationalization*. One aspect of complexification is the internationalization of crises, and as elsewhere the international component is becoming stronger in higher education and research. Students come from all over the world to every university, and research projects are increasingly a matter of international cooperation and collaboration. An inevitable consequence of this is increased vulnerability of institutions' public image both at home and internationally.

4. Higher education as a microcosm of society

This section looks at the risks enumerated in section 2 under the heading of higher education

as a microcosm of society. In this section they are broken down into primarily internal and primarily external impacts.

To begin with, here are some general conclusions from the survey and interviews.

The present state of affairs

The degree to which social safety and security is seen as a live issue varies widely from institution to institution. Most institutions say that they are paying more attention to the subject than in the past, yet half of them see no risks in the social sphere that necessitate taking new initiatives in this area. By contrast, the other half say that social safety and security has high, if not the highest, priority within their institutions. The majority of this group are universities situated in large towns and cities. They are taking the initiatives necessary to reduce risks in the area of social safety and security.

Risk perception, developments

The response to the questionnaire shows that institutions are wholly or almost wholly failing to identify many risks in the area of social safety and security. Only familiar risks such as theft, sexual harassment and violence are perceived as risks, and only a very few institutions see more diffuse threats such as extremism or terrorism as a risk against which some degree of countermeasures need be taken.

Institutions were asked about perceived developments in the field of social safety and security. Many referred to the more intensive collaboration between universities and colleges aimed at an integrated approach to safety and security issues. In general it is recognized that developments in society mean that the importance of effective safety and security policy is increasing. Reference was made to a sea change in thinking about safety and security: from loss control to providing a safe and secure environment. Part of this sea change is stressing the right norms and values that determine the parameters of social intercourse within the organisation. This is necessary precisely because scaling up and efficiency operations tend to lead to a decline in social control.

Reporting and recording incidents

Almost every institution reports incidents to its board of governors, a complaints committee or a security officer. Most institutions have reporting procedures which work with complaints forms and the like. Reporting frequency varies from institution to institution from daily to annually. At some institutions only very serious incidents are reported to the police.

Risk survey

In half of all cases, social safety and security is part of the institution's risk survey. Roughly a quarter of respondents say they do nothing in this area. The vast majority of institutions say they have no concrete plans to improve social safety and security.

Involving internal and external players

More than half the institutions say they encourage staff to make comments and suggestions in the area of social safety and security. In many of these institutions, staff are in one way or another kept informed of safety and security policy and any changes to it. This is achieved through personal contact, staff circulars, the website, items in house journals, and emails. Some institutions train their staff in how to get on with 'difficult' individuals, or give assertiveness courses.

Few social safety and security initiatives are developed to involve students. However, incidents when they occur are often the trigger for launching public education campaigns aimed at an institution's students. A limited number of institutions issue leaflets drawing students' attention to the complaints procedure and the presence of confidential consellors. Only a few institutions actively involve the student body in the design of safety and security policy.

There is still little consultation with relevant external players such as the police. Indeed, formal obstacles have led to some institutions being disenchanted with their experience of collaborating with the police. A few others, by contrast, have made considerable progress in social safety and security precisely through intensive collaboration with the police.

Social risks with a primarily internal impact

In this section we examine social risks with a primarily internal impact as they emerged during the study.

Theft

It is clear from the questionnaires returned that theft is one of the most frequently occurring types of incident.

Many institutions say they have trouble with persons unconnected with the institution committing theft or burglary. The institutions acknowledge that in general they are highly accessible, which makes them an attractive target for criminals. By and large the institutions have no clear picture of what percentage of thefts are carried out by their own staff or students, though

the security manager at one university estimates that 75% of thefts are committed by students or employees on an opportunistic basis.

> Two unknown men walked into a university and said they were employed by a local firm. At their request, two staff members helped them load two television sets into a van. It later emerged that the men were thieves.

Employees are seldom vetted, even if in the course of their duties they are likely to have access to virtually all the facilities of the institution. Even elementary checks such as asking for a good conduct certificate (a document obtainable from a person's local authority or police as evidence that they do not have a criminal record) or inquiries of former employers are not routine practice. Security staff expressed the opinion that if it were known that checks of this kind would be carried out, it would have a filtering effect: a person bent on criminal activity is less likely to apply for a job for which a good conduct certificate is required.

Where a person is found to have committed theft, the policy in many cases is to involve the police. In serious cases the institution's governing board will also be informed. However, in a substantial percentage of cases of theft the offence will not be reported to the police. Instead, equipment is recorded as having broken down. Part of the explanation for this behaviour is said to be shame on the part of staff who realize that by their naivety or lack of insight they have more or less made the theft possible.

Intimidation, sexual harassment and violence

A survey by the Open Universiteit shows that intimidation and sexual harassment are not confined to primary and secondary schools. Surveys of two universities of professional education revealed that, in their own perception, 16% of students had at some time or another been bullied, subjected to sexual harassment, 'shut out' or discriminated against (HBO Journaal, 2001). In the course of the present study it became apparent that little information is available on this subject, partly because it is still largely a taboo area. (This contrasts with the vocational and adult education sector, where intimidation is a current issue. See e.g: Van Zundert, 2002). Reliable statistics on violence, sexual harassment and comparable issues are simply not available when it comes to higher education. Following the Open Universiteit study, questions were asked in parliament of the then minister of Education, Culture & Science. The minister observed that the study was not a representative sample of higher education in the Netherlands, but conceded that the picture that had emerged from incidents at a number of faculties was 'worrying': 'Institutions of education must guarantee pupils and students a safe environment in which to learn. This is a sine qua non for any form of education.' (TK, 2001: 11510).

Staff at institutions of higher education are experiencing growing levels of intimidation and aggression from students. The explanation put forward for this is the growing propensity for students to make demands (a development that is part of the broader evolution of society at large, sometimes known as the development of the demanding society). If, in his own perception, a student's needs are not being met fast enough, every now and then this leads to threats and verbal intimidation. Respondents to the present study know of employees in service-providing departments of their institution, e.g. audiovisual services, who regularly feel that they are under serious threat.

