Safeguarding your group: a checklist

Your group could come under attack. For example:

- Damaging allegations are reported in the media.
- A disaffected member destroys vital files.
- Core funding is suddenly withdrawn.
- A key member is arrested.
- Confidential materials are leaked to critics.
- The group is sued.
- Key members leave — due to conflict or poor health — without sharing their knowledge.
- Forged correspondence is used to cause distrust.

It is worthwhile preparing for such contingencies. This checklist is designed to help assess the group's capacity to resist and survive attacks.

The focus here is on attack, subversion and undermining. The checklist does not cover conventional risks such as fire and poor investments. Theft for the thief's personal gain is a conventional risk. A less conventional risk is theft designed to cause disruption. Of course, preparing for unconventional risks such as subversion may help against conventional risks.

There are five sections.

1. Materials. Groups have many files that are important to protect or preserve. The focus is on information, not physical equipment.
2. Networks. Having strong links to other groups can help in resisting attacks.
3. Plans. It's important to be prepared for possible threats.
4. Skills. These are vital for responding to attacks.
5. Organisational dynamics. A well-functioning group is better able to withstand attacks.

The material here is a rough template rather than a detailed guide. You know your group and therefore are in the best position to fill out the template. The key thing is to think of possible threats and then of ways to prepare your group to deal with them.

1. Materials

Materials to ***protect*** are things that you don't want outsiders, especially hostile outsiders, to obtain. This might include membership lists, confidential information about individuals and passwords for bank accounts.

Materials to ***preserve*** are things needed for the group's effective operation. It doesn't matter so much if others obtain these materials. The key goal is to prevent them from being destroyed. They might include membership lists, photos and written documents.

a. List all materials to protect or preserve. Include electronic, paper and other materials.

b. Rate their importance by one of these categories:

- Essential: the group cannot function if this material is compromised.
- Vital: the group's operations are seriously damaged.
- Important: the group is hurt but can continue moderately well.
- Not so important: the group is hindered a little.

c. List methods by which the material is protected from (a) external threats and (b) internal threats.

- Where: what is the physical or virtual location (in general terms)?
- How: for example, encryption of correspondence; use of pass-words; back-up copies
- When: how often are measures implemented?
- Who: who is responsible?

d. On the basis of this assessment, develop a plan to better safeguard your materials.

A sample table of material to protect or preserve

Materials	Type	Importance	Threats	Response	Where	When	Who
Membership list	Electronic	Vital to preserve	Confiscation of computers	Copies emailed	Computers of office bearers	Monthly	Secretary
Credit cards	Plastic	Important to protect	Theft; loss	Prepare for e-banking		Next week	Treasurer
Old posters	Printed	Important for morale	Theft	E-copies	Interested members	Next 3 months	Photographer

2. Networks

If your group has strong links with other groups and individuals, then you are in a much stronger position to resist and survive attacks. Strong networks may help deter attacks in the first place.

The most useful networks depend a lot on the nature of your group and what threats you're considering. The basic principle for assessing networks is to imagine the ideal network and then compare your actual network to it.

a. List the categories of groups/individuals that would help your group resist and survive attacks. Some prime categories are:

- legal, including lawyers who can advise and, if necessary, defend you
- media, including journalists and editors who can help publicise your views
- same-sector groups (for example, if you are an environmental group, this means other environmental groups)
- activists and campaigners, who can help you develop plans and carry out actions
- political, such as politicians or senior officials who can present your case to high-level decision-makers
- other (depending on your situation)

b. Take account of local, national, international and virtual networks.

c. For each category, list the strength of your network connections. Strength is measured by the number of contacts and their willingness to act on your behalf.

nonexistent: you don't know anyone in this category

- weak: you know one or two individuals, but whether they would help is uncertain
- medium: you have a reasonable prospect of obtaining some assistance
- strong: you have powerful or energetic supporters
- embedded: members of your own group are in this category (for example, some of your members are lawyers or journalists)

d. On the basis of this assessment, develop a plan to strengthen your networks.

