# A Model Framework for Successful Cybersecurity Capacity Building

**By Adam Palmer**

Establishment of a long term capacity building plan is the foundation for success in achieving cybersecurity goals. Without a solid foundation, there is no likelihood of achieving success. Whether applied to government or private industry, a capacity building plan should establish a dynamic assessment and improvement process. This plan should be a long term strategy, but provide a flexible approach that may be modified as technology and threats evolve.

The most important concept of the long term capacity building plan is that each organization has unique needs on a spectrum based on an individual organization's risk based assessment. Each organization must identify critical capability areas that correlate with a desired security readiness outcome. Within each area are maturity levels. Maturity levels are established by measuring progress along a continuum of risk based preparedness from low readiness levels to advanced full capability. This risk and capability evaluation process allows senior decision makers to benchmark existing cybersecurity preparedness, evaluate core competencies, and provides an operational framework for capacity building that also dynamically measures improvement.

To effectively build capacity in critical areas, a capacity building plan should include phased development stages and processes leading to a state of readiness for achieving each strategic objective that is identified in the initial assessment. Capacity building ideally should be a holistic process. Failure is more likely to occur if the development approach is a patchwork of activities rather than a comprehensive and harmonized program across the organization. Capacity building should follow a multi-level process, encompassing not only "vertical" training of staff but horizontal efforts across an organization to promote effective policy and incident response planning as well. Although compliance is not "true security," as many threats can evade basic compliance measures, policy goals and compliance requirements are a starting point and foundation that can keep a capacity building program focused. Compliance always should be tightly focused on risk mitigation for each organization and not a self-serving mechanism to approve existing controls.

While the methodology for implementation of a capacity building plan will be different for each organization, the participation of senior decision-makers across all areas of the company is critical. Senior decision-makers provide support for solutions and incentivize internal groups to invest resources in security.

This article provides a model suggested approach to a long term policy and operational capacity building program that can be implemented by either a government body or private industry. The objective of this model framework is to develop, implement, and maintain a comprehensive capacity building and training program for cybersecurity and incident response. This is a long term development program that includes capacity building for threat intelligence coordination, cybersecurity planning, and incident response management. This program also includes a policy framework support designed to support holistic cyber defense capacity building that results in long term success against cyber threats. Cybersecurity is not just a technical solution. The foundation for all technical solutions should be based on a clear understanding of policy requirements and strategy goals.

## CAPACITY BUILDING PROGRAM

The overall objective of a capacity building program is to create an "adaptive defense" capability.

***Adam Palmer**, MBA, JD, CISSP, is based in Munich, Germany and manages international government affairs at FireEye, a leading advanced cybersecurity company. He may be reached at* adam.palmer@fireeye.com.

Adaptive defense is the ability to detect and respond to identified security needs by using intelligence based information and effective response planning.

A capacity building program needs to have a few central elements in order to succeed. The following should be included:

1. Assessment and Development of a procedural framework for capacity building and organizational development related to cyber threats, developing cyber intelligence analytics, and incident response management activities that comply with relevant national and international requirements.
2. Capacity building training to support development of internal legislative, procedural, and technical operational capabilities to prevent and combat advanced cybercrime in a holistic manner.
3. Training of investigators, prosecutors, incident responders, and support staff to understand and implement tools and techniques to effectively provide advanced response capabilities.
4. Long term sustainable methodologies to monitor training effectiveness, update approaches, and implement updated global best practices for success.

