Risk assessment basics [foundational material]

Introduction

We assess our risk all the time. This is how we survive. It is a process that is not unique to digital and/or information security.

When take a walk at night on a quiet street, we make decisions about which side of the street to walk on, how to behave, what to prepare, how to walk, based on our understanding of the situation: *Is this street known for being a dangerous one? Is the community where this street is a dangerous one? Do I know anyone on this street who could come to my aid? Can I run fast, if something happens? Am I carrying anything of value that I can bargain with? Am I carrying anything that can put me in greater harm? Which part of this street can I walk on to avoid possible harm?*

When our organisations plan a new project, we consider the ways in which it could fail. We make design decisions based on what we know of the context and the factors in it that would lead to the project not achieving its goals.

When we organise protests, we look at ways to keep the protest and those in it safe. We organise buddy systems. We make sure there is immediate legal support in case of arrests. We instruct those attending about how to behave to avoid being harassed by authorities. We strategise ways in which to conduct a protest peacefully in order to lessen the risk to those participating. We have people in the protest whose responsibility is to maintain its safety.

While assessing our own risks may be a practice that we do instinctively, risk assessment is a specific process we undergo – usually as a collective – in order to know how we can avoid threats and/or respond to those threats.

Risk assessment: Online and offline

Assessing our risks online is not as instinctive, for various reasons. Many of us do not understand how the internet works and where its threats and risks are – and these continue to evolve and grow. Some have the attitude of perceiving online activities, actions and behaviour as not being “real”, with less serious effects than what happens to us physically. At the other end of the

spectrum, those that know of or have experienced incidents where a person's "real" life was affected by their online activities (people being scammed on dating sites, people whose taboo internet interactions were made public, or activists being arrested for saying something against their government) tend to have a paranoid view of the internet.

The reality is that for many activists, the online/offline binary is false. The use of digital devices (mobile phones, laptops, tablets, computers, etc.) and internet-based services, apps and platforms (Google, Facebook, Viber, Instagram, WhatsApp, etc.) is commonplace in the work of many activists – in organising and in advocacy work. How we organise and do our work as activists has evolved as technology has advanced and developed – and will continue to do so. The internet and digital technologies are a critical part of our organising infrastructure. We use them in communicating, organising activities, building our community, and also as a site of our activities. In-person gatherings and advocacy events are often accompanied by online engagement, especially on social media and through hashtags. In recent protest movements, there is often a seamless flow between online and offline mobilising, organising and gatherings.

Instead of perceiving what happens on the internet as something separate from our physical realities, think of offline <-> online realities as interconnected and porous. We exist in both, most of the time, at the same time. What is happening in one affects how we are in the other one

This also means that the risks and threats move from online to offline and vice versa. For example, advanced state surveillance strategies against activists and their movements exploit un-secure use of technologies (i.e. clicking on unverified links, or downloading and opening unverified files) in order to be able to gather more information about activists and their groups and movements that may eventually lead to physical surveillance. Anyone who has experienced online gender-based violence (OGBV) knows the psycho-social effects of such attacks and harassment. There have also been cases where OGBV has escalated to affecting the physical security of those who have been targeted. Different forms of OGBV (stalking, doxxing, harassment) have been tactics used against feminist and queer activists in order to threaten them into silence and compliance.

Thinking about the porous online <-> offline nature of threats and risks can be overwhelming – *where do we begin assessing and knowing what the threats are and where they are coming from, and strategising what to do about them?*

What is risk assessment?

Risk assessment is the *beginning of a process* to become more resilient in responding to changing contexts and threats. The purpose of assessing risk is to be able to come up with strategies and tactics to mitigate the risks, and to be able to make more informed decisions.

In general terms, risk is the exposure to the possibility of harm, injury or loss.

In risk assessment, it is the capacity (or lack thereof) of an individual/organisation/collective to respond to the impact(s) of a realised threat, or the capacity of an individual/organisation/collective avoid a threat from being realised.

