Carnegie Mellon University
Software Engineering Institute

Enabling the Sustainability and Success of a National Computer Security Incident Response Team

Tracy Bills
Brittany Manley
James Lord

Contents

Introduction	2
Setting the Context—What Do We Mean by Sustainable and Successful?	3
Prepare for Stand-Up	3
Establish Policy and Governance	4
Engage with Your Constituency	5
Engage with Your Peers	6
Establish Effective Operations	8
Address Staffing Needs	10
Conclusion	12
Resources	12

Introduction

A national computer security incident response team (CSIRT) serves a unique role in protecting and defending its country or economy from cybersecurity incidents that can have an impact on national or economic security and public safety. It serves as a center of technical capability for the prevention, detection, and response coordination of cybersecurity incidents. A national CSIRT can be inside or outside of government, but it must be **specifically recognized by its government as having responsibility in the country or economy.**

Over the past thirty years, more than 130 national CSIRTs have been established. Also during this time, organizations have produced various documents and resources that address best practices for creating and managing CSIRTs, including national CSIRTs. However, because of differences in culture, economics, and government structure, the organization and responsibilities of national CSIRTs vary among countries and economies. Such differences include how many national CSIRTs serve a country, where they are located, who their constituencies are, and the nature of their services and responsibilities. With so many variables, how is it possible to ensure the sustainability and success of a national CSIRT?

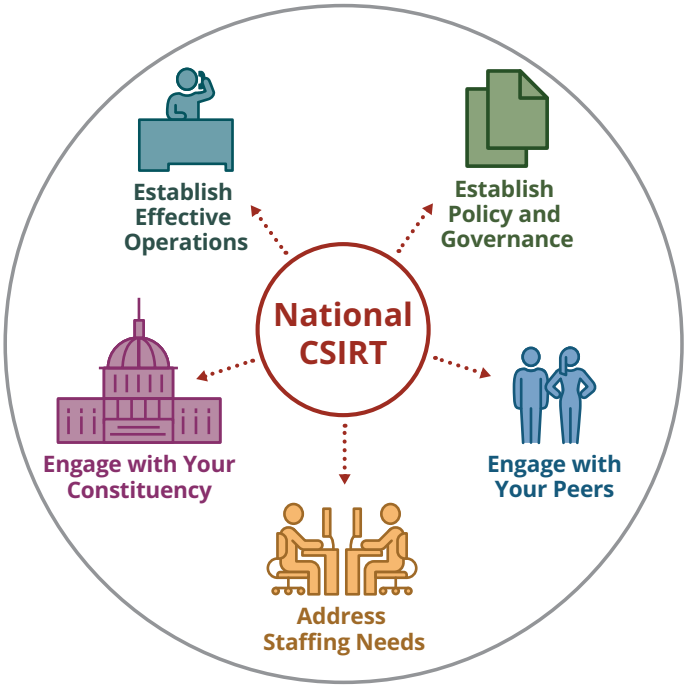
Audience

The primary audience for this document includes

- leaders, managers, and team members of national CSIRTs[1]
- facilitators and members of teams or committees tasked with planning and establishing a national CSIRT
- individuals or teams providing capacity building assistance to the above

How to Use this Document

While there are many available resources related to creating and managing a CSIRT, they can be overwhelming, making it difficult to identify what will be most effective in practice. In this document, we have captured lessons learned from our own capacity building work and those provided by national CSIRTs that have demonstrated sustainability and success. This document can be used in conjunction with existing resource materials to help you prioritize efforts for developing or enhancing your own national CSIRT.



1 While this document uses the term national CSIRT, some countries and economies use terms such as national cybersecurity center, national coordination center, etc. (the national CSIRT may even be a component of the center). Therefore, leaders, managers, and team members of such centers may also find this document useful.

Setting the Context—What Do We Mean by Sustainable and Successful?

The basic definition of sustainable is the ability "to be maintained or kept going, as an action or process."[2] However, to be effective, a national CSIRT needs to do more than just exist and keep its processes going. It also needs to be successful, which means having a "favorable or desired outcome."[3] In other words, a national CSIRT should conduct its activities in a way that ensures its long-term existence and also enables it to accomplish its goals.

