UNIVERSITETET
I OSLO

Guide – Security

Threat Assessment

Guide for management on how to handle threats to UiO staff

Contents

Guide – initial threat assessment

1 Introduction

It is important to respond rapidly and in the right way in order to ensure that a threat is managed properly and correctly. It is important to remember that security is a management responsibility and that every manager is responsible for the security of their staff. The security adviser in the Unit for HSE and Emergency Preparedness (HMSB) can advise managers on how to manage a threat.

2 Preventing threats

Threats are ‘intentional acts’. In most cases, it is impossible to control what a threat-maker will do. Prevention must therefore focus on education, training and exercises on how to manage threats when they are made.

HMSB organises and holds courses and training activities designed to teach managers and staff how to manage threats and threat situations. Managers have a responsibility to ensure that they and their subordinate managers have the skills necessary to manage such incidents properly.

3 Understanding threats

3.1 What is a threat?

The term ‘threat’ is often used quite ‘broadly’ and thus also a little ambiguously. But, in order to ensure incidents are handled properly, we need to take a closer look at what a threat really is.

3.2 What does the law say?

The Penal Code says the following:

> *Section 263. Threats*
>
> *Any person who by words or conduct threatens to engage in criminal conduct under such circumstances that the threat is likely to cause serious fear shall be subject to a fine or imprisonment for a term not exceeding one year.*

and

> *Section 264. Aggravated threats*
>
> *Aggravated threats are punishable by imprisonment for a term not exceeding three years. In determining whether the threat is aggravated, particular weight shall be given to whether it was directed at a defenceless person, whether it was made without provocation or by multiple persons acting together, and whether it was motivated by the aggrieved person's skin colour, national or ethnic origin, religion, life stance, homosexual orientation or impaired functional ability.*

To the extent that a definition can be derived from the Penal Code, it would be something like:

'A threat = a statement, act or behaviour directed at someone that causes the recipient to feel serious fear.'

This tells us that, in the above circumstances, and as the law defines threats, threats are punishable by law. We will come back to how the legal aspects should be followed up.

In terms of threat management, this definition is not particularly helpful – other than telling you that the threat-maker can be reported to the police. However, fear is an emotion, and it affects different people in different ways. Some people are more resilient than others and may therefore have a higher threshold for calling an incident a threat. Others might have a life history or other baggage that means their sense of fear is triggered at the other end of the scale.

As a manager, you know your subordinates best and can make an objective assessment of the person concerned's 'fear scale'. This is an important element of threat management and any future follow-up of the threat-recipient.

3.3 What does the security specialist say?

As already mentioned, the term 'threat' is often used so broadly that it makes creating a management strategy difficult. Therefore, we need to focus in on what the term actually means. What is a threat, specifically?

'Threat = a specific statement (act or behaviour) involving an intention to do harm!'

This definition narrows what is meant by the term 'threat' and results in much of what are perceived to be threats not being defined as a threat, viewed from a threat management perspective. This notwithstanding, much of what falls outside this definition may still constitute criminal speech, acts or behaviour. These situations will, however, be managed differently to threats.

4 Classification

We use the categories 'threat', 'intimidation', 'provocation' and 'weighted reference' to classify the popular concept of a threat into categories one can distinguish between and manage. What distinguishes these from each other is the **intention**.

4.1 THREAT

A specific statement (act or behaviour) involving an intention to do harm to the threat-recipient/target of the threat.

A statement like *"I'm going to kill you!"* is a threat since the statement involves a clear intention to do harm to the threat-recipient. Threats are identified by examining the intention of the threat-maker.

There is also little question that such a statement would, objectively speaking, be likely to evoke fear in the threat-recipient. It would, therefore, also be punishable under section 263 of the Penal Code.

- Must be managed as a SECURITY THREAT and may require security measures
- Must be reported to the police (punishable under the Penal Code)

- Must be managed by a manager, with support from the Unit for HSE and Emergency Preparedness (HMSB) and the Department for Organisation and Personnel (AP)

4.2 INTIMIDATION

Intimidation involves an intention to scare, rather than to do harm to, the threat-recipient, or to influence the threat-recipient through fear.

Statements like *"If you don't retract that report, I will break your kneecaps!"* do not involve an intention to do harm, the intention is to get the threat-recipient to retract the report. The statement also gives the threat-recipient the option to avoid the harm by doing what the threat-maker wants. This is often called a 'conditional threat'.

Intimidation is often also apt to evoke fear. It would also be punishable under the Penal Code, even though it is not a security threat situation.