Initiatives to combat advanced cyber threat activity must be placed within a solid procedural framework. This provides operational guidance and supports a comprehensive capacity building program resulting in successful outcomes. The basic elements of an effective operational framework include:

- Assessment of operational cyber intelligence and investigation response needs
- Risk based needs assessment
- Assessment of financial resources
- Training of staff on technical and procedural handling of digital evidence and incident response management
- Training on presentation of complex digital evidence and case development mechanisms
- Development of strategy and policy tools for addressing advanced cyber threats

Compared to the investigation of "conventional" cybercrimes, the development of cyber intelligence and advanced cyber response operations presents at least five key challenges:

1. *Access to Evidence*—Evidence of advanced cybercrime exists in electronic form across a variety of sources, geographic boundaries, and sensitive geopolitical environments. The lifetime of such evidence varies enormously from microseconds to months. The physical location of evidence also varies from a target's personal computer to data on servers held by third parties, such as Internet service providers or data storage providers. In light of the global nature of the Internet, such evidence, in principle, may be physically located anywhere in the world. Further challenges include the fact that relevant evidence may be contained within vast quantities of non-relevant data, and that evidence can be subject to advanced methodologies for hiding or obscuring such data. The laws to obtain such data are complex and require a careful analysis of multi-national legal standards.
2. *Handling Evidence*—Electronic evidence requires careful handling in order to ensure that it meets the necessary standards for use in court. Issues include the legal admissibility of electronic evidence, demonstrating chain of custody, ensuring the integrity of evidence, and its collection in accordance with due legal process. Evidence must be obtained in cooperation with global electronic service providers using appropriate procedural channels with global law enforcement and the intelligence community. Evidence must also be presented before a court or tribunal in a manner that clearly attests to the facts claimed and is delivered in such a way that a judge or jury can understand the relevance of the electronic evidence without requiring a deeper understanding of the technology involved. In advanced intelligence based cases, additional security interests also may need to be considered in the handling and disclosure of digital evidence.
3. *Identifying the Perpetrators*—Moving from monitoring and investigating advanced electronic evidence to the identification, disruption, and apprehension of the perpetrator(s) can represent a significant challenge. Information often is likely to be required from private sector service providers. When perpetrators are located in

multiple countries and information is distributed geographically, the investigation requires informal and formal cooperation mechanisms to facilitate further investigation.

4. *Protecting Operational Security*—Intelligence gathering of advanced electronic communication evidence requires an assessment of specific operational requirements and the development of a holistic framework for the privacy and security of operations. The framework must provide the strongest levels of operational security and be submitted to regular evaluation to confirm suitable functionality for the security of operations and to evaluate any potential security gaps that might result in a threat to operational integrity. Such complexities can place a significant strain on operational resources and requires an advanced understanding of operational security requirements that is regularly updated based on new technology and global best practices.
5. *Case Development and Investigation of Criminal Networks*—Implementing advanced techniques for investigating cybercriminal groups abusing digital networks requires tools and techniques that include not only collection of case evidence but also strategic actions designed to disrupt and frustrate attackers. Techniques may include advanced investigation and monitoring operations that are guided by careful procedural and operational controls for both security and handling of evidence.

## DESIGN OF THE PROGRAM

The capacity building structure should be designed to enable a comprehensive, long-term, and holistic approach to preventing and combating advanced cyber threats. The program design should ensure that current initiatives are not duplicated but build on what currently exists. The program also should make use of experts and institutions that already have developed proven tools and materials in the relevant areas.

In order to achieve this goal, a suggested program consists of three *activity areas* built on two *normative areas*. The activity areas consist of: (1) training; (2) sustainability planning; and (3) internal/external cooperation. The normative areas consist of: (1) framework development and (2) standards. The activity areas represent primary actions in training and staff development. The normative areas cover the development of operational procedures and security standards to be used for the purposes of implementing a consistent approach to cyber threats.

The modular design of the program is intended to offer a complete programmatic approach that can be applied at every level while incorporating a regional and global perspective in areas such as international cooperation. Specific activities may be tailored or selected from across work areas in accordance with needs and the results of a comprehensive needs assessment to be completed prior to commencement of activities.