These specialized CSIRTs frequently have goals such as

- being a national focal point within a country, economy, or region to coordinate incident handling activities, which includes cooperation with the global National CSIRT community
- analyzing and synthesizing incident, vulnerability, and threat information disseminated by their constituency, other teams, vendors, and technology experts to provide an assessment for their own constituency and communities
- facilitating communications across a diverse constituency—bringing together multiple sectors (e.g., government and military, critical services and infrastructures, commercial, academic, banking and finance, transportation) to share information and address computer security problems, such as widespread computer security incidents, threats, and vulnerabilities
- developing mechanisms for trusted communications within these communities[4]

Through our capacity building work and experience in the community, successful national CSIRTs most often

- have long-term relationships with their constituents
- are able to reach a lot of constituents and provide value to them
- provide actionable information and enable constituents to be able to react successfully to information security threats
- continue to get attention (while perhaps not with optimum speed) from national leaders and constituents, who continue to report new incidents to them
- are capable of reacting successfully to threats and incidents
- are well known, have developed credibility, and are respected globally

While sustainability and success are closely related, it is possible to have one without the other. For example, a national CSIRT may have secured long-term funding to contribute to *sustainability* and may be initially successful at providing valuable services to its constituency. However, if the constituents mature and outgrow the need for those services and the national CSIRT does not adjust, it can no longer be considered *successful* because constituents are an important part of every national CSIRT's mission. Therefore, it is important for you to balance your activities in a way that you are able to ensure your organization's long-term existence and enable it to accomplish its goals.

The information in this document was gathered through the following sources:

- our collective experiences working with various national CSIRTs in the incident response community and capacity building work we have done over the years
- our collaborations with national CSIRT staff that demonstrate broad knowledge of their national CSIRT planning and implementation
- courses we have developed and/or instructed
- a literature search and review of related articles and other documents that address creating and managing CSIRTs

Prepare for Stand-Up

As with any project, starting with an appropriate foundation of knowledge is important. Two common initial steps that have been taken when teams are tasked with the development of a national CSIRT are to

- gather and review existing documentation and guidance
- consult several existing national CSIRTs for their lessons learned and advice

If you are a new national CSIRT, you may find it challenging to determine what documented guidance is applicable to your circumstances. You will need to determine what aspects of other national CSIRTs are appropriate models to leverage while working within the requirements and constraints of your government and/or sponsoring agency. If given the opportunity to do anything differently during the stand-up phase, most national CSIRTs would have preferred that there were more teams in the global community that offered one-on-one consultations, coaching, and teaching to assist with identifying relevant information from documentation. While many agree this would have been beneficial, others who did leverage

2 **dictionary.reference.com**

3 **merriam-webster.com**

4 **resources.sei.cmu.edu/library/asset-view.cfm?assetid=53062**

national CSIRTs or other organizations (many for a fee), found the advisor lacked understanding of the internal workings of the country or sponsoring agency.

This led to a new set of challenges including the following:

- The national CSIRT was not placed within the appropriate governmental entity.
- The recommended or provided proprietary tools were difficult to maintain or upgrade.
- The implementation plan was more aggressive than the new national CSIRT could maintain.
- There was a high cost of consultation, and consultation did not extend past the stand-up phase.

When deciding which national CSIRTs to consult, consider the similarities between their structure and the intended structure of your new CSIRT (e.g., services offered, placement in government, constituency). It can also help to consult teams based on convenience factors (e.g., geographical location, culture and language similarities). Many find that such interaction and advice exchange only occur during the research and planning phase leading up to the stand-up phase. When selecting national CSIRTs to consult, you should take into consideration whether advice is needed on a short- or long-term basis so that you can identify teams that are willing to provide the appropriate amount of mentoring. Advice from other national CSIRTs is generally beneficial, but it is important to keep in mind that no two national CSIRTs are, nor should be, completely alike.

LESSONS LEARNED

- One-on-one consultations, coaching, and teaching with an advisor are more effective from those that understand, or are willing to take into consideration, the internal workings of the country/economy or sponsoring agency (especially during the stand-up phase).
- A good advisor is capable of making recommendations for applying best practices to your environment and does not just provide "one size fits all" guidance.

Establish Policy and Governance

As cybersecurity has become a more common topic on national political agendas around the world, policy and decision makers are becoming more aware of their national CSIRTs. Many early national CSIRTs were established in the absence of national cybersecurity policies, strategies, and/or legislation. Many of them played a key role in helping their country or economy develop the initial version of these important documents and continue to influence updates. In other cases, national CSIRTs were created as a result of national cybersecurity policies or strategies being implemented first.

There are differing opinions among national CSIRTs about whether a country or economy should have national cybersecurity policies, strategies, and legislation in place before creating a national CSIRT, or if it is best to create a national CSIRT first to aid in the development of these requirements. That said, many countries or economies that are still working on both are trying to do so simultaneously rather than chronologically.

