Lessons Learned

Cyber Incident Management Capacity Building

Executive Summary

Capacity builders focus on their work in a number of different types of initiatives, from short-term maturity and capability assessments and technical training, to providing long-term engagement and advice. These projects often face challenges, which include a lack of awareness of other, existing initiatives, or lack of long-term funding which focuses on short term deliverables. The key challenge is to find effective and efficient approaches that harness available resources to address capacity building needs over the long-term.

Capacity building projects tend to be more effective when they:

- **enable a long term relationship between the capacity builder and its partner(s)**;
- focus on incident management **infrastructure and processes rather than just skills**;
- build from **smaller projects onto larger, more challenging deliverables**;
- are developed in **a** multi-stakeholder way; and
- focus on interoperability and **sustainable impact**.

Background

This document introduces Lessons Learned from Cyber Incident Management Capacity Building projects, as collected by the GFCE Community. In 2018, the GFCE assembled a Working Group on Cyber Incident Management, and as part of its efforts, started collecting information on factors that impacted the delivery of capacity building projects.

This document is intended to be a resource for the GFCE community and other potential partners on how to improve future capacity building projects and increase their impact. The GFCE is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim of the GFCE is to identify successful policies, practices and ideas and multiply these on a global level. Together with other partners from NGOs, private companies, governments, and academia, the GFCE can be leveraged to develop and promulgate practical initiatives to build cyber capacity including cyber incident response management principles and approaches. It can also be leveraged as a network of incident management capacity building experts, or a “clearing house for capabilities” to improve the development and delivery of capacity building capabilities.

Examples of Cyber Incident Management Capacity Building projects

CIM capacity building projects can be characterized either by their intended outcomes, or through the methodologies used. At a high level, most capacity building projects we surveyed intended to achieve one of the following outcomes:

- Understand the current maturity of the CSIRT environment;
- Upgrade the CSIRT environment in capacity or capability;
- Build relationships between the national CSIRT environment and partners.

These goals are achieved through a number of different mechanisms:

- *Maturity assessments* of the current state of a cyber security incident management capacity. These assessments often consist of interviews and surveys, and assess maturity against cyber security incident response standards, such as SIM3 or the CERT Resilience Management Model.
- *CSIRT Implementation projects*: projects to work together with a recipient to build a CSIRT “from scratch” or significantly upgrade the capabilities of a CSIRT.
- *Training*, both at the national and organizational level. Training can be on processes, technology (such as software tools) or both.
- *Exercises and cyber drills*: organize exercises, which can vary from internal “table top exercises” through national level exercises, or “cyber drills” involving multiple national CSIRTs within a region. Typically these exercises simulate an incident, and test the effectiveness of each participant.
- Projects to *build networks across CSIRTs within a specific community*. This can be focused on incident responders within a specific industry, government (for instance connecting the teams at internet service providers), country or region.
- Members also conduct smaller projects and *informal ongoing engagement*, such as giving presentations, sponsoring conferences, or regular engagement with CSIRT within a region to make them aware of other initiatives and events in the region.
- Two GFCE members had projects involving *“roving advisors”*. These are incident management specialists who travel within a region and provide quick impact workshops and shorter bits of advice to individual teams. These advisors were often seen as individuals that connected entire communities, and generated long-term connections.

Capacity building projects are often implemented with a partner. In these cases, a partner tends to focus on one part of a curriculum, for instance policy or general organization, and additional partners provide support in terms of domain knowledge and expertise. Partners are also used to provide longer term, ongoing support in the region. For instance, a capacity building organizer may have the capability to provide training in a specific domain but may not have people in the region to provide long-term follow up.

Of note, not every capacity builder actually implements projects themselves. They may often contract it out, based on very specific requirements, to get a specific skill in the mix, or optimize spending across their investments.

Case study: Roving advisors (APNIC and FCO)

Two GFCE members have a project involving roving advisors. The United Kingdom invests in a small number of these advisors, who travel to various places with needs around incident management capability. The advisors are senior individuals who have, for example, set up domestic incident response capability. They now visit others to share the UK's experience. There is high level access through government organizations, and an ability to build up a long term understanding of what each partner country is implementing. A typical visit is three days, during which both organizational and technical conversations can be had.

APNIC has a Senior Internet Security Specialist who provides on-site training and guidance to new and emerging CSIRT across the region. The specialist also travels to local and regional events and as such builds up a long term relationship and experience with most countries covered by the region of the regional internet registry. He or she also promotes technical best practices by visiting internet service providers and other network operators, and by organizing security sessions at other, non-security events organized by APNIC and the community.

