

LIST OF OFFICE CAPACITIES AND VULNERABILITIES IN THE FILM

	Capacities	Vulnerabilities	Notes
Environment / Location			
Type of road	*		Main road – generally this is positive (good access, neighbours etc) but depends on context. Some organisations may prefer to be located in a quieter area (where it may be harder for surveillance to operate)
Public transport	*		Metro nearby – good and (probably) safe transport for organisation's workers and beneficiaries
Cafe / snack bar next door	*	*	Neighbouring cafe workers may become friends and advise HRDs of any suspicious activity in area. (Or cafe workers may be threatened or bribed to inform against the HRDs)
Street lighting		*	No street lights visible; attacks more likely in the dark.
Located in business district	*	*	Depends on context which location is safest – but offices in more isolated areas are more vulnerable to attack.
Building structure			
Walls, roof	*		Solid structure
Front door	*	*	Front door is solid, but it is kept open.
Technology		*	No technology. * CCTV can be an asset if it is appropriate (ie if it is normal for organisations in this region to have this level of security) and if it is properly monitored
Stairs and lift	*	*	* Good to have a lift as well as stairs (2 exits) * There is no access from the street for people with disabilities.
Stairs and lighting		*	Poor lighting on the stairs – note that physical attacks in stairwells are common in some countries

Resource 7: List of Office Capacities & Vulnerabilities in the Film

	Capacities	Vulnerabilities	Notes
Office structure			
Office front door – double door very strong	*	*	Good door but the time it takes to lock / unlock it could make someone vulnerable.
No spyhole inside door to check visitors		*	
Windows		*	No bars at windows. It depends on the context whether they are needed.
Office practices / procedures			
Staff awareness and training		*	Overall it is clear that there is no awareness of risk, and no practices to reduce risk
Sign with name of organisation	*		This can be taken down very quickly if a threat is made against the organisation and it would be better if their location was not easy to find
Door		*	<ul style="list-style-type: none"> * Door is sometimes left open * Some HRDs say that their best defence is being 100% open including keeping their door open, BUT * if there is a risk of attack, robbery etc, it is best to have a strong door, and keep it closed / locked * beneficiaries of an organisation will appreciate that security precautions are taken
List of emergency numbers	*	*	* Good if the list is kept up-to-date and does not contain information that could be misused (eg here the Chairperson's mobile number)
List of what to do in case of a search of the office	*		<ul style="list-style-type: none"> * If a police search of the office is a likely risk, then training the office workers and having a reminder note visible can be a good thing, depending on context. * There might also be some additional actions personnel may take in this situation which may be in security guidelines but not pasted on the wall!
Guard	*	*	<ul style="list-style-type: none"> * There is a guard * The guard has no duties or visibility, so is virtually useless
Fire extinguisher	*	*	<ul style="list-style-type: none"> * Good to have an up-to-date fire extinguisher * It should be easily accessible (and not in the bathroom!)

Resource 7: List of Office Capacities & Vulnerabilities in the Film

	Capacities	Vulnerabilities	Notes
Visitors policy		*	<p>* There is no policy for how to deal with visitors, such as:</p> <ul style="list-style-type: none"> - checking name, organisation, purpose in visiting - having a waiting area where there is no access to computers, confidential materials or items and where visitor cannot overhear confidential conversations - having a policy of escorting the visitor to the person being visited (so no opportunity to steal or plant anything) - visitor escorting also applies to family members and friends - whose visits should anyway be discouraged - if visit by service engineer (phone, power, water, etc), verify that there is a fault, check their identify and verify identity with their company - monitor service engineer at all times
Visitor book for signing	*	*	<p>* It is usually good practice to have a list of who is in the office at any time</p> <ul style="list-style-type: none"> - and keep a note that visitors arrive and leave as appropriate <p>* If visitors include vulnerable people (eg survivors, witnesses etc) then the book might contain information putting people at risk. In this case consider options such as: a) code names for vulnerable witnesses; b) special arrangement; c) visitor's list be encrypted and stored on secure computer</p>
Keys		*	<p>There is no key policy. A key policy should include:</p> <ul style="list-style-type: none"> * number of copies of keys strictly controlled * keys are colour coded, not labelled * keys are kept in locked box with access only by named persons * workers report immediately lost or stolen keys; locks should be changed * also change locks when a key-holder leaves the organisation
Information management policy		*	<p>* There does not appear to be an information management policy. This could include:</p> <ul style="list-style-type: none"> * regulating access to and usage of confidential material (and also its format - eg electronic data only) * Regulation of types of information not to be disclosed, eg home addresses of organisation members, telephone numbers, location, etc
Taking work home		*	<p>Receptionist takes the 'Confidential' files home, which can lead to:</p> <ul style="list-style-type: none"> * endangering clients * endangering HRD's family if very sensitive material is stored at home

Resource 7: List of Office Capacities & Vulnerabilities in the Film

	Capacities	Vulnerabilities	Notes
Computer screens, shutdown mechanisms etc	*	*	Direction of screen is good as computer screens visible through a window could be surveilled. But computer is visible to the guard and any visitors. There is no sign of use of a screen shutdown when leaving the computer unattended.
Office relationships	*	*	* Disgruntled employees can be a great threat * There are no overt signs of disharmony here, but the guard does not look after the receptionist, the receptionist does not look after the director and the director does not look after the workers (she has not organised any training of the staff in security issues)
Other issues in film:			
Medicins Sans Frontieres (Doctors Without Borders - MSF) upstairs	*		The presence of an international human rights organisation Medicins Sans Frontieres as a neighbour upstairs is a great capacity because plans and resources for security can be shared
Issues related to office not covered in the film			
Local crime rate			Security measures should be appropriate to risk.
Basic services: electricity, water, telephone etc			
Gates & fences			As appropriate - keep in good repair
Threat of bombing including suicide bombing			* Install steel rods at access points to block vehicles * Clear policy on how to deal with parcels * Installation of x-ray machine for bags etc, if appropriate
Vehicle parking			If no secure parking, consider risks to vehicles of planting of tracking devices, explosive devices etc and take appropriate precautions
Landlord			Know who the landlord is and their background - do they have access, or will they give access to attackers to search, steal or plant items?
Infiltration of the office			* Offices may be infiltrated by government agents * Try to avoid this by careful recruitment practices * If it cannot be avoided, contain the infiltration by sharing information on a need-to-know basis