Regardless of development order, the general consensus is that it is critical to develop both a cybersecurity policy and a national CSIRT for the purposes of national security. National CSIRTs also agree that government buy-in and support of the national CSIRT is important for sustainability and success of the national CSIRT. This can be challenging to obtain and maintain because government officials

- are not always very involved or interested in the national CSIRT
- have misconceptions about what the national CSIRT should do
- do not see the value of the national CSIRT

For some, such leadership positions can have a high turnover rate, which then requires the national CSIRT to continuously educate others about their mission and relevance. This is why many national CSIRTs find it essential to have a member of their staff in a dedicated engagement role (see the Address Staffing Needs section for more detail).

Another challenge national CSIRTs have experienced in the area of governance, pertains to where in the government structure the CSIRT is situated. Some have discovered that a more thorough research and planning phase should have been conducted prior to creating the CSIRT. A national CSIRT needs a parent organization that will be a champion for its mission and funding. A national CSIRT should also have the authority and influence needed to engage its constituency. This is especially true when constituents are also government entities. Because this aspect of CSIRT formation may not have been completely considered during planning, some national

CSIRTs have found themselves part of one ministry or sector while their constituents are part of a completely different one. This disconnect can make it difficult for national CSIRTs to carry out their missions.

LESSONS LEARNED

- Regardless of order of development, national cybersecurity policies, strategies, legislation, and national CSIRTs are all necessary for national security.
- National CSIRTs need government buy-in and support and careful selection of organizational placement, the authority or influence to engage constituents, and a parent organization that serves as a champion for its mission and funding.
- Hire a dedicated staff member responsible for leadership engagement.

Engage with Your Constituency

A national CSIRT may have many different constituencies, and in some countries or economies, more than one national CSIRT has been created to serve different constituencies. Frequently, national CSIRT constituencies include some or all of the following entities.

National CSIRTs consider constituents and their needs to be an important part of the mission and its success. To understand how to effectively meet those needs, you must understand who makes up your constituency and the capability of those entities. Then you can determine how best to help your constituents. It is important to also understand that a constituency can be comprised of many sub-constituencies with different needs that may require different services.

Some national CSIRTs—especially those that include private sector entities in their constituency—found that it was more productive to start in one sector and define processes and build trust before doing so in other sectors. Even within a sector, some national CSIRTs found it beneficial to hand-pick specific organizations to work with first. This allowed the national CSIRT to prove that they would do what they said they would. As a result, other organizations within that sector, and eventually other sectors, were more willing to report events or share incident data with the national CSIRT. Whether your charter is to be a focal point for the entire country or just a smaller subset, garnering trust and proving your value to your constituency are key factors to success, especially if your national CSIRT has no legally binding authority over its constituents.

The most common methods national CSIRTs found to be helpful in building trust and understanding the needs of their constituencies include providing

- written guidance and in-person workshops for constituents about what the national CSIRT can do for them
- written guidance and in-person workshops for constituents about what and how to submit reports to the national CSIRT
- continuous feedback mechanisms

Throughout the life of a national CSIRT, the defined constituency can change as its individual capabilities mature. As the constituency changes, the national CSIRT should update its understanding of their needs and create, discontinue, or adjust its services to meet the needs of its changed constituency. To accomplish this, national CSIRTs routinely gather feedback from their constituents. The methods used vary from annual surveys to informal discussion, and feedback requests pertain to topics ranging from new services desired to applicability of reporting content.

If possible, you should also develop relationships and collaborate with law enforcement organizations, even if they are not part of your constituency. Information sharing may not be bi-directional, and it can be challenging to establish routine exchanges. However, collaborating on cybercrime events by providing support with forensic analysis, reporting, or mitigation actions is beneficial for overall national security and can increase the visibility of your capabilities.

LESSONS LEARNED

- Conduct trust-building activities with constituents (start with a subset of the constituency and build out over time).
- Routinely communicate with constituents and gather and analyze their feedback to implement, adjust, or discontinue services as constituency needs and abilities evolve.
- Collaborate with law enforcement but manage your organization's expectations based on your mission, capabilities, and constituency.

Engage with Your Peers

National CSIRTs Within the Country/Economy

In cases where a country or economy has decided to distribute national CSIRT responsibilities across more than one team, it is essential that those teams work closely together.[5] While some sectors can experience unique threats to specialized technology not used in other sectors, most threats and vulnerabilities are similar across sectors and constituencies. Because resources are limited, it is essential that these teams share information, such as indicators of compromise (IOCs) and the tactics, techniques, and procedures (TTPs) of threat actors.