There is a known formula for risk assessment:

Risk = threat x probability x impact/capacity

Wherein:

- Threat is any negative action aimed towards a person/group.
  - Direct threats are declared intention to cause harm.
  - Indirect threats are those that happen as a result of a change in a situation.
  - In defining threats, it is important to identify where the threat is coming from. Even better, who is the threat from.
- Probability is the likelihood of a threat becoming real.
  - A related concept to probability is vulnerability. This can be about location, practice and behaviour of the individual/group that increase the opportunities for a threat to be realised.
  - This is also about the capacity of the groups/individuals that are making the threat, especially in relation to the individual/group that is being threatened.
  - To assess probability, ask if you have real examples of a threat happening to someone or a group that you know – and compare that situation with yours.
- Impact is what will happen when the threat is realised. The consequences of the threat.
  - Impact can be on the individual, organisational, network or movement.
  - The higher the degree and number of impacts of one threat, the greater the risk.
- Capacities are skills, strengths and resources a group has access to in order to either minimise the probability of the threat, or respond to the impact of the threat.

image-1605451259399.png
Image not found or type unknown

Case study - threats and mitigation

Case study: Deya

To illustrate this, let’s use the fictional but fairly common experience of Deya. Deya is a feminist activist who uses her Twitter account to call out those who promote rape culture. As a result of this, Deya has been been harassed and threatened online.

The threat she is most concerned with are the people that promise to find out where she lives and share that information on the internet to invite others to cause her physical harm. In this case, the impact is clear – physical harm towards Deya. There are other threats such as harassing her employers to fire her from her job, and to harass her known friends online.

To do risk assessment, Deya will have to go through these threats and analyse them to assess their probability and impact – in order to plan how she can mitigate her risks.

Threat 1: To find out where she lives and share that information online

Most of the threats come from accounts online – most of whom she does not know, and cannot verify if they are actual people or fake accounts. She recognises a handful of those participating in these online threats as known actors who often take part in attacking women online. Based on her knowledge of their previous attacks, she knows that personal details have sometimes been published online, and this has created a real sense of fear for her personal safety.

Is there are a way for her to prevent this from happening? How likely is it that her harassers and attackers will find out where she lives? She needs to figure out how likely it is that her address is either already available on the internet or can be made available by one of her attackers.

In order to assess this, Deya can begin by doing a search for herself and the information that is available about her online – to see if there are physical spaces that are associated with her, and if these will point to her actual physical location. If she discovers that her home address is available on the internet, is there something she can do about it? If she discovers that her address is currently searchable on the internet, then what can she do to avoid having it publicly available?

Deya can also assess how vulnerable and/or secure her home is. Does she live in a building with guards and protocols for non-tenant access? Does she live in an apartment that she has to secure on her own? Does she live alone? What are the vulnerabilities in her home?

Deya will also have to assess her own existing capacities and resources to protect herself. If her home address is made public on the internet, can she move locations? Who is available to offer her support during this time? Are there authorities that she can call on for protection?

Threat 2: To harass her employers to get Deya fired from her job

Deya works for a human rights NGO so there is no threat of her being fired from her job. But the organisation’s office address is publicly known in her city and available on their website.

For Deya, the threat of being fired from her job is low. But the publicly available information about her NGO may be a vulnerability to Deya and the staff’s physical security.

In this scenario, the organisation must do their own risk assessment as a result of the threats being faced by one of their staff.

What to do with risks? General mitigation tactics

Beyond identifying and analysing threats, probability, impact and capacities, risk assessment also deals with making a mitigation plan for all the risks identified and analysed.

There are five general ways to mitigate risks:

Accept the risk and make contingency plans

Some risks are unavoidable. Or some goals are worth the risk. But it does not mean that they can be dismissed. Contingency planning is about imagining the risk and the worst case impact happening, and taking steps to deal with it.

Avoid the risk

This means decreasing the probability of a threat happening. This may mean implementing security policies to keep the group more secure. This could also mean behavioural changes that will increase the chances of avoiding a specific risk.

Control the risk

Sometimes, a group may decide on focusing on the impact of a threat and not on the threat itself. Controlling the risk means decreasing the severity of the impact.

Transfer the risk

Get an outside resource to assume the risk and its impact.

Monitor the risk for changes in probability and impact

This is usually the mitigation tactic for low-level risks.

