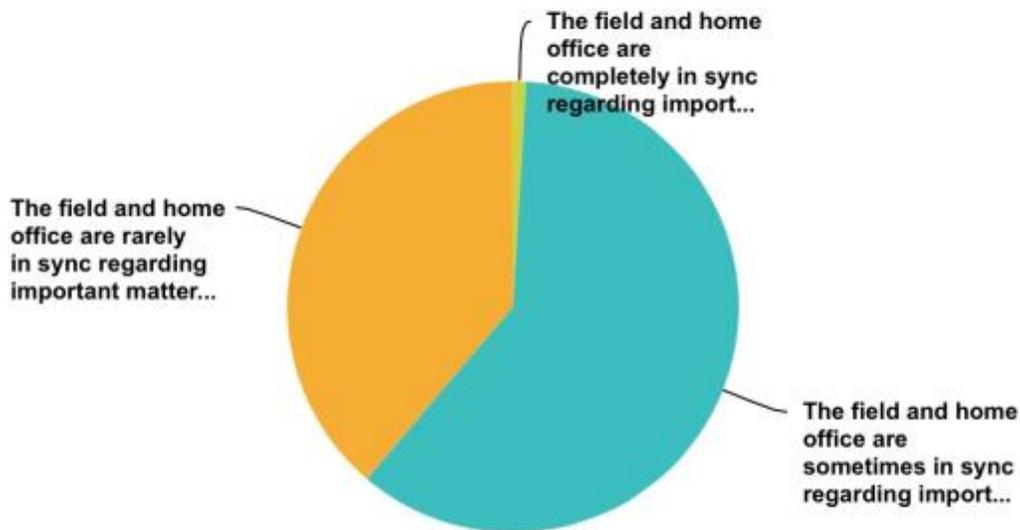




Feeding the Beast: Knowing and Understanding the Needs and Expectations of the HQ

Which statement below best describes your views regarding the relationship between the "home office" and the "field" in the aid industry?"

Answered: 766 Skipped: 244



Answer Choices	Responses
▼ The field and home office are completely in sync regarding important matters like priorities and processes.	0.91% 7
▼ The field and home office are sometimes in sync regarding important matters like priorities and processes.	60.31% 462
▼ The field and home office are rarely in sync regarding important matters like priorities and processes.	38.77% 297
Total	766

Why does a strong connection with the HQ Matter?

- **It help you *do* a better job** – Holding the line/decision support (ex. COP/Security conflicts), training, emergency support, budget needs, etc. As your in-country supervisor may not be focused on or prioritizing security, the HQ will be your best resource or backstop.

- **It helps you *have* a better job** - HQ may not make the ultimate decisions on ongoing performance reviews and retention, etc. but almost always have a say/input into them. They are, however, key for promotions, regional security positions, and for career advancement within the organization and long-term networks within the industry. They will jump in to provide support on internal decision making on things that help retain the talent they need in the FO.



1 - Know the Needs...

Different contexts, different needs. A good field staff member needs to be an entrepreneur. The best are often like mini-Executive Directors: they are relentless, energetic, driven, and there is often get things done by asking for forgiveness rather than permission. Headquarters staff, in many cases, are often functional experts or compliance auditors. They tend to be highly analytical, often think in terms of systems and standardization, and may be detail-obsessed perfectionists.

Know their needs to make their jobs easier – The HQ security team generally has the ultimate responsibility for safety and security and accountability upwards to the CSuite. In short, they need to be able to know enough to feed up critical emergency and emerging risk trend information and help you respond to them appropriately. You are important to allow *the team* to do the following:

- Supporting Field Office Crises/Emergencies
- Conducting security risk assessments (threat, vulnerabilities, and risk analyses) at HQ level, this might be granular/tactical or top-level/strategic but will require strong inputs from you, the experts on the ground;
- Ensuring Global Security Policies and Security Management Processes (procedures, SOPs, documentation, personnel, sourcing) are appropriate;
- Conducting security management audits to ensure the above are actually implemented on the ground;
- Managing global monitoring systems and practices to detect early warning signals of any foreseeable crisis;