Beyond sharing information and expertise, sharing specialized capabilities can also help you use limited resources more effectively and provide better services to your constituents. If a country or economy does not take this approach, the overall effectiveness of all teams is reduced because resources and capabilities are duplicated, and needed capabilities are not developed due to lack of resources.

By comparing and understanding the reasons for commonalities and differences in the information being shared within the different constituencies, the collective group of national CSIRTs may be able to improve collaboration by measuring its effectiveness and addressing its constituency's needs. By bringing the separate constituencies together to discuss current efforts and challenges, national CSIRTs may be able to identify additional opportunities for cross-constituency cooperation.

Example

Two national CSIRTs of a particular country sign an agreement to share cybersecurity information with each other. While one national CSIRT handles policy and operational matters within government agencies, the other national CSIRT handles operational matters in the private sector. This relationship enhances their individual success at providing relevant threat information to their constituencies and improves their country's overall cybersecurity posture.

National CSIRTs Outside the Country/Economy

To improve effectiveness and increase capability, national CSIRTs find it essential to build strong relationships with national CSIRTs in other countries and economies. Since all national CSIRTs operate in a unique space with constrained resources, each one benefits from sharing information, expertise, and capabilities, and from collaborating on tool development.

Information about threats, vulnerabilities, and incidents needed for operational situational awareness within the national CSIRT is frequently not unique to the country—many threats and vulnerabilities affect multiple countries or regions. By sharing information with other national CSIRTs, the global community can gain a better understanding of ongoing incidents or potential threats. This approach may even lead to collaborating on tasks such as conducting analyses and determining mitigation actions.

Because of language, cultural, and political considerations, and time and budget constraints, it is not practical for a country or economy to develop strong relationships with all national CSIRTs. However, it may be easier to develop formal and informal relationships with national CSIRTs of countries within your region (or among those with similar languages and cultures). These relationships often take the form of a regional CSIRT[6] or a Regional Internet Registry.[7]

5 For example, in some countries, one CSIRT is only responsible for all government entities (and may be referred to as a government CSIRT, or GovCERT) while another CSIRT is responsible for critical infrastructure and/or the general public.

6 Regional CSIRTs enhance cooperation and facilitate information sharing among national CSIRTs and others in a specific region. Regional CSIRTs are usually voluntary and allow teams that share similar legislative, cultural, and time zone issues to collaborate and coordinate incident handling activities. Examples of such CSIRTs include APCERT, OIC-CERT, and AfricaCERT.

7 A Regional Internet Registry is an organization that manages allocating and registering Internet number resources (e.g., Internet Protocol (IP) addresses and autonomous system numbers (ASNs)) within a specific region of the world. Examples include AFRINIC, APNIC, ARIN, LACNIC, and RIPE NCC.

These organizations can provide national CSIRT participants or partners with access to information and resources they otherwise would not have, while still maintaining day-to-day operations. Examples of such resources may include the sharing of training costs and opportunities to participate in joint incident handling exercises.

Some national CSIRTs may not reach out to other national CSIRTs until it is necessary to do so as part of incident response actions, especially if the activity emanates from an entity within the other national CSIRT's country. A common challenge encountered during this type of effort is that the other national CSIRT may be unresponsive, which can be due to anything from lack of skilled staff or processes, to the national CSIRT only being able to respond to activity related to its chartered constituency (government entities versus private sector entities). If a relationship between the two national CSIRTs did not exist prior to the incident, the effectiveness of the outreach may be limited. However, national CSIRTs find that effective interactions during incident analysis and response build trust and can develop into ongoing collaborative organizational relationships.

> Two of the top factors national CSIRTs have found to contribute to developing global national CSIRT relationships are **collaborating or interacting during incident handling** and **developing personal contacts and associations.**

Many national CSIRTs have also found that personal or individual relationships among people from different national CSIRTs tend to grow into organizational relationships. People who train together or participate in other collaborative events tend to create relationships with each other and then leverage these personal relationships once they are back at their respective organizations. However, if these relationships are not institutionalized, they can fall apart when one of the individuals leaves their organization. As your staff participate in global face-to-face events, ensure they routinely take actions such as adding their new contacts to central repositories and introduce additional team members to the new contacts during future events or collaborations.

> Two events that many national CSIRTs agree foster both individual and organizational relationships are the annual Forum of Incident Response and Security Teams (FIRST) conference and the Annual Technical Meeting of CSIRTs with National Responsibility (NatCSIRT).[8] Likewise, national CSIRTs have found that formal meetings throughout the year with regionally focused groups such as a regional CSIRT or a regional internet registry strengthens those relationships as well.