About a third of the institutions surveyed for this study call intimidation and violence one of the larger risks for educational establishments.

Like other forms of aggression, intimidation and sexual harassment fall within the scope of the Working Conditions Act of 1998. This means that the employer has a duty to take preventive steps to protect both employees and students. At the same time an institution also has an obligation to install measures that will limit the impact of an incident, e.g. by appointing counsellors or psychologists who can help the victims of an incident. Here too it is up to the institutions themselves to determine what form their policy on such matters should take, though there is an obligation to carry out a risk survey and evaluation.

Growing use of weapons

Along with intimidation, sexual harassment and violence, the rising tendency for pupils at schools to carry firearms is a potential danger. At the time of writing we know of no cases of incidents at higher education establishments involving firearms in the possession of students. But when there are signs of a growing weapons-carrying culture at secondary schools, attention to the potential for problems in higher education would seem desirable.

No statistics are available for the carrying of weapons in higher education institutions or incidents involving weapons in higher education. This applies not only to the Netherlands but seemingly to other countries as well. The carrying of weapons, then, is not seen by most institutions as a major problem, and accordingly virtually no steps are taken to detect weapons or to prevent people entering buildings or institution premises while carrying a weapon.

Intolerance resulting in discrimination or violence

The multi-ethnicity of Dutch society is reflected, albeit still largely to a lesser extent, within the country's higher education system. In the larger towns and cities, particularly, there is a broad palette of different cultures. One effect of this is that events in other parts of the world can act to help create tensions between people of different cultural or religious backgrounds. As with the risk of the growing culture of carrying weapons, although higher education establishments in the Netherlands have so far been spared any serious problems in this area there is no guarantee that the problems that are already occurring in secondary schools will not also materialize in higher education.

Quite a few institutions indicated that they recognize this risk and are alert to it. Following the war in Iraq the University of Amsterdam's crisis management team, for example, has met several times in order to carry out a risk analysis of the situation.

Social risks with a primarily external impact

In this section we examine risks with a primarily external impact as they emerged during the study. The risks in question have no direct impact on safety and security within institutions, but are nevertheless closely linked to it.

Individual students' problems leading to incidents outside the institution

Numbers of students calling on the services of a student psychologist have risen sharply in recent years. There are various reasons for this, including loneliness, depression, fear of failure, problems with personal relationships, and the pressures of academic work (Smit 2001). The result may be alcohol and/or drug abuse, declining academic performance and even suicide.

> Following eleven suicides in the space of two academic years the Catholic University of Leuven (Belgium) initiated an investigation of the causes. Of the eleven victims, nine were male. Student suicide is a problem for which few statistics are available, whether in Leuven or at universities in the rest of Europe. More work has been done on the subject in the US. The three main immediate factors in student suicides, the university found, were personal problems, study-related problems and financial problems. (Vandendriessche & Raskin, 2000)

The majority of the institutions surveyed in the Netherlands say that very serious incidents (e.g. suicide) relating to individual students' problems are rare or non-existent. The institutions have a system of study supervisors, counsellors and psychologists to whom students with problems can turn. In urgent cases the student will be referred to one of the organisations providing professional help. The risk itself is recognized: the University of Twente, for example, has taken steps to ensure that it is no longer possible to jump off tall buildings.

Incidents caused by placement students and student assistants at other institutions

It occasionally happens that a placement student or student assistant comes off the rails and passes on sensitive, confidential information or causes damage. The placement student's 'home' institution has a certain responsibility for the behaviour of its students, but the extent to which that responsibility entails liability depends partly on the wording of the placement contract and the preparation or supervision given to the student. At one of the institutions surveyed for this study, a number of serious incidents led to the complete redesigning of its placement contracts so as to limit the institution's liability in the event of damage.

Antisocial behaviour connected with student societies

Over the years there have been a number of incidents in student societies in the Netherlands leading to injuries and even fatalities. Most of these have occurred in the context of initiation rites, and in many cases there had been excessive consumption of alcohol.

In principle an institution has no direct responsibility for what goes on either inside or outside student societies. Every institution does, however, have a natural sense of having a duty of care towards its students – in addition to which, incidents can have a damaging effect on the image of the institution. This is why more recent incidents have elicited a more active response from the governing boards of the institutions concerned.

> In 2001 sanctions were imposed on Veritas and Unitas, two student societies in Utrecht, when it emerged that incidents had occurred during society initiation rites. Both the University of Utrecht and Utrecht University of Professional Education broke off relations with Veritas. A senior student had extinguished a cigarette on the arm of an aspiring member. Unitas was less severely punished with a conditional suspension and withdrawal of subsidies. (NRC Handelsblad, 17 October 2000)

Alcohol and drug use among students

In the Netherlands the Education Council (*Onderwijsraad*) has established that, unlike smoking and obesity, alcohol consumption is greater among the well educated than among the less well educated (Onderwijsraad, 2002: 44). At the same time consumption of narcotics and stimulants among students in higher education is considerable. According to a survey of 750 students at the University of Amsterdam conducted by the university newspaper *Folia*, roughly a third of all students occasionally smoke a joint (Folia, 2002). One in ten students say they sometimes use cocaine. The five most popular drugs to emerge from the *Folia* survey are cannabis, ecstasy, cocaine, mushrooms and speed. The respondents said that they tended to take drugs mainly at the weekends and in the evenings.

Most consumption of alcohol and drugs at higher education establishments in the Netherlands takes place outside the walls of the institution. The institution has no primary responsibility for it, but some nevertheless take the problem seriously. In 1997 the rector of Delft University of Technology said publicly that he wanted students to change their drinking habits. This followed an incident of excessive alcohol abuse at a student society initiation in Groningen which resulted in one death and a serious injury after the victims each drank a litre of Dutch gin. The rector announced that he wished to engage in a dialogue with all the Delft student societies, not in order to impose rules or prohibitions, but to bring about a change in attitude. 'This may not be our direct responsibility', he said, 'but the University still *feels* responsible' (Delta, 1997).