- create new contacts
- strengthen links with existing contacts
- develop skills and experience of embedded contacts

A sample table of network assessment

Network category	Locality	Rating	Details	Plan	When	Who
Legal	Local	Medium	Know several lawyers: [names]	Strengthen ties with these lawyers	next 3 months	[name]
Media	Local, national, international	Embedded and strong	One member is freelance journalist; know several other journalists			
Disability (same sector)	Local, national	Strong	Regular contact with several groups			
Activists		Non-existent		Contact several activist groups	asap	[name]
Political	local	Weak	One politician might be willing to help	Ask politician for suggestions	next month	[name]

3. Plans

Your group should have specific plans to deal with the most likely threats, and general plans to deal with unlikely ones.

a. List the most likely threats, for example theft of materials, arrest of members, destruction of files, circulation of damaging stories and subversion by a hostile member.

b. Assess your plan for each threat by key questions, such as:
- Do you have a plan?
- Is the plan detailed or vague? Is the plan narrow/specific or flexible?
- Is the plan widely understood?
- Have you practised executing the plan?
- Are members ready and willing to carry out the plan?

c. On the basis of this assessment, take steps to improve your plans.
- develop plans
- improve existing plans
- practise executing plans

A sample table of plan assessment

Threat	Plan?	Detail level	Understanding	Execution	What to do	When
Theft of materials	Yes	Highly detailed	By key members only	Good readiness, no practice	Practise executing plan	Within next year
Arrest of key members	No				Develop plan	Next 3 months
Damaging stories in media	Yes	General approach	Good understanding due to previous experience	Good readiness, previous experience	Make plan more detailed	Next 3 months
Destruction of files	Yes	Highly detailed	By key members only	Good readiness, no practice	Practise executing plan	Within next year
Internal dissension	No		Problem well understood!		Develop plan	next month

4. Skills

The greater the skills of your members, the better able your group will be to resist and survive attacks. Furthermore, groups possess collective wisdom, greater than the sum of individual wisdom. Also relevant are skills in the group's network. (The word "skill" is used here to include knowledge, understanding and wisdom.)

a. List the key areas of skill for your group. Examples are:
- Information technology
- Filing, information management
- Writing
- Public speaking
- Networking
- Organising (meetings, rallies, etc.)
- Analysis of problems
- Strategic planning
- Emergency response

b. For each area, assess your group's capacity using questions such as:
- What is the level of skill in the group? What about in the group's network?
- How dispersed is the skill? Is it held by just one or two people, or widely shared?
- How easily can the skill be shared with others?

c. On the basis of this assessment, take steps to improve your skills.
- current members acquire skills
- recruit new members with skills
- practise using skills

A sample table of skill development

Skill	Level	Dispersal	Ease of sharing	What to do	When	Who
Computing	High	One expert only	Easy for some tasks, difficult for others	Share skills with others	Over next year	Expert and volunteers
Public speaking	Low	Little experience		Encourage members to practise	Next 6 months	Volunteers
Organising	High	Wide across group	Basics are already widely shared	n/a		

5. Organisational dynamics

If your members work well as a group, are highly committed to each other and to the group's purpose, and can make decisions efficiently, then the group is better able to resist attacks.

a. List the key areas of organisational dynamics for your group. Examples are:

- Trust
- Decision-making
- Equality
- Resilience
- Moods

b. For each area, assess your group's capacity using questions such as:

- Trust. Can members rely on each other to get things done? When does distrust undermine the group's effectiveness?
- Decision-making. Can decisions be made promptly, sensibly, unclouded by special agendas or wishful thinking, with many people participating?
- Equality. Is there dependence on a few people at the top, or does everyone have a similar stake in the group?
- Resilience. Can the group continue to function well if key people are not present?
- Moods. Are members optimistic or pessimistic? Are they happy or depressed? Do they feel full of energy or depleted?

c. On the basis of this assessment, take steps to improve your dynamics. This is seldom easy: a rethinking of processes and assumptions may be required. Having an outside adviser may help.

This checklist was developed by Schweik Action Wollongong, a small voluntary group in Wollongong, Australia, fostering awareness of nonviolent responses to aggression and repression.

The group is named after the fictional character Schweik (or Svejk), a soldier who created havoc in the Austrian army during World War I by pretending to be extremely stupid. See Jaroslav Hasek, *The Good Soldier Svejk and His Fortunes in the World War* (Penguin, 1974).

This version 2 September 2006. Please send us your suggestions for improving the checklist.

Contact us at PO Box U129, Wollongong NSW 2500

Phone
02-4228 7860 (Brian)
02-4229 9369 (Sharon)
02-4226 3584 (Yasmin)

Email
bmartin@uow.edu.au (Brian)
sharmary@1earth.net (Sharon)

See http://www.uow.edu.au/arts/sts/bmartin/others/SAW.html (or put "Schweik Action" into Google) for more information and copies of our articles.