One of the key challenges national CSIRTs have experienced when trying to develop global relationships and share cybersecurity information is language differences. Many national CSIRTs have found that if they agree to communicate in English they are more successful because they find the language more suited for technical topics. For example, the term phishing loses its meaning when a suitable translation for it is attempted in certain languages. A common regional language or common technical lexicon are good alternatives. For example, community-wide training for national CSIRTs can provide your staff with a common foundation of knowledge and terminology for communicating cybersecurity threats and incidents. These sources of training can include, but are not limited to:

- Software Engineering Institute (SEI)
- Forum of Incident Response and Security Teams (FIRST)
- European Union Agency for Cybersecurity (ENISA)
- SANS Institute

Such technical trainings and certifications will also aid you in conveying your team's credibility to others.

LESSONS LEARNED

- Share information, expertise, and specialized capabilities among other CSIRTs.
- Develop regional and global national CSIRT relationships by
  - collaborating or interacting during incident handling
  - developing personal contacts and associations
  - institutionalizing these activities

8 **first.org** and **cert.org/natcsirt**

Establish Effective Operations

Select Your Services

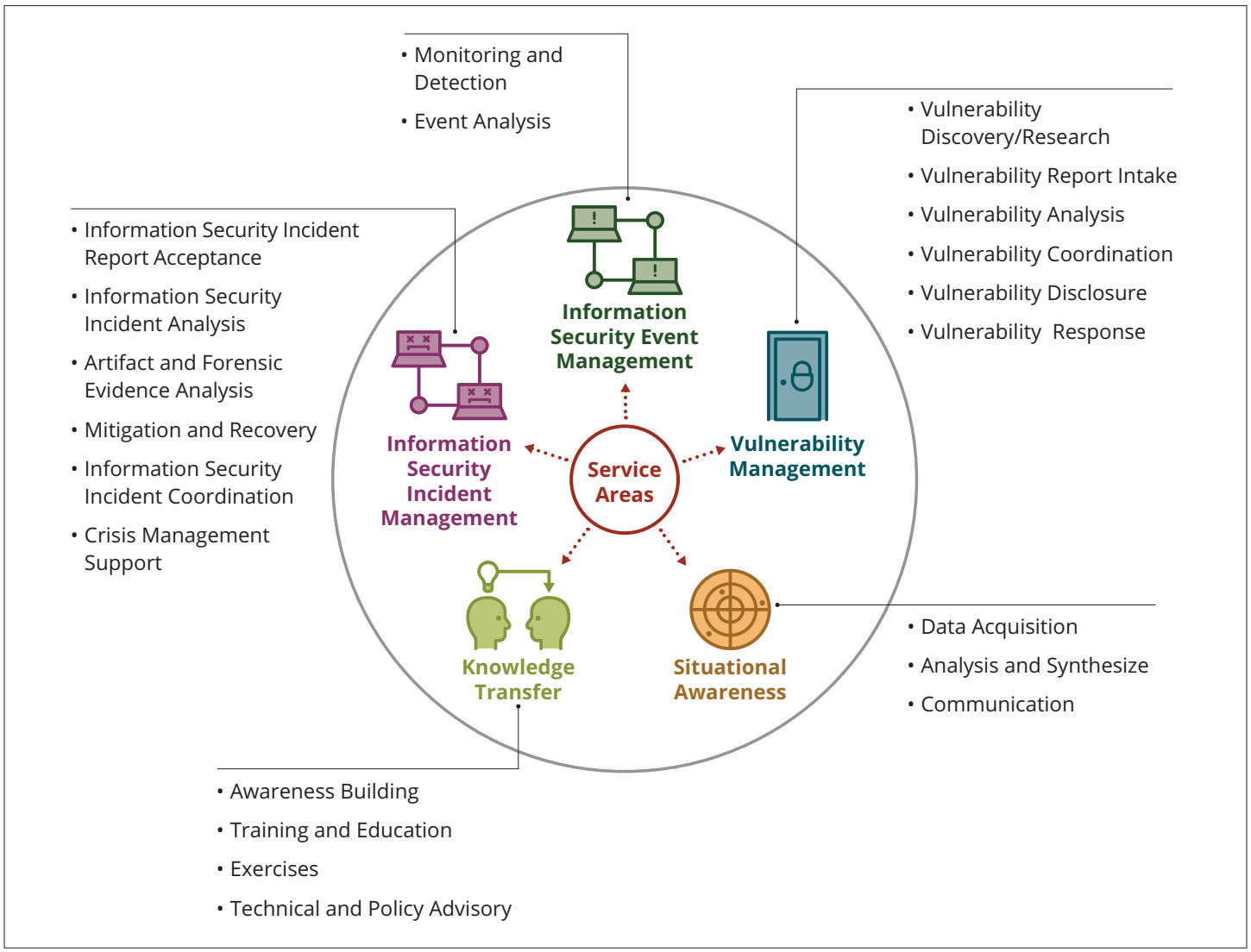
One of the biggest challenges for national CSIRTs is scalability. Since the size of your constituency is likely to be much greater than those of other types of CSIRTs, it is important to provide services that yield the most value. National CSIRTs have found that a key way to do so is to provide information and services that are not readily available to constituents using other means. As previously discussed, many national CSIRTs rely on the feedback obtained from constituents to determine what services to initially provide and what changes are needed over time. There is no consensus on what minimum services a national CSIRT should provide. This reinforces the best practices encouraged by the SEI and others that a CSIRT should start with two or three services, perform them really well, and then add new services over time—as the needs of the constituency evolve and the capabilities and resources of the national CSIRT expand.