Extremism in higher education

Students, as highly educated citizens, have always had a tradition of criticism. Interest groups and single-issue parties often find fertile ground for their ideas in the institutions of higher education. Most of these groups express their criticism in peaceful and often entertaining protest, but there are also those who are prepared to use violence to lend force to their arguments, and in the area of antiglobalism, the environment and animal rights there are groups and individuals in the Netherlands who have shown themselves willing to resort to violence and destruction of property. Because of their very nature, then, the institutions of higher education may find themselves the unintentional catalysts of social unrest.

Terrorism

The situation as regards terrorism may be seen as broadly similar to the above. The nature of higher education establishments makes them attractive to terrorists, not so much as targets but as centres of recruitment and places where they can go to ground. In the higher education sector this problem and its associated risks are still receiving very little attention (COT, 2003: 4).

One of the blackest scenarios is having a terrorist cell inside the institution. Mohammed Atta and other aircraft hijackers studied at the university of technology in Hamburg, where they held informal meetings (Flinn, 2002): actual recruitment took place in the city's mosques. Fundamentalist Muslim groups have also found supporters in the Netherlands, and are recruiting students for campaigns of violence. According to the security services most of those involved are members of the Moroccan community. 'On the surface they are well integrated, but some of them turn out to have such a radical, anti-Dutch and anti-western philosophy that they are prepared to take part in violent terrorist activities' (AIVD, 2002: 39).

> Two students from Eindhoven were recruited in the Netherlands for the Jihad. In January 2003 they were shot dead by Indian border police. 'Most of [those being recruited] are Moroccan youths – not kids hanging around on street corners but well-educated young people of university or college level struggling with a serious identity crisis and looking for a way out through radical politics and martyrdom in the name of Allah. The established Islamic bodies such as mosque foundations, schools and welfare organisations do not play a direct part in this. They do not engage in recruitment themselves, but contribute to the creation of the fertile ground' (Brouwer, 2002).

Threats outside the premises of the institution

Sometimes higher education establishments are sited in places where they run an added social risk, in particular areas that are unsafe or perceived to be unsafe at night. Students and staff can be molested, robbed, or confronted with verbal or physical aggression or even assault.

The University of Professional Education in The Hague is in such a high-risk area. To reach the university from Hollands Spoor station it is necessary to pass through a pedestrian and cycle subway, 'and that's where things go wrong. Drugtaking and robberies are the order of the day. The Participatory Council demands action'. The university itself has no direct responsibility for the situation outside the walls of the institution, but it still takes the situation seriously. 'Naturally we also have a duty as far as possible to guarantee the safety and security of students, staff and other employees. For some time now

the the University has been concerned by the decline of the area round the station, where in the evenings the streets are full of drug dealers and addicts' (De Posthoorn 2001). According to the police, the worst problem is the sense of insecurity, since in statistical terms there is no reason to suppose the situation has become any more unsafe. Even so, 80 per cent of the university's students think the station is 'creepy', according to the student paper *Atrium* (Haagse Courant, 2002). With the growing feeling of unease, consultations took place between the police and the university, after which the police adjusted their levels of surveillance to tie in with the lecture timetable. At the same time extra CCTV cameras are to be installed.

5. Higher education as an organisation

Introduction

This section is concerned with the organisational safety and security risks facing higher education. These are broadly the same risks that face other similarly sized organisations outside the higher education and research sector.

An important part of all these risks is maintaining physical integrity in the face of threats to buildings, land and movable property belonging to the institution. Fire and burglary are examples of such risks, but this chapter also covers risks of quite a different character such as fraud, the ordinary risks of any working environment, threats to the internal working environment etc.

In this chapter we shall consider risks under two main headings: risks with a primarily internal cause and risks with a primarily external cause.

Using the methodology of the safety and security chain we look first at the options open to educational establishments for managing risks and incidents in the area of organisational safety and security. The experience of higher education institutions will also be presented.

First of all, however, here are some general conclusions from the questionnaire and interviews.

General

Many institutions report that there has been growing interest in the theme of organisational safety and security in their organisations. Safety and security are increasingly finding their way onto the agendas of governing boards and many boards already have designated members with responsibility for safety and security.

There is general agreement that the level of awareness of risks amongst staff and students is comparatively low. At the same time, institutions believe that technical solutions could be more widely employed than they are at present. Sprinkler installations, automatic alarm systems and burglary prevention systems can contribute to the security of the organisation.

Risk perception and current developments

Institutions tend to see burglary and fire as the principal risks to the safety and security of the organisation. Most institutions still barely recognize other sorts of incident as a realistic threat.

Since the fireworks disaster in Enschede and the café fire in Volendam, institutions report that they perceive higher levels of enforcement of statutory and other regulations in the area of physical threats to safety. At the same time, insurers are imposing ever more stringent requirements on institutions. One unexpected consequence of this is that where budgets remain unchanged, the investment in safety and security that is required means reduced investment in the institution's primary process, i.e. teaching or research.

Reporting and recording of incidents

Almost all the institutions surveyed record and analyse incidents affecting the safety and security of the organisation. However, the extent to which they have a systematic way of doing so varies from institution to institution. Some higher education institutions have also started keeping accurate records of near accidents, and in some cases annual programmes of risk inventories and evaluations are operated. In such cases the learning points are taken forward into the planning and refining of the in-house emergency services.

Risk survey

The survey revealed that about a two-thirds of all institutions carry out a regular risk inventory and evaluation, in many cases using advice from external consultants. By and large these studies are of a fairly standard health and safety nature.