For the program as a whole, the primary expected outcome is increased efficiency and effectiveness in the detection, investigation, disruption, and management of advanced cyber threat activity, leading to greater deterrence and successful management. This should include the ability to obtain and handle complex digital evidence obtained thru complex operations, awareness of operational risks, and adoption of protective operational procedures to mitigate loss of sensitive intelligence information. The foundation of this must include efficient and effective long-term organizational response to advanced cybercrime, including coordinating mechanisms, effective procedural frameworks, and advanced team capabilities to counter cybercrime, leading to a sustainable response. Finally, the program should successfully develop the capability to maintain advanced cyber intelligence and incident response operations and apply disruptive tools against criminal groups targeting the organization.

Each activity domain within the program can be summarized as follows:

- **Framework Support:** The assessment of operational needs and development of a strong sustainable framework that provides comprehensive operational security and procedures for operations. The development of this framework must be done with full compliance for local and international legal standards.
- **Operational Standards:** Comprehensive assessment of existing legislative policies covering criminalization, procedural law, electronic evidence, jurisdiction, private sector responsibilities

and liabilities, and international cooperation, using good practice benchmarks and relevant regional and national standards.

- **Operational Training:** Delivery of investigator training at basic level, intermediate level, and advanced level on advanced electronic evidence collection and handling.
  - For Government, the delivery of prosecution training at basic, intermediate level, and advanced level on the role and presentation of electronic evidence and applicable substantive and procedural law in the prosecution and adjudication of advanced cybercrime cases.
  - Organization of public private partnership expert working groups to create protocols on involvement of specialized procedures, use of investigative measures, guidelines for intelligence sharing operations, and the introduction and consideration of electronic evidence in legal forums.
- **Sustainability:** Provide long term coordination and support mechanisms across organization to effectively transfer capability from global experts or security vendors to internal organizational staff and to maintain team readiness.
- **Cooperation:** Facilitation of working relations between law enforcement and local offices of key global electronic service providers.
  - Development of procedures and due legal process requirements and facilitation of sharing of strategic threat information from key global cybersecurity providers to intelligence analysts.
  - Establishment of advanced teams working with law enforcement and intelligence groups to apply legal, procedural, and technical tools to monitor and respond effectively against threats.

The program is created as an on-going long term project to support independence and internal capacity development. Implementation of the program requires the delivery of substantive expertise by international technical experts. It also requires expertise in crime prevention, public–private cooperation, international cooperation, legislative review and reform, and procedural law. These areas require highly skilled personnel with specific high demand skills. This program is best achieved (and requires) the delivery of training, services, and guidance by global experts as part of a multi-year program. No specific vendor or provider is highlighted, but each organization will need to evaluate the best provider to increase capacity for a specific area, and that is feasible within the organization's cost limitations.

## IMPLEMENTING THE PROGRAM

A suggested approach for a Phased Implementation Plan is outlined below.

**Phase I—Operational Framework Assessment and Development**

- Assessment of operational, procedural, and training requirements
- Development and review of capacity building framework and capacity building program recommendations

**Phase II—Implementation**

- Establish on-site cooperative partnership teams led by global experts to implement a capacity building program from basic to advanced
- Training on advanced detection and response capabilities that ensure compliance with international regulatory frameworks and best practices
- Evaluation of implementation and adjustment to meet identified standards goals

**Phase III—Sustainability and Maintenance**

- Additional support for staff as needed on tools and techniques as determined necessary by monitoring and evaluation
- Implement long term external cooperation and support mechanisms

## CONCLUSION

Progress in implementation of the program should be tracked through ongoing monitoring of

the needs indicators established in the initial assessment. The purpose of ongoing monitoring will be to ensure accountability through transparent and clearly-documented records, with a view to enabling clear oversight, decision-making, and transparent operations. Information required for the indicators should be collected periodically, within a timeframe appropriate to each indicator, taking into account the time required for outputs and outcomes to have effect. Results from calculated indicators that are available can be used to ensure that activities, outputs, and outcomes are in line with the expected results.

The challenge of advanced cyber threats is unlikely to be resolved in the near future. Both private organizations and governments must commit to a long term program of capacity building for prevention, detection, and response. It is critical that capacity building actions aim towards a sustainable response. Investment should be made in establishing functional and sustainable solutions that create a solid foundation for the future.