LESSONS LEARNED

Provide services with the most value and impact for constituents and adjust as needed.

FIRST CSIRT Services

The FIRST CSIRT Services Framework, illustrated in the diagram below, describes services and functions of incident response teams within a high-level framework in order to assist in a community-wide standardization and the selection and establishment of a team's services portfolio. It is important to note that you are not expected to provide all services, and each team should select its services based upon its mission, constituents, resources, and capacity. The structure of the framework is based on four elements: service areas, services, functions, and sub-functions.[9] Five service areas and their associated services are highlighted in the graphic below.



9 first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Develop Sound Documentation

Documented policies and procedures are required for the provision of consistent, accurate, and trustworthy services. While you may choose not to document every process, at a minimum you should maintain accurate and documented standard operating procedures (SOPs) for your core incident response procedures.

Ensuring your staff maintain, understand, and follow SOPs ensures efficient and accurate response actions when both routine and critical incidents occur. This will greatly contribute to the long-term sustainability and success of your CSIRT. Sound documentation can also help your CSIRT recover from significant national-level events.

Example

Some national CSIRTs have been affected by large-scale national events (e.g., country revolution, constitutional changes). Such events resulted in significant staff turnover, reorganization, and/or changes in CSIRT constituency. While operations in general decreased during these events, and some came quite close to dissolving the CSIRT completely, it was their documentation that aided in preventing that from happening. The loss of senior staff during these events was addressed by quickly placing remaining staff in those vacancies. By following accurately documented procedures they were able to continue carrying out critical functions. New and more junior staff were trained to steadily reestablish the CSIRT's full capabilities and services. When constituencies changed (i.e., increased or decreased), SOPs and services in general were reevaluated and adjusted as needed. While none of these actions were quick solutions, they provided the CSIRT with the foundation needed to recover.

LESSONS LEARNED

Ensure policies and procedures are accurately documented, routinely reviewed, and updated as needed; ensure they are understood and followed by staff.

Determine Information Sources

As a national CSIRT, you may not have intrusion detection sensors that you monitor or direct access to your constituents' network infrastructure; you may depend on constituents and others to report incidents or share information such as indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) of threat actors. However, constituents have varying amounts of accurate information. Some national CSIRTs place constituents in the three following general groups.

THOSE WITH SIGNIFICANT CAPABILITIES	These organizations have a formal and effective information security program that includes highly trained and capable staff and an effective set of tools.
THOSE WITH MODERATE CAPABILITIES	These organizations have an information security program, minimum staff, and some tools. However, they have significant gaps in each of these.
THOSE WITH FEW CAPABILITIES	These organizations do not have effective information security programs and/or adequate resources.

Those in the first group are likely to have the best sources of accurate information and the capabilities to effectively analyze that information. They are usually the best constituents to develop close information sharing relationships with and are the ones most likely to help you analyze and understand an incident.

Additional information sources include other national CSIRTs and regional CSIRTs. You may also choose to subscribe to indicator or intelligence feeds from commercial sources. Since the information used to provide alerts, advisories, and other reports to your constituents usually comes from external sources, timeliness is a challenge. National CSIRTs consider being able to trust their data sources as key to providing timely and accurate reporting. This allows you to spend less time on testing and validating information received.

Unfortunately, it takes time to determine the technical accuracy of an information source to deem it generally trustworthy. National CSIRTs have experienced the need to stop accepting, or to at least thoroughly vet, information from sources that routinely provide inaccurate data or analysis. This can be a sensitive situation if it is a constituent because you need to maintain a relationship with them; however, your technical reputation can be at stake if you further disseminate inaccurate information. In the end, you cannot allow low value communications to impair your ability to effectively communicate with those who have valuable information.