One or two institutions say they have incorporated the principle of the learning organisation into their own organisation. Safety and security staff at the various faculties maintain each other's alertness. From time to time building managers go through each other's buildings to pick up hints and help eliminate mistakes. At another institution an unannounced inspection is carried out roughly once a quarter by the facilities manager and a member of the governing board. This includes a random sample of basic elements such as the state of power points, step-ladders etc.

Collaboration with internal and external players

Preventive policy in the area of organisation safety and security is almost nowhere arrived at

in consultation with staff and students. However, this is an area in which there has always been a high level of involvement on the part of both staff and students in the preparation and response phases as regards physical risks: the staff contribute the members of the in-house emergency response team, while both staff and students take part in fire drills and evacuation exercises.

Most institutions employ specialist outside consultants when it comes to designing and implementing the organisation's safety and security policy. One result of this is that many institutions appear not to have a clear overall picture of this area. Many institutions, for example, consult closely with the local fire services on matters of fire safety. This clearly has benefits, but it means that there is a risk that the institution will lose sight of the fact that looking after the continuity of its operations is different from the fire service's primary responsibility for the personal safety of individuals.

Organisational safety and security risks with a primary internal cause

Fire

Fire is one of the most obvious risks to any organisation. In preparing their in-house emergency response teams and disaster plans, institutions will naturally pay attention to the various fire prevention systems installed in their buildings. Most institutions also regularly hold fire drills and evacuation exercises which are intended partly as a means of raising awareness amongst students and staff.

However, the effects of the major fire at the University of Technology in Enschede were an eye-opener for both institutions and insurers. The result has been the imposition of increasingly stringent requirements by insurers, since on closer inspection fire turned out to be a much more serious doom scenario for many institutions than had been supposed. For example, only a few higher education establishments were found to have backups and alternative computing facilities outside their own complexes. Many institutions are housed in old buildings – many of which, of course, are of historical importance – with concomitant limited fire safety. And many institutions hold collections, often completely irreplaceable, which are in danger of being lost to fire.

Arson

Arson deserves a separate mention as a risk because fire prevention systems are by and large not designed to cope with the rapid spread of fire that is often a result of deliberate fire-raising. The fire on the complex of the University of Twente in Enschede, referred to above, is a case in point.

It is not easy to prevent arson. The experience of insurance companies shows that the symptoms often fail to be picked up as the early warning indicators of more serious incidents to follow. For example, a burning waste-paper basket is often overlooked as a failed attempt at arson, being merely interpreted as an act of vandalism aimed at the waste-paper basket concerned.

One important motive for arson may be revenge by employees, former employees, action groups and students who have 'come off the rails'. Action groups will usually target laboratories known or suspected to be carrying out tests on animals or other socially sensitive experiments. Locations depend on motives, and in such cases are usually chosen with considerable care. Attempts at arson inside buildings need to be prevented by effective surveillance. To sum up, important factors in combating arson are a) raising awareness among students and staff and b) implementing or improving early warning systems.

Safety and security at work in general

As employers, higher education institutions have a responsibility for the health and safety of both their staff and their students. Some courses will naturally be more prone to physical accidents than others: the risk of injury is greater for a student of physical education than for a trainee accountant. In other words, the risks attendant on every kind of course need to be assessed individually. Work in workshops and laboratories call for extra safety measures.

To varying degrees, institutions are banking on increasing staff and student awareness of the risks they run. Some institutions said that risk awareness was low, particularly among students. Some have developed policy in this area, partly because of fear of litigation in the event of an accident. One best practice we came across was to give laboratory staff safety training and then have them sign for receipt of a safety manual.

A survey carried out at the University of Utrecht showed that 40% of the students complained of symptoms of RSI. The university's governing board says it plans to take steps to improve the ergonomics of computer rooms, but at the same time expresses the view that RSI is the responsibility of the individual student. 'Students must accordingly take their own limits into account when it comes to RSI prevention using programs such as Workpace.' (Willemars, 2002)

Safety and security at work: the threat to the interior environment from hazardous substances (e.g. asbestos)

Several institutions had been faced with the threat of pollution of the interior environment. In most cases this followed the discovery of asbestos, but in some cases it was a matter of releases of hazardous materials that were being used for teaching or research purposes. In one establishment, for example, a formalin leak led to the fire brigade being called upon to remove the leaking storage container (Provinciale Zeeuwse Courant, 2004). Incidentally renovation work can release other hazardous materials besides asbestos, including paint dust. Some institutions have particular concerns about safety and security in and around laboratories. What is curious here is that they all appear to believe that the safety and security situation in their own laboratories is well regulated: it is at the laboratories of other institutions that they foresee more serious safety and security risks. One risk commonly mentioned in the surveys is burglary, and in particular the danger that vandalism or inexpert handling may cause hazardous materials to be released. One of these institutions has implemented steps to limit this risk: not equipping computers on the ground floor with flat screens and not making laptops available to members of staff has led to a reduction in the security risk for the whole building.

A number of institutions covered by the survey work with microbiological pathogens.[2] Safety and security measures for laboratories working with such materials are classified in four levels which apply all over the world: the biosafety level (BSL) scale. Those with operational responsibilities who were interviewed for the study have concerns about the safety and security of such laboratories, largely as a result of budgetary tensions between safety and security measures on the one hand and the primary process of research on the other.

Fraud

Fraud is a multifaceted problem, even in higher education establishments. As in any organisation, the first step to take is to try to ensure that the institution's own staff are not exposed to temptation.

