GISF Virtual Launch Event | Questions and Answers | April 2020

Green: Answered by panel during event
Navy: Answered in chat during event
Blue: Answered by panel after event

- *So Steve, do you think Security risk management systems should be stress tested to see if they will actually work when they are needed? Should teams in the field be regularly tested with contingency plans to see if they will follow them when required? Perhaps using a hypothetical scenario to see how they respond?*

Hugh King: I believe so. SRMs are no different to Business Contingency plans. They are only as good as the most recent review, stress test and adaption.

Steve Dennis : The question: "Steve, do you think Security risk management systems should be stress tested to see if they will actually work when they are needed?" In a calibrated way, yes. There are professional ways to run a simulation to achieve high results of learning… and there are ways to traumatize your staff instead. The first is better.

Steve Dennis: to get an individual or team up to the desired level of knowledge, skills and attitude towards something like a contingency plan, yes, exercises/simulations could be an effective tool, when done correctly. One wouldn't send a fire-fighting student on their first day to tackle a large blaze, but rather a little ramp up to realistic scenarios would be a more appropriate approach before the final exam. Also, too little stress, and the participants may relax too much to learn. Too much stress and you risk the associated trauma distracting the learning. Too many times contingency plans are being learned in the emergency, not before, and that is critical time wasted.

As for teams have regular testing of contingency plans? If a response to an incident requires three elements, being plans, resources and skills, trying out a contingency plan may highlight shortcomings in the appropriateness of the plans to likely risks, the expiry or non-existence of essential resources (human or other) as well as shortfalls in skills. Also, practice may increase skill levels too.

Lastly, staff in this industry move to different organizations a lot. People remember good examples of planning and preparedness and can be agents of positive talent exchange to bring that culture elsewhere.

- *Steve - you mentioned the importance and influence on focus in relation to stress - are you able to expand on this, and perhaps discuss wellbeing and what you consider still needs to be done in the wider humanitarian and development sector?*

Steve Dennis: To the question, "Steve - you mentioned the importance and influence on focus in relation to stress - are you able to expand on this…?" Yes: As an emergency

manager, I find 10% of my time is spent on setting and meeting objectives and 90% of my time supporting teams to avoid the things that stop them from performing well. If someone doesn't have confidence in the way their security risk management is implemented, then they are distracted from achieving their humanitarian objectives. I've been in projects where multiple people resigned due to lack of confidence in the SRM, and I can only do the math that in the months before those moments, those people (and many more people) were not focused on their work.

Steve Dennis: As for what specifically still needs to be done? A greater mindfulness in organizations' leadership that with proper SRM, you are not only lining yourselves up to have better outcomes in incident likelihood and impact, but also your staff will be able to focus better on their work for better outcomes there too.

- How do we overcome the situation were security has traditional been seen as an almost separate unit within an organization, while it should be incorporated within all sections of an organisation, it should be an enabler of programmes, not a barrier.

Answer: This is a problem that has existed for so long and continues to persist. I think the growing recognition that it is Security Risk Management rather than security management helps but many organisations still struggle with where SRM should fit within their structure, we see it under programmes, audit, human resources. This doesn't help with creating a sector wide understanding of who we are and what we do. GISF makes an effort to reach out to and work with organisations that focus on other areas to try and help break down some of the barriers, for example CHS on human resources, wellbeing and safeguarding. We are also planning a series of webinars aimed specifically at crossing some of the silos. Any specific suggestions would be most welcome.

Steve Dennis: I think two things are essential to have security and safety risk management incorporated in the culture of an organization: Individual buy in and top level leadership. I've experiences teams that were involved in identifying risks in their units/departments were more invested in the measures to reduce probability and impact. This comes out in project proposal staff asking for conversations with safety/security staff on 'how can we?' instead of 'is this okay or not?' Secondly, for risks that are known through macro data (ex organization wide road traffic accidents) that might inform individual project behaviour (adhering to speed and seatbelt policies), leadership that explains why and what enforcement is required is essential.

- Security risk managers are often accused of creating a risk adverse culture within organisations, and the sector as a whole, how do we get the balance right?

Answer: I think this follows on from the question above. With a lack of understanding of what we do and where we sit, this allows perceptions, such as being risk averse, to flourish.

From Steve Dennis: The analogy of 'how' to operate in Ebola clinic can be used to bridge the logic-disconnect. There is no question, we must intervene with Ebola, but experts in infectious disease must describe 'how' we do it. Similarly, we are driven by humanitarian imperatives to intervene in high security risk environments, so security risk experts must describe the 'how' to go.

From Fredrik Pålsson: The humanitarian imperative of delivering support to those most in need should be the cornerstone of any security risk assessment, and as such will involve a level of exposure and vulnerability. It is built on as little risk as possible to allow program activities to happen. A security plan has to enable the program to happen. Staff implementing security protocols need to understand the objective of why they are there and mitigate risk to an acceptable level for the organisation and the people working there. Accepting residual risk and remaining in high-risk areas can be a tough decision, as it requires recognition. It is within the organisation's duty of care to reduce the risk to an acceptable level to keep staff safe so that they can give their informed consent to work in the knowledge of the residual risk they face.