Case study: Deya

To use Deya’s example again, she has options about what to do with the risks she is facing based on her analysis of each threat, the probability of each threat happening, the impact of each threat, and her own existing capacities to handle the threat and/or the impacts of the threat.

In a scenario where Deya’s home address is already searchable on the internet, the risk will have to be accepted and Deya can focus on making contingency plans. These plans can range from improving the security of her home to moving homes. What is possible will depend on Deya’s existing realities and contexts.

The other option for Deya in this scenario is to ask where her address is publicly available to take down that content. But this is not a foolproof tactic. It will help her avoid the risk if none of her harassers have seen it. But if some have seen it and taken a screenshot of that information, then there is very little that Deya can do to stop the information from spreading.

In a scenario where Deya's address is not publicly known and available on the internet, there is more breathing room to avoid the risk. What can Deya then do to prevent her home address from being discovered by her harassers? Here, she can take down posts that are geo-tagged that are close to her home, and stop posting live geo-tagged posts.

In both scenarios (about her address being publicly available or not), Deya can also take steps to control the risk by focusing on protecting her home.

Good risk mitigation strategies will involve thinking about preventive strategies and incident response – assessing what can be done in order to avoid a threat, and what can be done when the threat is realised.

Preventive strategies

• What capacities do you already have in order to prevent this threat from being realised?
• What actions will you take in order to prevent this threat from being realised? How will you change the processes in the network in order to prevent this threat from happening?
• Are there policies and procedures you need to create in order to do this?
• What skills will you need in order to prevent this threat?

Incident response

• What will you do when this threat is realised? What are the steps that you will take when this threat happens?
• How will you minimise the severity of the impact of this threat?
• What skills do you need in order to take the steps necessary to respond to this threat?

image_1605451259399.png
Image not found or type unknown

Reminders

Risk assessments are time-bound

They happen within a specific time period – usually when a new threat emerges (e.g. change in government, change in laws, changes in platform security policies, for example), a threat becomes

known (e.g. online harassment of activists, reports about activists' accounts being compromised), or there is a change within a collective (e.g. a new project, new leadership). It is important, therefore, that risk assessments be revisited, because risk changes as threats emerge and disappear, and as the ability of a group and individuals within that group to respond to and recover from the impact of a threat changes.

Risk assessment is not an exact science

Each person who is part of a group that is undergoing a risk assessment process comes from a perspective and a position that affects their ability to know the likelihood of a threat to be realised, as well as their own capacities to either avoid a threat or respond to the impact of it. The point of risk assessment is to collectively understand these different perspectives within the group, and have a shared understanding of the risks they face. Risk assessments are relative. Different groups of people may face the same risk and threats, but their ability to avoid those threats and/or their ability to respond to the consequences of the threats differ.

Risk assessment will not ensure 100% safety, but it can prepare a group for threats

As there is no such thing as 100% safety and security, risk assessments cannot promise to guarantee that. What they can do is to enable an individual or a group to assess the threats and risks that can potentially affect them.

Risk assessment is about being able to analyse risks that are known and are emerging, in order to figure out which risks are impossible to predict

There are different types of risks:
• Known risks: Threats that have already been realised within the community. What are their causes? What are their impacts?
• Emerging risks: Threats that have occurred but not within the community that the person belongs to. These could be threats that result from from current political climates, technological developments, and/or changes within the broader activist communities.
• Unknowable risks: These are threats that are unforeseeable and there is no way of knowing if and when they will emerge.

Risk assessments are important in planning

They allow an individual or group to look at what will cause them harm, the consequences of those harms, and their capacities to be able to mitigate the harms and their consequences. Undergoing a risk assessment process allows groups to make realistic decisions about the risks they are facing. It allows them to prepare for threats.

Risk assessment is way to manage anxiety and fear

It is a good process to go through to unpack what people in a group fear – to create a balance between paranoia and complete lack of fear (pronoia), so that, as a group, they can make decisions about which risks to plan for.

Revision #2
Created 18 April 2023 04:29:00 by Kira
Updated 27 June 2023 13:38:22 by Kira