A recent example of widespread fraud by students is the cash card fraud at the Fontys colleges. Early in 2003 the college administrators became aware that students had been illegally loading their chip and PIN cards on a large scale. The board thinks the loss may be around 50,000 euros, but it may be even higher. Using a device on sale from mail order firms, it proved quite easy to load cards without handing over any money. This kind of trick had previously been observed on a small scale, but when the practice became widespread the board decided it was time to intervene. The college sent all students a letter informing them of an amnesty for those who came forward voluntarily, unless they had enriched themselves by trading in the loading of cards (Fontys, 2003). By the time the amnesty ran out 120 students had gone to the security department to admit the offence. The reporting on this fraud in the regional media is an illustration of the crisis trends referred to in section 2: 'It is a typical case of centralizing services leading to too great a distance between the shop floor and service-providers. The service-providers sit in their ivory towers and ignore signals that things are going wrong. And when things do go wrong, Fontys immediately gets things wrong too. The result is that once again we can read in the papers what policy makers have been doing with money that should have been used for teaching' (Brabants Dagblad, 2003).

Apart from monetary fraud, educational establishments are also faced with examination fraud, mainly in the form of plagiarism. This will be discussed in more detail in the following chapter on the security of information.

Incidentally fraud involving student funding is common. However, it falls beyond the scope of the present study as the institution is the owner of neither the problem nor its effects.

Organisational safety and security risks with a primarily external cause

Burglary

Most institutions see burglary as a major risk, not just in terms of the risk of losing hardware but also, just as importantly, the risk of losing valuable information. Security outside office hours is by and large considered adequate, with access control and ID card systems for each building.

During the day, however, colleges and universities provide an open environment in which persons of malicious intent can easily and anonymously do their worst. Insurers are urging institutions to institute special telephone lines to make it easier for people to report unusual events or people anonymously.

Extreme weather

Extreme weather conditions are barely seen as a problem. Despite this, they can lead to considerable damage and inconvenience. In 2002 two cloudbursts at the University of Twente caused substantial flooding and the fire service had to be called to pump basements dry. It is advisable in advance to identify which rooms within the institution are below ground level and the extent to which problems may arise in the event of

cloudbursts or extremely heavy or enduring rain or snow. Particular attention should also be paid to vulnerable buildings which may be liable to collapse in severe storm conditions.

The University Library in Maastricht has developed a disaster plan to bring whole collections of books to safety in the event of fire and/or water damage. The plan is based on the disaster manual published by Overleg Kunst(historische) Bibliotheken Nederland * Art Libraries Society / The Netherlands (OKBN * ARLIS/NL), which gives instructions for avoiding and limiting damage as a result of fire, flooding and mildew. The book also provides instructions for packaging and recording material to be evacuated and the requirements with which drying rooms must comply.

There is one weather phenomenon that is expressly excluded from many insurance policies and is nevertheless not perceived by most institutions as being a problem: lightning strike causing induction currents in electronic equipment. In this way lightning can seriously damage or even completely destroy computers, television sets and sensitive measuring equipment even at a considerable distance from the strike. In modern educational environments it is impossible to switch all hardware off when the weather turns bad: servers generally run day and night, as do faxes, telephone switchboards, alarm systems and so on. Without the necessary protection, not only the equipment but also the knowledge held within it can literally disappear in a flash.

Infectious diseases

Infectious disease can strike anywhere, and that includes institutions of higher education. Students in higher education, unlike pupils in primary schools and at some boarding schools, do not constitute a special risk group. Even so, it is still possible for a student to contract an infectious disease such as TB or hepatitis A and infect fellow students.

One special case here is legionnaires' disease, caused by the bacterium *Legionella pneumophila*. The buildings of any institution can harbour the disease in their water systems or, more particularly, in other damp locations such as cooling and air conditioning systems. When water evaporates, aerosols are created: tiny droplets which can cause infection when they enter the lungs. In 1999 the Netherlands experienced a major outbreak in which some 300 people were infected, of whom thirty died. The source was found to be a bubbling pool that was part of the decor for a flower show. Stricter regulations were subsequently introduced.

The SARS epidemic has shown how easily an infectious disease can spread in hospitals. Many infections are nosocomial infections: that is, infections that arise in hospitals. Hospitals accordingly have policies and plans to cater for this eventuality.

With 250 or so Chinese students, the Hogeschool Zeeland in Vlissingen (Flushing) was quick to see the potential danger of the SARS outbreak. The university took a number of measures including approaching these students by email recommending that they did not travel home for the time being. Risk areas were closely monitored so that if a student should display relevant symptoms a doctor could be promptly alerted. Six students returning from a visit to Shanghai were placed in voluntary quarantine (De Telegraaf, 2003).

Terrorist threats

Many institutions' emergency plans cater for the eventuality of a bomb threat. It is left to the police to decide how seriously any given threat should be taken, though in the case of a terrorist threat involving nuclear, chemical or biological materials the fire service is brought in too. In either case, evacuation procedures are followed.

Following the anthrax letter bomb attacks in the United States in 2001, numerous hoax letters containing powder were sent in the Netherlands. Obviously a letter of this kind can cause just as much unrest, anxiety and uncertainty as a bomb threat.

Institutions at which experiments are carried out with animals are exposed to a constant threat. Up to the time of writing a number of incidents have taken place involving opponents of animal experiments. These have included three occupations and a number of bomb threats, demonstrations and arson attacks as well as destruction of property. Institutions involved in experimentation with genetically manipulated organisms are also under constant threat. The institutions concerned do their best to promote a better understanding of their work, but this has predictably little effect on the more radical elements who are responsible for the more serious campaigns.

> One research establishment said that attempts had been made to infiltrate the institution by animal rights activists. One of the perceived risks of such an infiltration is the possibility that certain acts or situations could be staged in the laboratory and then photographed, after which the photographs would be used as the basis of propaganda against the institution.

6. Higher education as a custodian of knowledge

The core task of higher education and research is to gather, develop and disseminate knowledge.

To achieve this goal, the institutions of higher education and research must have a range of facilities available for the use of students and teaching staff. Knowledge is gathered, analysed and applied through access to an intranet and to the Internet, in computer rooms and libraries, and through lectures, seminars and tutorials.