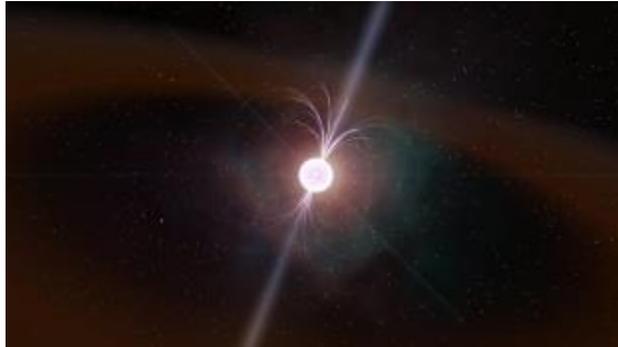
- Ensuring security training and information provision for security and non-security staff;
- Coordination across the global security network to enable leveraging when needed.

To do their job well the HO must: *hire and promote the right people, give them the tools and resources to do their jobs, trust them to do so, and then fight for their growth and retention.*

Be a STAR.



How to be the HQ's brightest STAR – The specifics will look different in every organization but the foundations are solid coordination between the Field and the HQ. This will boil down Field Security leads that are marked by **Solid reporting, Transparency, Activity/Anticipation, and Reliability.**



2 - *Solid Reporting-TAR*

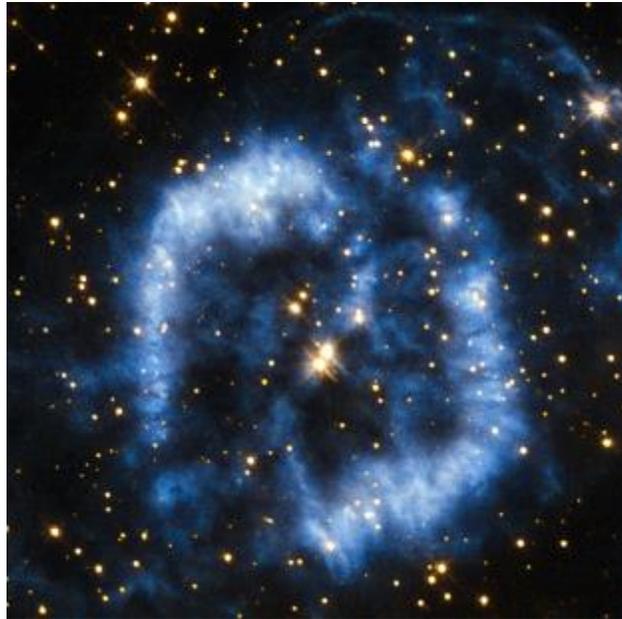
Solid Reporting – The keyboard might not be the weapon of choice but it will be the key tool to mobilize resources to solve problems. *What happened (or didn't), what is the impact to my team, what should my team do about it?*

Solid reporting comes from your network, your knowledge, and your ground-work but has to get documented and communicated clearly and regularly or it doesn't count! This includes all types of reporting; programmatic (They are traveling to where?!, They are doing what type of activity?!, The project is getting extended!? The COP is being replaced?!); security-centric or atmospheric; internal (from staff, M&E, etc) or external (PLSO or the PLSO network, military, government, etc); rumor or verified; tactical or strategic...

-
- *Good - VALUEADD: Professional, credible (or at least graded), timely, actionable.*
 - *Bad - VALUELOSS: No reporting. "Damn emails. The world was beautiful before emails and the immediate responses needed by someone at HQ. That's why I like to work in the field where I can decide that the internet 'didn't work for several days'." - Field office*
 - *Ugly - Sloppy, non-credible, inapplicable, late.*

ACTIONS: Agree on a template/format and a schedule that adds value (to all stakeholders) without driving you mad.

POLL Question #1: What kind of reporting is the most important to do your work? Medium-term trend analysis, heat mapping, tactical incident reporting, atmospheric data.



3 - S-Transparency-AR

Transparency.