What are contributing factors to a successful program?

The following factors were identified as contributing to the success of a capacity building program:

1. Long term investment: Systemic investments that seek to build comprehensive incident management capacities are preferred. Projects that run over a longer period of time, and consist of repeated follow-up rather than a one-off meeting, tend to have longer term effects.
2. Project context: projects tend to be more successful when they followed a comprehensive needs assessment that provided a complete picture of the cybersecurity needs in the country.
3. Regional capability or partners: having partners either in the country where the capacity building project takes place, or within the region, that can make repeated trips or have a long term presence, is a strong indicator of long term impact. The partner can continue to follow up and provide in-person support as needed.
4. Being politically, commercial and technologically neutral: projects which are not tied to a specific technology, or support a wide range of technologies, are more likely to be accepted by the recipients of capacity building.

5. Situational Context: knowing “who is who”, and what they are responsible for, is a key component of initiating a solid project. With this information, initiatives can be focused on the right people.
6. Multi stakeholder approaches: where possible, have participants be from multiple stakeholder groups in the country. This ensures that groups have an opportunity to hold each other accountable over time. Projects such as desktop exercises and seminars can be focused to show how interconnected the incident management community is, and bring people along from the start.
7. Project coordination: when they have strong awareness of existing projects in the country, capacity builders can engage and discuss their project with others ahead of time, and ensure there is no duplication of effort, and more alignment.
8. Project preparation: projects were deemed most successful when they included “site visits” for trainees. Capacity is most effectively built when the recipients have the ability to, after training or exercises, actually participate in the work in a different organization, such as another national CSIRT.

In particular, GFCE members found it valuable when a project followed an existing capability assessment. This allowed them to focus on very specific and tailored programs that will help build a specific capability. However, they noted that quite often, capability assessments do not exist, or have not been published.

It was also very important for members that the effectiveness of a program is measured. Methods of measurement include surveys, evaluating to what degree the new CSIRT is effectively handling incidents reported to them, or evaluating their level of outreach to others after the capacity building program finishes. Output metrics, such as the number of unique engagements between the capacity builder and the recipient is not a helpful metric by itself. Outcome metrics would be preferred but are rarely possible without long term engagements.

Case study: Being technologically neutral (APNIC)

APNIC’s ethos is to be bottom-up, community-driven and include the cyber/technical community in its projects. It does not support or prefer specific vendors.

APNIC trainings do not focus on a specific technology, but teach internet standards and principles that will always require some “localization” by the participant in a project. Technology within their coverage region is very heterogeneous and the approach reflects this. This vendor-neutral approach has proven very valuable in building trust. It also helps APNIC be less technology focused and able to “bring everyone along” during a project. They take a community based approach, usually starting with the network operators and then including local vendors, service providers and government.

What are high level challenges in implementing capacity building projects?

The following were identified as key challenges in implementing capacity building projects:

- *Projects are often operated with a wide set of capacity building providers, but no clearly defined Roles & Responsibilities.* This is especially the case when these providers are governments, and there may not be a clear distinction between who is the lead on the project. This could be improved through better planning and coordination.
- *There is no easy way for capacity builders to quickly identify who else is working in a country or region.* It would be helpful to have a central coordination mechanism that can help identify existing projects, and in particular existing needs assessments.
- *Too often, the target country is considered merely a "recipient" and is not a partner in the project, which can lead to distrust or lack of buy-in.*
- Target countries are often the best positioned to map out the activities in their economy, rather than only looking to engage with funders/delivery partners; and they should be involved or drive these efforts. *There is a lack of turn-key solutions that can be applied in projects.* Just as a CSIRT is made up out of different skills and expertise, it's challenging to have a single person or even organization who can address all CSIRT needs.. Capacity building organizations should bundle their strengths, and build technology independent turn-key solutions for common initiatives, such as information exchange and the incident management process and tracker, recognizing that the implementation in the local landscape (building relationships with government, regulator, civil society) would for instance always need to be bespoke
- *Projects are often implemented with too little understanding of the local culture and institutions.* It is challenging to understand these aspects unless you have had historical on the ground expertise, and most projects are often overly focused on providing training, rather than putting in place the institutional support and awareness building that is needed to make them successful. Also, capacity building materials are often only published in English or in the local project language, and are not always easy to translate between projects or cultural contexts.
- *States and organizations often have specific historical security incidents, which would make great case studies for future capacity building efforts.* It is usually hard to help advance the capabilities of an incident response entity if the threats that they are dealing with are not understood. These incidents often have not received a formally documented post-mortem, and as such they are often not well understood by those initiating a project. Spending time as part of needs assessment studying previous incidents that mattered to stakeholders is helpful but not frequently done.
- *There are some human rights challenges with projects.* This is especially the case when laws may not define what a security incident is, or have a wide definition which also includes for instance the distribution of offensive content. There is a lack of frameworks on how these risks can be managed and monitored.