Most educational establishments try to be as flexible as possible in their provision of access to information for students and teachers. At the same time, however, they run the risk that the facilities they offer will be abused. This chapter looks more closely at the risks that institutions run in their function as custodians of knowledge. The target of policy in respect of the security of knowledge consists of two main elements: a) abuse of the systems in which knowledge is developed, stored and processed, e.g. computer networks, and b) abuse of knowledge as a 'product' with which the educational sector works.

It will be readily apparent that the balance between the unfettered transfer of knowledge, on the one hand, and security, on the other, is a precarious one. Too great an emphasis on security will compromise the core task of higher education and research. For example, it would today be inconceivable to make it impossible for students to access the Internet, since this would clearly have a major impact on the dissemination and collecting of knowledge. Conversely, however, unconditional access to facilities is attended by major security risks. Making the Internet accessible without some kind of security system also means easy access for viruses, worms and other forms of digital unpleasantness, in addition to offering unauthorized persons an opportunity to abuse the facilities made available.

In this section we shall further break down the risks into those with a primarily internal cause and those with a primarily external cause.

First of all, however, here are some general conclusions from the questionnaire and interviews.

General

Without exception, the institutions taking part in the survey report that in recent years they have been taking a growing interest in the security of ICT systems. Many governing boards now have an ICT portfolio holder tasked with overseeing matters of computer and network security. On the other hand, those who are responsible for the actual operation of these systems observe that although more attention is being paid to these problems, the problems themselves appear to be growing at an even faster rate. Whereas previously ICT incidents were relatively rare, now they are the order of the day. The extent to which systems are secure varies from institution to institution. Many institutions have, or are working on, a policy for ICT security.

Risk perception and developments

ICT is penetrating ever further into the education system. Electronic learning environments are gaining in popularity and, if possible, have to be accessible worldwide. With this growing penetration of ICT systems, however, the vulnerability of institutions is also growing. This in turn makes increasing demands on security requirements for authorization, authentication and protection, including encryption. Institutions acknowledge this growing risk to varying degrees, but in every case the security of information is swallowing up an ever larger part of the ICT budget. Yet the users and financial administrators of ICT systems see no measurable result of these rising costs. The fact that a system has not been hacked is not, after all, a measurable entity. The absence of incidents then leads to renewed pressure on the available budget.

Reporting and recording of incidents

The recording and analysis of ICT incidents is something that most institutions now take seriously, but there are still clear differences in the professionalism of their approaches. Those at the forefront in this field have their own central computer emergency response teams (CERTs) which have the skills and hardware to tackle, record and analyse incidents.

Risk surveys

A minority of institutions engage in the systematic analysis of information security risks (including ICT risks). A third of the institutions taking part in the survey confirm they have just started or are just about to start such a scheme.

Collaboration with internal and external partners

When it comes to the security of knowledge, collaborating with external players does not appear to be part of most institutions' thinking. Nor do they have any knowledge of any obvious organisation to which they might report incidents in this area, or to which they could turn for advice.

Students and teaching staff are engaged in the security of knowledge mainly by promoting awareness, and in particular by having their attention drawn to the use of access codes and codes of conduct. Some institutions actively raise awareness levels through advertising campaigns warning of the dangers of the Internet and stressing the need to use security software, make regular backups of data files and treat passwords with appropriate caution.

Knowledge security risks with a primarily external cause

Types of threat to the ICT infrastructure: digital activism and hacktivism

The various forms of threat to the ICT infrastructure of higher education establishments can be broken down into digital activism and hacking:

- *Digital activism:* Digital activism is the use of the Internet or an intranet in the service of a particular cause.
- *Hacking:* Hacking is the process of gaining or attempting to gain access to (supposedly) secure parts of the ICT infrastructure or other computers. Thus hacking does not by definition cause damage, but it can do so if the hacker makes changes to files or routines in the target ICT system.

In recent years there have been some spectacular and successful attempts by activist and hackers to disrupt vulnerable national and international communication networks (Denning, 2001: 241).

Knowledge gathering for illicit purposes

Almost all educational establishments operate an open door policy, which means that anyone wanting to accumulate knowledge is welcome to take part in the learning process. The criteria on which students are selected are previous education and adequate financial resources. Screening on aspects relating to security is unheard of. The same applies, in general, to teaching staff and researchers. In the case of many courses there is no need for this to be any different, given that what is being taught is not in any way confidential. But there are exceptions. Establishments and departments engaged in teaching and research in the fields of physics, chemistry and medicine can be of interest to countries, groups or companies wishing to steal or misapply knowledge.

> At TNO, the Netherlands' principal defence contract research organisation, a constant watch is kept against the leaking away of knowledge that might be abused for commercial purposes or for the fabrication of weapons of mass destruction. Given the organisation's history as a supplier to the defence industry, this is hardly surprising. TNO has its own safety and security managers to carry out monitoring and training, but at university research establishments this awareness of security issues is still far less well developed.

At the present time neither the Netherlands nor the European Union has legislation governing the way citizens are supposed to handle sensitive information and knowledge. In the US, by contrast, such legislation does exist in respect of e.g. biological agents such as anthrax.

'Over the past few years in a number of countries Chinese students and scientists studying or working in the West have been discovered to be involved in intelligence activities. Most of them were in the West under one or other of the Chinese government's official programmes for boosting knowledge in that country. These are public programmes the purpose of which is to enable China's knowledge economy to catch up with the West. Taking part in such programmes is sometimes clearly no more than a cover, however. Some years ago two Chinese students in the US managed to gather information that was useful for the production of a chemical substance used in sensors and weapons. They succeeded in passing this information on to China before their activities were discovered.' (AIVD, 2004: 10).

Possibly the best-known example of such an abuse of hospitality in the Netherlands is that of Dr Abdul Khan, known in his own country as the father of Pakistan's atom bomb. Much of his expertise was gained when he was working on a sponsored project in the Netherlands during the 70s. He concluded his placement with the theft from his employers and hosts of the design of a sophisticated device used for uranium enrichment (AIVD, 2003: 19).