- How can we avoid becoming the department of NO… and setting up security audits to check if safety and security procedures are followed (compliance checks) and where practice on the ground (code of conduct related) are well followed? Fearing that non respect of security rules leads to disciplinary actions and could end up in complaints handling and verification and investigations in case of severe misconduct that creates threats to others in the organisation...

From Steve Dennis: Reviewing behaviour and implementation should also have a higher focus on catching people doing things correctly. "Thank you for the additional radio call when you suspected your plans changed." "Thank you for the double check on vehicle first aid kits." Etc. You can get across just as much information in a positive comment as a negative one, but also build the relationship, for those times when you will need to raise negative comments.

From Fredrik Pålsson: Whatever the context, NGOs are required to understand the risk they place their employees under and share these known risks, as well as put mitigations in place to lower the risks. Only then can the staff member can give informed consent to work under those conditions. Security situations change and assessing the organisational risk appetite has to be a continuous process. The measures put in place at one instant, will not give employers immunity from litigation should a staff member later be exposed to violence while deployed, as mitigations put in place should give the best possible working environment to avoid violence throughout the employee's deployment. Hence a fluctuating context need to be regularly assessed, to see that is it stays within the acceptable risk appetite for the organisation. If risk is understood from field to governance level, there is also greater acceptance for "department of NO", when we are operating outside of personal or organisational comfort zone.

- Whilst we have focussed on management being negligent there is the other side of the coin to consider. That being the field staff member who ignores security

advice and takes chances without repercussions. Whilst we should not be risk averse nor should we accept reckless behaviour which, in my experience has been, on occasion, prevalent.

Answer: When organisations do not fully embrace and understand SRM it often leads to the negative misperceptions and a reluctance to follow security decisions that they are not involved in. And, again, when organisations do not have a good security risk management culture rules and regulations may not be applied consistently – which means there are no consequences when rules are ignored.

From Steve Dennis: Security risk management is sometimes ambiguous as to whether the information and recommendations are for individuals to implement as stated or to interpret and make their own decisions. Related to that is, how to consult/inform security advisors if a unique situation arose needing new risk interpretation? I'd say that most individuals that make decisions derogating from security plans think it is in their delegation of authority, and have little evidence to the contrary. So, firstly, expanding the statements above signatures beyond, "Have read on date ____" to something more binding, "Have read, understood, agreed with and agreed to be held accountable to the above on date___". Prevention of sexual harassment codes of conduct are shedding some good examples to cutting the ambiguity to interpretation vs. instruction.

Secondly, many individuals that take somewhat risky behaviour, do that with the calculation against their own personal risk tolerance, and don't consider the consequences of their actions to other staff, programme, organization or assets. This has to be highlighted more.

Lastly, let's not forget the intersection of both sides of the coin, management that are taking individual decisions against security advice. In an example I was part of, months of reckless behaviour flagged higher and higher in the organization against managers taking high risks, was not enough to correct the action. Effective whistleblowing channels are needed too.

- I am wondering how we can measure and prove the effectiveness of security risk management. If it goes right, security risk management remains invisible or perceived as a barrier to main activities. Many only see the need when there has been a tragedy and security risk management actually failed. How can we tell a positive story of security risk management successes?

Answer: Through sharing of information and collaboration GISF helps organisations to learn from others, not just when they have incidents of their own. Through the DFID funded HuGS project we are currently looking at our approaches to MEAL and how, as a sector, we can get better at evidence based monitoring and reporting on the impact of SRM. If we can get better at positive evidence based reporting of effective SRM this can help us overcome the silo's and negative perceptions.

- Do the panel think that the income of NGOs and other humanitarian organisations are likely to shrink in the recession / depression following COVID-19? In which case what are the strongest arguments to protect spending on security within organisations, when every other department will be arguing similarly for special treatment?

From Steve Dennis: If funding is thought to be reduced, now is specifically not the time to have costly incidents. Also, many SRM elements cost very little. I don't know what a kilo of management buy-in to safe driving behaviours costs, but there are good ROI in SRM that can be focused on in slimmer times.

From Fredrik Pålsson: I have not seen donors cutting short security cost due to covid-19, on the contrary, what we have seen so far is that the general trend in-country offices show that we have been given wide flexibility from donors locally to re-programme existing grants. In our donor discussions; security is a very easy sell to donors, as security and HR are core components in any response package for safe program implementation.

- It's interesting to hear from Fredrik about decentralisation - I'd also be interested to hear more about the localisation agenda which might be really important in the post Covid world - how could we help build the capacity of smaller local NGOs to manage their own security? (I have some ideas here)

Answer: GISF is currently finalising the results of their research project on security risk management from the local partner's perspective. This will form the foundation for phase 2 of the project which is to look at practical ways that we can empower local NGOs to be better able to manage their own security risks. CV-19 will have to be taken into consideration as we look at phase 2. And very happy to discuss your ideas further!

- Question for the panel: what innovations do you expect (or hope) to see in NGO security risk management in the next 5 - 10 years?

Answer: Look at the notes from the GISF Rome Forum, September 2019. While we had considered these innovations – what is currently unknown is the extent of the impact of Covid-19 on humanitarian response and what this might mean for SRM. We must ensure we remain flexible to be able to meet these challenges as we get used to a 'new normal'.