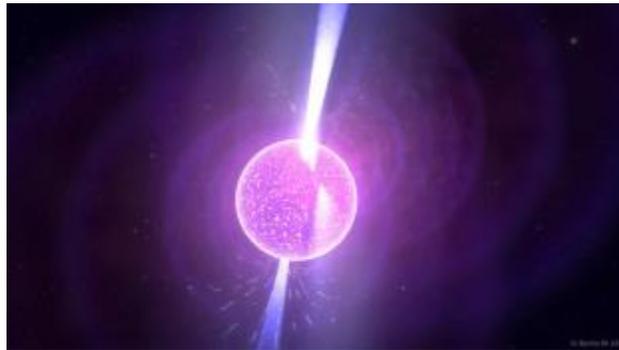
- *Practice transparency: Game playing reduces trust and the confidence of colleagues and others. Listen attentively, speak candidly, and treat others respectfully. Be vocally vulnerable, even when doing so is awkward or embarrassing.*
- *Integrity is non-negotiable. Tell the truth. Keep promises or don't make them. Compromising ethical standards is a sure route to trouble.*
 - *External - Information-sharing and collaboration within the security community.*
 - *Internal - **No surprises!***

-
- *Mistakes happen but the objective is to keep them from worsening, or from repeating.*
 - *Knowing what you don't know and admitting it.*

- *Every accident, error, or weakness is an opportunity to improve.*
-

Storytime: A rolling stone of mistakes.

ACTIONS: Think of one group whose information/knowledge you would love to have, and one that would want to have yours. How would that information best be shared?

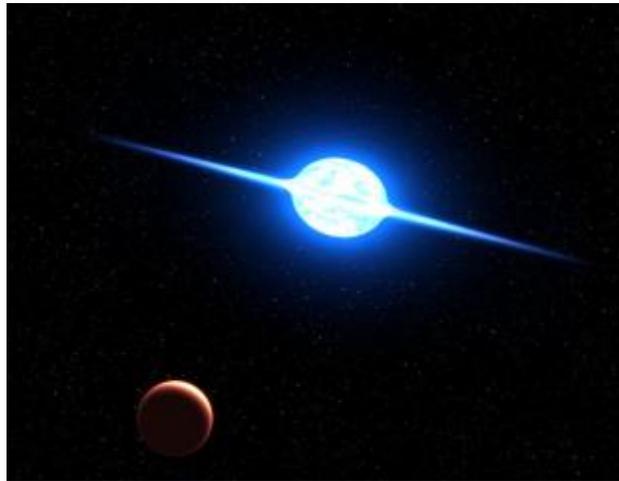


4 - *ST-Activity/Anticipation-R*

Activity and Anticipation *Be proactive and enterprising: There's always more that can be done, but it will generally be up to you to identify the gaps.*

- *Think long term and don't sacrifice long-term value for short-term results. Think strategically.*
 - *Anticipate problems before they become crises; the earlier you address a problem, the greater your options and the more likely it can be solved.*
 - *Speed matters. Many decisions and actions are reversible and do not need extensive study. Value calculated risk-taking. You have strong judgment and good instincts so seek diverse perspectives, work to disconfirm your beliefs, and then take action.*
 - *In the loop, networked: It's okay to not be the expert if you know or can find the expert.*
 - *Be curious about new possibilities and act to explore them.*
-

ACTION: Make a work-plan (with KPIs) and bring your HQ counterpart into that process.



5 - STA-Reliability

Reliability. This is broad! The HQ Security team is dealing with the management of plenty of problems, they are certainly stretched regardless of the size of the company, and they have to be able to provide resources and put up guard rails and trust their team to implement. This requires you to:

- *Be trusted. When emergencies happen or "No's" have to be said, you need to be the one that can make the hard decisions and be listened to.*
 - *Show up! What ultimately counts is getting the job done. Focus on the key inputs and deliver them with the right quality and in a timely fashion.*
 - *Take ownership and accountability.*
 - *Make good judgments.*
-

Storytime: From Security Manager to Chief of Party

ACTION: Involve the HQ in your personal development plan and mentorship.

POLL TIME

Poll Question #2 What aspect of STAR do YOU value the most? Solid Reporting, Transparency, Activity/Anticipation, Reliability

Poll Question #3 What aspect of STAR do you think the HQ values most? Solid Reporting, Transparency, Activity/Anticipation, Reliability