Knowledge security risks with a primarily internal cause

Misuse of ICT facilities

In the perception of most higher education institutions the most serious risk for ICT systems is their misuse by students and staff. Misuse in this context is taken to be use in any way other than that envisaged by the institution. This can include the dissemination of seditious messages or pornographic images, but it also covers the deliberate deletion or corruption of files, the disabling of systems and the unauthorized use of access codes. The extent of possible misuse is closely linked to the degree of security applied to the system.

Those with operational responsibility for the security of ICT systems in institutions warn of limited security awareness among end users: in short, user-friendliness comes before security. Although most ICT departments provide information about security as part of their general conditions of use etc., users tend to see this more as an unnecessary imposition than as helpful information.

The University of Twente in Enschede has one of the fastest computer networks in Europe and is thus a particular favourite for computer enthusiasts. Not all of them are entirely innocent,

however, as the above incident shows. At the end of 2001 the university found itself in the spotlight when it became apparent that its computer network was at the centre of the European trade in illicit software. Several persons were arrested during raids on the campus and their computers confiscated. They are suspected of being part of an organized crime syndicate.

Accidental loss of knowledge

The consequences of fire in any building or complex of buildings depend largely on how much attention has been paid to the physical aspect of the security of the organisation. Being prepared for fire is a prerequisite for being able to tackle a fire effectively. Fire extinguishers, smoke alarms and fire retardant materials are all extremely important. For the security of knowledge, fire – or any risk that can lead to physical damage – is a major threat. The destruction of computers, databases and/or libraries can mean an irreparable loss if the knowledge stored in them is lost.

The November 2003 fire in the computing centre of the University of Twente, referred to earlier, led to estimated tangible losses of €40–50 million. The intangible losses, however, were felt far more painfully: from one moment to the next staff lost unique research material from their own rooms, doctoral students lost research results, and project reports and written examination papers were burnt.

One very important link in the chain of the teaching and research that go on at universities and colleges is of course the people who develop and convey all the knowledge concerned: the teaching staff, from professors down to the humblest junior lecturer. If any one of them is lost to the institution due to illness or death this can mean the loss, too, of knowledge that cannot, or cannot quickly, be replaced. Clearly, this can lead in turn to problems of continuity in both research and teaching.

Intellectual fraud

Intellectual fraud, whether by staff or students, is a threat to the reputation of the institution concerned.

Over the past few years the Netherlands has seen a number of cases of possible plagiarism by teaching or research staff. In 1996 the case of clinical psychologist René Diekstra caused a great deal of commotion. In the end it became clear that Diekstra was innocent – but not before he had been forced to resign and his reputation and that of the university concerned had been damaged. The affair led to debate about the necessity of paying attention to this risk. 'Whistle-blowing is useful and not something that should be censured, it seems to me. If you want to avoid misconduct, you must get everyone to be on the lookout for transgressions and transgressions must be made a possible subject of discussion' (Zandbergen, 1996).

Of course, staff members are not the only people who may be guilty of plagiarism. An American study revealed that 122 out of 1500 student papers examined contained instances of plagiarism. This was established by using a simple computer program to compare phrases in different papers (Fokkinga, 10 May 2001).

Following a study carried out by his inspectorate, in 2002 the Netherlands' chief inspector of higher education called for more attention to be paid to the scale on which intellectual fraud of this kind was being committed, and warned universities and colleges that they were insufficiently alert to fraud in academic papers and theses (NRC Handelsblad, 2002). Institutions immediately endorsed the importance of having and implementing hard-hitting sanctions to counter this form of intellectual fraud because 'this kind of behaviour ... damages the very essence of science and scholarship' (Rector of the University of Tilburg, 2002). Since then, many institutions have taken steps to detect fraud in academic papers and theses. But fraud control stands or falls by the number of available files with which papers can be compared, so collaboration with other faculties is essential (Universiteit var Tilburg, 2002) – yet collaboration between universities and colleges to combat fraud has yet to materialize. Nor is there any uniform policy on sanctions, though individual institutions have announced severe punishments including dismissal and even seeking criminal prosecution. Some institutions have developed codes of conduct for dealing with plagiarism.

7. Conclusions

This study shows that higher education institutions still do not routinely have an integrated policy on safety, security and crisis management. Within individual institutions, there is little communication between the three domains (social safety and security, organisational security and the security of knowledge). Institutions, staff and students have limited awareness of the range of risks to which they and their environment are exposed. At the same time, establishments tend not to share their experiences in this field with others. Even within individual institutions, there is often little involvement of staff and students in safety and security policy and its implementation.

In the area of *social safety and security*, establishments are seen to be mainly focused on what can now be regarded as the 'conventional' risks such as theft, sexual harassment or the problems of individual students for which provisions have in many cases already been made in the form of confidential counsellors, complaints procedures

and sanctions policies. Establishments still seem to be relatively unaware of the risks that particular developments in society bring with them. They are also less well prepared to deal with incidents occurring outside the establishment but in which students or staff are involved.

In the area of *organisational safety and security*, establishments are found to make preparations only for the familiar risks in that area, e.g. fire and burglary. Less common events such as fraud, the release of hazardous materials or organisms from laboratories, or the threat of terrorist attack, are still given low priority. It is precisely within this area that establishments are currently experiencing increasing pressure from external parties such as licensing authorities, inspectorates and insurers.

In the domain of *security of information and knowledge*, establishments currently focus most of their attention on the risks associated with the use of information technology. Efforts to control other risks in this domain, such as intellectual fraud and the risk that sensitive information will pass into the hands of undesirable individuals or organisations, are generally at a much more rudimentary stage.

Notes

1. Risk management is here defined as all activities aimed at managing risks, i.e. preventing them from materializing as incidents. Crisis management is combating the consequences of an incident once it has taken place.
2. This category of materials is here taken to include viruses, bacteria, prions, fungi and parasites.