- *It is sometimes not clear who is responsible for running a national CSIRT*. This is sometimes the subject of competition for resources or authority between government departments.
- *Many CSIRTs have small budgets and/or weak human resource management processes* (e.g. not recruiting on merit; not incentivising good performance; not investing in training, for systemic workforce management reasons wider that might affect all departments, etc.). Cyber security capacity building projects can not address these systemic issues on their own and even where there are public sector reform projects addressing them these can take several years to have an effect.

Detail: Challenges involved in incident response projects (FIRST)

In 2018, during the UN Internet Governance Forum, FIRST partnered on a project with Access Now, an NGO working to protect digital rights, on a workshop to identify key issues in inter-stakeholder relationships. During this session, a number of typical challenges were identified by the participants, who were from the Technical Community, Government and the Incident Response Community:

- The configuration of a CSIRT can have implications on its effectiveness. A CSIRT built into an intelligence agency may not always be trusted by the private sector, or one that is part of the regulator may not be trusted to report incidents for which they can typically be fined. While each of these cases can work, they require specific mitigation to ensure that the incident response capability can be effective.
- In some countries, issues involving human rights violations may lead to less trust in a government managed CSIRT. In one organization, a CSIRT had developed principles from the top down aligned with the UN Declaration of Human Rights, which were translated down into actual policy discussed with technical stakeholders. This eased the relationship with external stakeholders significantly.
- There were also concerns raised around the “criminalization of technical expertise”, which may make the use of technologies by incident responders outside of government difficult. When the use or import of tools is restricted, vital open source tools may not be usable by the incident response community. It is important that capacity building projects stress the need for why specific tooling is required and helpful, and translate this to the right levels of decision-making.

Key opportunities for improvement

Implementers of CIM Capacity Building projects identified the following key 6 recommendations to improve the effectiveness of capacity building projects:

1. Funders should ensure that funding is focused on longer term investments, with follow-up to programs, rather than one-off trainings or engagements.

While one-off events can be helpful, results are often not seen when there is no ongoing support in implementing the changes that they intend to accomplish.

2. Implementers should focus on incident management infrastructure and processes, rather than purely skills-based training. Then, partner with regional and local organizations that can continue to share the learnings across an ever widening community. Where skills-based training is valuable, a focus on train-the-trainer sessions can help provide long term benefits.
3. Implementers should start with smaller projects, and increase their commitment over time by starting to work on more challenging topics. For instance, an initial project may be focused on solving a single technical issue, or building out a high level incident response plan. A subsequent project may then focus on more challenging implementations.
4. Implementers should ensure they have a wide set of local partners, ideally across multiple stakeholder communities. These types of engagements build lasting change by building local networks that may not exist prior to the project. Implementers should connect with their peers in international networks and widely advertise their projects. When treating the target of the capacity building work as a partner, and giving them a clear say in identifying their needs and the appropriate program, one typically acquires better results. Everyone is equal, and partnerships should go in both directions, avoiding for instance northern and southern hemisphere divides.
5. Implementers should consider building turn-key solutions for specific problems, that are very open to being customized to the local situation. As CSIRT are intended to cooperate, it is important to have interoperable systems and frameworks.
6. Sustainability of impact is key, since available funding is mostly made available on a short to mid-term basis. This can be most effectively implemented through obtaining local buy-in for ongoing costs, such as salaries and ongoing training.

Case study: Using the GFCE to help design a project (FCO)

In September 2018, the UK Foreign and Commonwealth Office was designing a new project to develop cybersecurity capacity across Commonwealth countries in Africa. Before designing the project FCO wanted to know what other similar projects were being run and what advice or lessons others had for them. They therefore asked the GFCE's Working Group B, focused on Cyber Incident Management, for this information.

The FCO sent the Working Group a one page note explaining the intended project goals and the information and advice they were looking for. They received several responses. With these they designed the content of the project and learned lessons from past projects. Even better, some organisations offered to attend the training events to provide their own expertise. The FCO accepted these offers. This resulted in better training events and less duplication of effort among donors and capacity building organisations.