- Must be managed as FEAR MITIGATION – does not require security measures, although other follow-up may be required
- Should be reported to the police (punishable under the Penal Code)
- Must be managed by a manager, with support from the Unit for HSE and Emergency Preparedness (HMSB) and the Department for Organisation and Personnel (AP)

4.3 PROVOCATION

Provocation often involves 'hate speech'. This is experienced as unpleasant but it is not a threat since it does not involve an intention to do harm. Example: *"Bloody hell. You should be deported back to Ungabunga land you f...g j...s!"*

This type of speech is unpleasant and could conceivably also cause the target to feel a certain amount of fear. If it did, it might be punishable under sections 263 and 264 of the Penal Code.

- Hate, harassment, racism, sexism, discrimination, etc.
- Must be managed as UNPLEASANT incident – does not require security measures, although other follow-up may be required
- Consideration should be given to reporting it to the police if it is punishable under the Penal Code.
- Must be managed by a manager, with support from the Department for Organisation and Personnel (AP)

4.4 WEIGHTED REFERENCE

Weighted references are clear references to incidents expressed in a manner that means they are often perceived as threats. For example: *"Remember Utøya!"* Naturally, the context is important here and is an essential element of the assessment/classification.

This type of speech is unpleasant and could subjectively cause the target to feel a sense of fear. But here too, it does not involve an intention to do harm to the threat-recipient.

- Must be managed as UNPLEASANT incident – does not require security measures, although other follow-up may be required

- Consideration should be given to reporting it to the police if it is punishable under the Penal Code.
- Must be managed by a manager, with support from the Department for Organisation and Personnel (AP)

This guide only addresses threats from the perspective of security.

Intimidation, provocation and weighted references – and other unpleasant forms of communication – must be managed by the manager in consultation with the Department for Organisation and Personnel (AP).

5 Threat assessment (initial)

In order to start managing a situation, it is important to be clear about what you are actually going to be managing. As shown above, many things may feel like a threat without actually constituting one. Therefore, an initial threat assessment must be conducted by the manager in order to determine how the situation should be managed from here on.

In principle, an initial threat assessment is quite simple and mainly consists of answering three questions:

Is this a threat or just an unpleasant experience?
Is the threat credible?
How vulnerable/accessible is the threat-recipient?

5.1 Is this a threat or just an unpleasant experience?

Classify the situation as described in chapter 4. Is it a threat, intimidation or an unpleasant experience (security threat or not)? This question is designed to determine whether or not the threat-recipient is in potential physical danger or not.

> *To ensure assessments are comprehensive, this should be assessed as: Threat = HIGH, Intimidation = MODERATE, Provocation and weighted references = LOW*

5.2 Is the threat credible?

Very few threats are actually carried out. It is, therefore, important not to include likelihood as part of the assessment, for the time being. The aim here is to determine the extent to which the threat could be carried out/acted on.

- Would it be physically possible to carry out the threat?
- Is the threat-maker known, is there a history?
- Was the threat made in a credible manner?
- Is the threat specific?
- Does the threat-maker appear serious, sane, sincere?

Credibility is assessed as HIGH – MODERATE – LOW

5.3 Is there a time window associated with the threat?

Has the threat-maker specified a time factor in relation to carrying out the threat?

The purpose here is to assess how long one might have from the threat being made to it being carried out. This indicates the urgency of the work.

Has a time factor been specified for the threat?

Time factor ('degree of urgency") assessed as HIGH – MODERATE – LOW

5.4 How immediately vulnerable/accessible is the threat-recipient?

The purpose here is to assess the degree of immediate danger the threat-recipient might be in. If we know that the threat-maker is physically far away from campus and is threatening to "...strangle you!", the threat-recipient is not immediately accessible to the threat-maker.

If the threat-recipient works on a service counter, they are more accessible than they would be were they behind two locked doors.

Vulnerability is assessed as HIGH – MODERATE – LOW

5.5 Assessment

It is important to point out that these are rough assessments and, to some extent, qualified 'guesswork'. In principle, it is always better to overreact in the immediate phase rather than play down the risk. Give the threat-maker every benefit of the doubt such that assessments are adjusted upwards in the absence of confirmatory information that would lower the overall assessment's severity.

This is an initial assessment designed to allow management of the immediate phase after a threat has been made. This assessment can easily be reassessed as more information is obtained and the situation becomes clearer.

5.6 Assessment matrix

Factor	HIGH	MODERATE	LOW
Threat factor			
Credibility			
Degree of urgency			
Degree of vulnerability (at this precise moment)			

6 Threat management

If your assessment is that we face a THREAT and it is CREDIBLE – it must be managed with a focus on security.

It is important to understand that incidents in all four categories require action on the part of the manager – but that actual threats require getting HMSB involved and a security mindset. This guide was produced with this in mind.

6.1 Immediate action points

6.1.1 Assess: Does the threat constitute an immediate danger?

This means to both the threat-recipient and any other people in the same situation (for example, everyone working in the same office/reception area, etc.).