References

AIVD (2002), *Jaarverslag 2002*, The Hague.

AIVD (2003), *Profileratie van massavernietigingswapens; Risico's voor bedrijven en wetenschappelijke instellingen*, The Hague.

AIVD (2004), *Spionage en veiligheidsrisico's; actueel, onzichtbaar en divers*, The Hague.

Brabants Dagblad (2003), 'Honderdtwintig studenten melden fraude bij Fontys', 26 February.

Brouwer, A. (2002), 'De Algerijnse connectie', in *De Groene Amsterdammer*, 16 November.

Bruin, J. A. and Heuvelhof, E. F. (1999), *Management in Netwerken*, Lemma, Utrecht.

COT (2003), *Aandachtspunten OCenW dreiging oorlog Irak* (draft), The Hague.

Delta (1997), 'Rector wil beraad over drankgebruik', jaargang 29, no. 28.

Denning, D. E. (2001), 'Activism, Hacktivism, and Cyberterrorism; The Internet as a Tool for Influencing Foreign Policy', in Arquilla, J. and Rohnfeldt, D. (Eds) *Networks and Netwars: the Future of Terror, Crime and Militancy*, RAND, Santa Monica.

De Posthoorn (2001), 'Hogeschool wil af van onveilige tunnel', 2 May.

De Telegraaf (2003), 'Maatregelen SARS op Hogeschool Zeeland', 3 April.

Finn, P. (2002), 'Sept. 11 plot came together in Germany', *The Washington Post*, 11 September.

Fokkinga, P. (2001), 'De bedrieger bedrogen', *www.edusite.nl*, 10 May.

Folia (2002), Available online at: http://www.foliacivitatis.nl.

Fontys (2003), Available online at: http://www.fontys.nl/nieuws/nieuws_artikel.asp?docid=1905.

Gezondheidsraad (1995), Commissie Risicomaten en risicobeoordeling, *Niet alle risico's zijn gelijk. Kanttekeningen bij de grondslagen van de risicobenadering in het milieubeleid*, The Hague.

Haagse Courant (2002), 'Het onveilige gevoel rond Hollands Spoor', 19 April.

HBO Journaal (2001), 30 May.

NRC Handelsblad (2000), 'Erasmus straft studentencorps voor wangedrag', 17 October.

NRC Handelsblad (2002), Available online at: http://docenten.nrc.nl/nieuwsbrief/archief/2002/10.html.

Onderwijsraad (2002), *Samen leren leven, Verkenning, onderwijs, burgerschap en gemeenschap*, The Hague.

Provinciale Zeeuwse Courant (2004), 'Giflek bij Ziekenhuis', 10 June.

Rector of the University of Tilburg (2002), quoted in: 'Plagiaat en spieken strafrechtelijk vervolgen' in *Univers Online*, 17 October.

RIVM (2003), *Nuchter omgaan met Risico's, Milieu- en Natuurplanbureau (MNP)*, Bilthoven.

Rosenthal, U. (2001), 'Veiligheidsniveaus: over menselijke fouten, het systeem en nieuwe zondebokken', *Ramp en Recht*, Boom.

Rosenthal, U., Boin, R. A. and Comfort, L. K. ed. (2001), *Managing Crisis*, Charles Thomas Publishers, Springfield.

Rosenthal, U., Charles, M. and 't Hart, P. (1989), *Coping with crisis*, Charles Thomas Publishers, Springfield.

Sjöberg, L. (2002), 'Are received risk models alive and well?', *Risk Analysis*, pp. 665–9.

Slovic, P. (2000), *The Perception of Risk*, Earthscan, London.

Smit, H. (2001), 'Studentenpsycholoog krijgt steeds meer klachten, Drank, depressie en discipline', *NRC Handelsblad*, 14 April.

Starr, C. (1969), 'Social benefits versus technological risk', *Science*, Volume 165, pp. 1232–8.

TK (2001), 11510.

Universiteit van Tilburg (2002), Available online at: http://www.uvt.nl/faculteiten/frw/trom-l/j4n11/.

Vandendriessche, D. and Raskin, K. (2000), 'Zelfmoord aan de KU Leuven: onderzoek en beleidsimplicaties, Studeren aan de universiteit: levensgevaarlijk?', *Studentenweekblad van de Leuvense Overkoepeldende Kringorganisatie*, no. 16, 17 January.

Van Zundert, D. (2002), *Agressie en geweld in het onderwijs*, bijdrage in het kader van de vierde werkconferentie, georganiseerd door het platform Veiligheid en Geweld in de BVE-sector, 6 June.

Vlek, C. A. J. (1990), *Beslissen over risico-acceptatie: een psychologisch-besliskundige beschouwing over risicodefinities, risicovergelijking en beslissingsregels voor het beoordelen van de aanvaardbaarheid van riskante activiteiten*, The Hague.

Vlek, C. A. J. and Stallen, P. J. M. (1996), 'A Multi-level, Multi-stage, Multi-attribute Perspective on Risk Assessment, Decision Making and Risk Control', *Risk Decision Policy*, pp. 9–31.

Willemars, M. (2002), Available online at: http://www.edusite.nl/edusite/nieuws/10699.
Zandbergen, P. (1996), 'Zaak-Diekstra is testcase', *UT Nieuws, weekblad van de universiteit Twente*, Volume 31, Number 25, 5 September.

Supplementary material

The following supplementary material is available for this article:

- Appendix 1: Complete results of the nationwide risk survey questionnaire.
- Appendix 2: The report of the administrative working conference.
- Appendix 3: The Higher Education Safety and Security Audit.

This material is available as part of the online article from http://www.blackwell-synergy.com/doi/abs/10.1111/j.1468-5973.2006.00490.x (this link will take you to the article abstract).

Please note: Blackwell Publishing are not responsible for the content or functionality of any supplementary materials supplied by the authors. Any queries (other than missing material) should be directed to the corresponding author for the article.