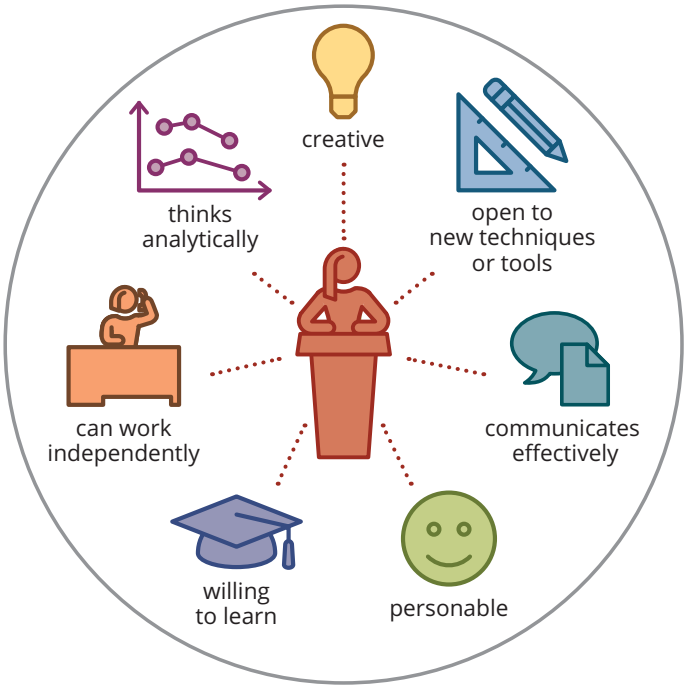
LESSONS LEARNED

Thoroughly vet information from all sources and consider not accepting information from those that routinely provide inaccurate data or analysis.

Address Staffing Needs

Determine Needed Roles and Skills

Competent technical analysts are key to successful national CSIRTs, but the consensus is that it is important to hire individuals who have a combination of technical and soft skills. While it makes the hiring process more challenging, it is highly beneficial to the organization's success to have staff who possess the characteristics below.



Most national CSIRTs favor a model where each person may have one or more specialty skills, but everyone knows how to perform a specific set of basic tasks. In times of crisis, anyone can fill in where needed for these basic tasks. For larger national CSIRTs, it is easier to have more specialists, but smaller teams tend to thrive if some level of cross-training is conducted.

Some national CSIRTs also suggest hiring analysts who are at various skill levels. This is because they initially hired a very small team of analysts that were beginners in cybersecurity and a manager that served as the senior analyst. As the only senior analyst, the manager was frequently given additional responsibilities leading to many areas of work not getting adequate attention. One of the most common additional responsibilities given to the senior analyst/manager was developing relationships with constituents and/or with organizational and policy leaders. This is another example why you should have a member of your staff in a dedicated engagement role.

LESSONS LEARNED

- Hire individuals who have a combination of technical and soft skills, and analysts at various skill levels.
- Designate someone other than the operational manager to perform engagement functions.

Cybersecurity Workforce Development

There are many resources that can be utilized for workforce development and planning. One example is the National Institute of Standards and Technology (NIST) Workforce Framework for Cybersecurity (NICE Framework),[10] which details knowledge and skills required to perform particular tasks; these tasks are then associated with particular work roles that can be used to develop job descriptions, individual development plans, and other workforce development documentation. Ideally, the knowledge, skills, and work roles should be aligned to the services that you provide constituents; therefore, supplementing the FIRST CSIRT Services Framework with the NICE Framework is a best practice for the development or expansion of resources and skills associated with a particular service.

Implement Professional Development Mechanisms

While it is critical to hire the right people and establish effective roles, it is also important to implement mechanisms to encourage ongoing professional development for your staff. This practice will help you retain existing staff and improve your overall capabilities.

Internally, many national CSIRTs encourage implementing something as simple as a "right-hand ride" or "job shadowing" process, which can simply mean pairing junior staff with senior staff to advance their skillset for their current role. It can also mean pairing staff at various skill levels and within various specialties with someone in a different specialty.

These methods have the added benefit of helping the national CSIRT recover more easily and quickly when they lose key experts. National CSIRTs have determined that if they increase the number of their skilled, trained personnel, there is stability across the organization, even if staff move around within it.

10 csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Due to funding issues, some national CSIRTs may need to be more selective in how they source training. However, most acknowledge the importance of encouraging professional development and establishing annual training plans and requests. The table below suggests a variety of professional development approaches.