Action points:

Call the police on 112	• In case of immediate danger, call the police! 112 • Next notify the Security Operation Centre (VAS) by calling +47 22 85 66 66 (or use any VAS panic buttons) – inform VAS whether or not the police have been called
Secure the premises	• Lock the doors, check perimeter protection • Inform the staff

6.1.2 Report the incident

Ensure the necessary agencies are informed of the incident

- WHAT has happened?
- WHERE did it happen?
- WHO was involved?
- WHEN did it happen?
- What have you done so far?

Action points

- Notify the Security Operation Centre (VAS) by calling +47 22 85 66 66
- Notify the unit's manager
- Notify the unit's local emergency preparedness coordinator

6.1.3 Assess and implement local protection

Assess the need to implement immediate local security measures. Implement the necessary measures immediately. If you are unsure, it is better to implement too much than too little. It is easier to deescalate later.

Consider the following security measures:

- Lockdown the premises, lock the doors. VAS can help to 'lock' card readers.
- Presence of security guards (ordered from VAS). This can have both a protective effect and a morale boosting effect for staff, since the presence of security guards can be reassuring
- Closing the department if it is open to the public (reception areas, student information, etc.)
- Consider other local security measures, preferably in consultation with the unit manager, HMSB and local emergency preparedness coordinator

6.1.4 Shield the threat-recipient

This must be done for both security and psychosocial reasons.

Find suitable premises for the threat-recipient, both to shield the person and to be able to meet and talk with the police, security guards, security adviser as part of the continued immediate threat management. Also consider posting another member of staff there to be present as ‘moral support’.

Avoid serving caffeinated or sugary drinks but ensure that there is drinking water in the room.

6.1.5 Ensure the effective assembly and interaction of responding resources.

- Prepare to receive the police/security guards. Send someone to meet them.
- Assemble the necessary resources such that they are available to the police, HMSB, local emergency preparedness management and others.
- Ready meeting premises and any waiting areas for the responding resources.

6.1.6 Contribute to good information gathering and a good situational picture.

Use the form for recording threats as a starting point.

Help the threat-recipient complete it – helpful for the police/VAS/HMSB/local emergency preparedness management team.

6.2 Intermediate phase

In many ways, the manager must tackle the initial phase on their own since other resources will not necessarily be physically or immediately available for support. Support will eventually arrive, and the threat management will transition into a sort of intermediate phase.

The responding resources who can help the manager make a more thorough assessment of the threat and its subsequent management could be, for example: VAS, CSIRT, HMSB, the police, the unit’s senior manager and the unit’s emergency preparedness coordinator. In this phase, the manager can also get support from the Department for Organisation and Personnel (AP) and the Occupational Health Service (BHT).

In this phase, it is important that the manager both maintains a focus on the threat-recipient, in relation to follow-up, care and support, while actively contributing, personally and via subordinate resources, to further analysis and management of the actual threat.

This includes:

- Actively contributing information and input to threat analyses and VTS analyses
- Providing the resources necessary to conduct threat analyses and VTS analyses
- Implementing the security measures deemed necessary in the unit and in relation to the threat-recipient
- Assisting with information for reporting the incident to the police

6.3 Post-incident work

Once the security of the staff member(s) has been ensured, the manager has to produce a plan for following up the threat-recipient.

This includes:

- Operating and following up and evaluating security measures that have been implemented in the unit
- Following up and evaluating security and protection measures that have been implemented for the threat-recipient
- Psychosocial follow-up, with support from AP and BHT

7 References

- Policy for threat management
- Procedure for threat management
- Form for recording threats
- Checklist for threat-recipient
- Checklist for manager of threat-recipient
- Online course: Threat management for managers

8 Explanation of concepts

AP	Department for Organisation and Personnel
BHT	The Occupational Health Service
CSIRT	The University of Oslo Computer Security Incident Response Team
HMSB	Unit for HSE and Emergency Preparedness
Security	Security
Security threat	Here: potential danger to life and heath
Target of the threat	The person towards whom the threat is directed. Someone else may be the actual receiver of the threat.
Threat-recipient	The person who receives or who is the target of the threat.
Threat-maker	The person making the threat
VAS	Security Operation Centre (our security centre which is manned around the clock)
VTS (analysis)	Model for risk assessment based on the factors Value-Threat-Vulnerability (NS 5832)

9 Resources

Security Operation Centre (VAS)
https://www.uio.no/english/about/organisation/los/ea/facilities/supports/security/index.html

Unit for HSE and Emergency Preparedness (HMSB)
https://www.uio.no/english/about/organisation/los/ehms/index.html

UiO CSIRT https://www.uio.no/english/services/it/security/cert/index.html

Department for Organisation and Personnel (AP) https://www.uio.no/english/about/organisation/los/ap/index.html

The Occupational Health Service Unit (BHT) https://www.uio.no/english/for-employees/employment/hse/ohsu/