COMMON TYPES OF PROFESSIONAL DEVELOPMENT	Informal internal training (e.g., self-study or cross-training with other staff)
	Conferences relevant to staff roles and cybersecurity in general
	SANS or other formal technical courses
	Other training based on the skills the national CSIRT is looking to nurture or establish
	Activities through capacity building efforts of partner teams and/or countries

Some national CSIRTs also develop extensive in-house training; however, this approach is most commonly designed for newly hired or junior staff. Sending at least one or two people to key annual global conferences is especially important. As mentioned previously, these events are essential for ongoing development of regional and global engagement and collaboration, and can introduce newer staff to the community at large.

LESSONS LEARNED

Establish plans, funding, and processes for professional development.

Evaluate and Implement Tools

While having the right staff is important to the overall operation of a national CSIRT, it is also important for staff to use efficient and effective incident management and analysis tools. Determining which tools to acquire and implement will greatly depend on what services you provide and your available budget. Since commercial products can be costly and cannot always be modified, many national CSIRTS have found it beneficial to either develop their own tools or customize open source tools that are available. That is why it is important to consider these decisions when determining staff requirements to ensure that appropriate skills have been acquired.

Because of budget constraints, some national CSIRTs operate almost completely with open source tools. These national CSIRTs caution others to avoid getting caught up in maintaining these tools, especially if the staff responsible for doing so also have other responsibilities. Other national CSIRTs have the budget for commercial options yet spend their resources to hire skilled and motivated staff instead. They have discovered that creative employees can maximize the value of open source tools.

The one exception to using open source tools or developing them in-house is when a tool is used in specialized areas, such as data acquisition or artifact and media analysis. There is widespread agreement that using the most common commercial products for these specialized areas prevents mistakes, enables sharing among others, and enables better support requirements for law enforcement reporting. Additionally, many national CSIRTs have discovered that custom scripts and open source tools are good for triaging incidents, but are sometimes lacking some of the features needed to conduct in-depth fusion analysis and correlate incidents or multiple data sources.

While not a widespread concern, some national CSIRTs have experienced lack of trust from constituents who use commercial tools when the national CSIRT does not. Another issue experienced by some national CSIRTs was being advised to acquire proprietary tools. These national CSIRTs were unable to quickly make any needed modifications, and changes usually incurred costs.

LESSONS LEARNED

- Select tools based on the services you are providing and your budget.
- Evaluate tool requirements in conjunction with assessing skills needed to hire the right staff.

Conclusion

While this document cannot cover all of the pressing issues that you will face as a national CSIRT, we hope it leaves you with some best practices and considerations for establishing sustainable and successful operations. When developing your team, capabilities, and services, remember to

- ☐ Understand your environment and gather the necessary information prior to the standup phase.
- ☐ Establish sound policies and governance to enable your team to meet goals.
- ☐ Engage with your constituents, peers, and community to develop and maintain relationships and build trust.
- ☐ Establish effective CSIRT operations through selective consideration of services, policy documentation, and information sources.
- ☐ Continually address staffing, resource, and tool requirements as your mission and capabilities evolve.

In the dynamic field of cybersecurity and incident response, achieving sustainability does not always equate to long-term success. Even after your team is established and operational, it is important to revisit these areas to ensure that services and activities remain aligned with constituencies and missions, enabling both sustainability and success.

Resources

SEI

Cybersecurity Center Development

sei.cmu.edu/our-work/cybersecurity-center-development/

Steps for Creating National CSIRTs

resources.sei.cmu.edu/library/asset-view.cfm?assetid=53062

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

resources.sei.cmu.edu/library/asset-view.cfm?assetid=9221

Other National CSIRT Resources

resources.sei.cmu.edu/library/asset-view.cfm?assetID=505132

Other CSIRT Resources

resources.sei.cmu.edu/library/asset-view.cfm?assetid=505118

FIRST

Forum of Incident Response and Security Teams [various resources]

first.org

FIRST CSIRT Services Framework

first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

NIST

Workforce Framework for Cybersecurity (NICE Framework)

csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)

nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

ENISA

European Union Agency for Cybersecurity (ENISA) [various resources]

enisa.europa.eu/topics

OAS

Organization of American States (OAS) [various resources]

oas.org/en/sms/cicte/prog-cybersecurity.asp

SANS INSTITUTE

Training resources

sans.org

Your feedback is welcome.

If you have feedback you'd like to give on this publication, we would love to hear it. Please send an email to **security-operations@cert.org**

The development of this document was sponsored by the U.S. Department of State, Office of the Coordinator for Cyber Issues and derived from information originally published in a limited distribution report authored by Tracy Bills, Wassie Goushe, and James Lord.

DM21-1071

About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu