



NATO Science for Peace and Security Series  
D: Information and Communication Security - Vol. 54

# Next Generation CERTs

Edited by  
Alessandro Armando  
Marc Henauer  
Andrea Rigoni

**IOS**  
Press



*This publication  
is supported by:*

The NATO Science for Peace  
and Security Programme

Copyrighted material

# Next Generation CERTs

Edited by

**Alessandro Armando**

*University of Genova, Genova, Italy*

**Marc Henauer**

*MELANI, Switzerland*

and

**Andrea Rigoni**

*Cyber Risk Services, Deloitte Risk Advisory, Italy*

**IOS**  
Press

Amsterdam • Berlin • Washington, DC

Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on New Generation CERT: from  
Response to Readiness – Strategy and Guidelines  
Chiavari, Italy  
28–30 March 2017

© 2019 The authors and IOS Press.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system,  
or transmitted, in any form or by any means, without prior written permission from the publisher.

ISBN 978-1-61499-996-6 (print)  
ISBN 978-1-61499-997-3 (online)  
Library of Congress Control Number: 2019946978  
doi: 10.3233/NICSP54

*Publisher*

IOS Press BV  
Nieuwe Hemweg 6B  
1013 BG Amsterdam  
Netherlands  
fax: +31 20 687 0019  
e-mail: [order@iospress.nl](mailto:order@iospress.nl)

*For book sales in the USA and Canada:*

IOS Press, Inc.  
6751 Tepper Drive  
Clifton, VA 20124  
USA  
Tel.: +1 703 830 6300  
Fax: +1 703 830 2300  
[sales@iospress.com](mailto:sales@iospress.com)

LEGAL NOTICE

The author(s) of this publication is/are solely responsible for its content. This  
publication does not reflect the opinion of the publisher. The publisher cannot be held  
liable for any loss or damage that may occur because of this publication.

PRINTED IN THE NETHERLANDS

# Contents

Foreword	v
<i>Gregory Shannon</i>	
Preface	vii
<i>Alessandro Armando, Marc Henauer and Andrea Rigoni</i>	
Acknowledgments	xi
Abbreviations	xiii
Introduction	1
<i>Andrea Rigoni</i>	
<b>Part I. State of the Art</b>	
An Introduction to CERT Types, Services and Organization Models	5
<i>Andrea Rigoni and Davide Veneziano</i>	
Information Sharing to Secure Cyberspace	20
<i>Mark T. Maybury</i>	
<b>Part II. Next Generation CERTs</b>	
Securing Alliance Federation – A Conceptual View on Evolution of CERT Capabilities and Services for NATO Operations	33
<i>Konrad Wrona and Geir Hallingstad</i>	
Cybersecurity Exercises: Wargaming and Red Teaming	44
<i>Lorenzo Russo, Francesco Binaschi and Alessio De Angelis</i>	
<b>Part III. The Experience of CERTs</b>	
The Evolution from SOC and CERT to the Cyber Defence Operation Center	63
<i>Stefano Bordi, Davide Dell’Orto, Antonio Rossi, Federico Rutolo and Umberto Mosca</i>	
Transformation: Evolving from SOC to CERT	82
<i>Luigi Ballarano and Matteo Macina</i>	
Wargaming: The Core of Cyber Training	88
<i>Federico Casano and Riccardo Colombo</i>	
Subject Index	101
Author Index	103

This page intentionally left blank

# Introduction

Andrea RIGONI<sup>a,1</sup>

<sup>a</sup>*Cyber Risk Services, Deloitte Risk Advisory, Italy*

The problems related to cyber security are now a priority for organizations and entities operating in all sectors of society. In fact, the approach used so far in this field is no longer adequate to deal with current threats and new risks arising from the so-called fifth domain. It is therefore essential for organizations to improve and develop the ability to identify, prevent, mitigate, react and respond to cyber attacks according to a readiness-based approach. Another essential component entities have to focus on when dealing with cyber is resilience, namely the ability to prepare for, respond to and recover from cyber attacks. Resilience helps an organization to protect against cyber risks, defend against and limit the severity of attacks, and ensure service continuity despite the occurrence of an attack.

In this perspective, Computer Emergency Response Teams (CERTs) are fundamental pillars of cyber security and their strategic relevance in guaranteeing prevention and reaction in case of cyber incidents is now universally recognized. Their main role is to coordinate, support and monitor the activities of prevention, response and restoration of critical cyber incidents, by enabling and coordinating internal and external communications and by supporting compliance with reference standards and regulations. Because of the services provided, nowadays CERTs are considered the focal points for cyber readiness and cyber resilience, both in the public and private sector.

There is no single way to conceive a CERT: considering its functions and capabilities, a CERT is adapted to the context in which it operates and be targeted on the established goals and the defined mission of the organization. In fact, the role and scope of a CERT are established according to the needs of the relative Constituency. CERTs can be of different types based on the sector in which they operate - academic, commercial, CIP/CIIP, governmental, internal, military, national, etc. - but they all rely on four essential components: governance, people, services and technology.

The CERT Governance encompasses the policies, the key performance indicators, the plans and all the aspects related to the management of the CERT. It should follow specific criteria and be continuously updated and improved in order to be effective. Another key pillar for CERT operation depends on the accessibility of skilled experts to be hired permanently or on an ad-hoc basis. In fact, the recruiting of dedicated people with the correct skillset, as well as a proper defined organizational structure, are critical aspects to support effective operations and proactivity of a CERT. In terms of personnel, the composition of a CERT should contain people with a mix of technical, legal and communication skills and backgrounds. In general terms there are four categories of personnel who should be involved: manager, staff, operational technical team and external consultants. In addition, there are some additional figures as legal specialists or communication experts that could be helpful to have on board.

---

<sup>1</sup> Partner, Deloitte Risk Advisory , via Tortona 25, 20144, Milan, Italy. E-mail: arigoni@deloitte.it

The catalogue of services is the reflection of the CERT's capabilities and is based on the mission, business needs and resources of the organization. The services are the core of the CERT activities and should therefore be structured and tailored to the expectations of the Constituency. Likewise, the technologies in use are a fundamental element for a National CERT, and each component should be easy to use and resilient. Among the various instruments, it is necessary to adopt solutions that support the collection and analysis of intelligence data, both internally and externally. For this purpose, info-sharing platforms allow to promptly receive and exchange information on threats and vulnerabilities, while the adoption of secure communication mechanisms reduces the risk of information disclosure. Moreover CERTs should have a repository that contains information about threats, incidents and related solutions, and the adoption of an automation workflow tool could increase the incident handling capabilities.

Despite the attention paid to these essential aspects, CERTs as conceived so far have not given tangible and sensitive results to the various Constituencies. To date, CERTs have mainly served as technical response teams or public relations bodies. Given the increasingly prevalent cyber needs, there is a need to evolve the role of CERT. The CERTs should in fact perform a function of coordination between the strategic government and the more technical part, in order to be able to address the growing needs and the ever higher expectations of the Constituency. CERTs should therefore focus mainly on the proactive aspects of their role: only an evolution in this sense will in fact make it possible to face the new challenges related to cyber.

The author(s) of this publication is/are solely responsible for its content. This publication does not reflect the opinion of the publisher. The publisher cannot be held liable for any loss or damage that may occur because of this publication.

Part I  
State of the Art



This page intentionally left blank

# An Introduction to CERT Types, Services and Organization Models

Andrea RIGONI<sup>a</sup> and Davide VENEZIANO<sup>a</sup>  
<sup>a</sup>*Cyber Risk Services, Deloitte Risk Advisory, Italy*

**Abstract.** The goal of this chapter is to outline the main characteristics of a CERT based on its type, primary mission, authority on incident response, and capabilities required to achieve the strategic objectives. In particular, different organizational models are thoroughly investigated, outlining the different layouts through which services and capabilities can be offered to the Constituency.

**Keywords.** CERT, Constituency, governance, organizational model, intelligence.

## 1. Introduction

The main objective of a CERT is to act as a reference point in the prevention and management of cyber threats and incidents. CERT's mission and role might be significantly different according to the Constituency but is commonly articulated around the following key areas:

- Act as a reliable and trusted, single point of contact for emergencies;
- Facilitate communication among Constituency, other CERTs and experts working to solve security problems;
- Maintain close ties with research activities and conduct research to improve the security of existing systems;
- Initiate proactive measures to increase awareness on information security and computer security issues;

In order to effectively achieve its strategic goals, the CERT has to develop the required capabilities to detect, respond and prevent threats, manage cyber incidents, and establish Shared Situational Awareness among its constituents. A CERT's operating model and service portfolio also depends on the mission that the CERT decides to pursue. The mission influences how the CERT should be built, and it must be clearly communicated within the Constituency that CERT serves.





## 2. CERT Types

Over the years, the activities and mission of CERTs evolved to reflect the non-homogeneous nature of Constituencies. There are different types of CERT based on their primary constituencies (Table 1).

CERT Type	Primary constituency
<b>Corporate</b>	Internal and external users (employees, consultants, contractors, etc.) in the same organization
<b>Sectorial</b>	Users of specific industries or characterized by common interests (e.g. academia, banking, industrial, etc.)
<b>National</b>	Citizens and businesses that belong to a specific country

**Figure 1.** CERT Types

The primary mission of the CERT, its authority on incident response, and the capabilities required to achieve its strategic objectives derive from the constituency the CERT is serving, as depicted in Figure 2.

	<i>Corporate CERT</i>	<i>Sectorial CERT</i>	<i>National CERT</i>
 <i>Primary Mission</i>	<ul style="list-style-type: none"> <li>Prevention and cyber incident response</li> <li>Corporate Situational Awareness</li> <li>Point of Contact for Cyber Incidents and Crisis</li> </ul>	<ul style="list-style-type: none"> <li>Prevention and Incident Response coordination</li> <li>Sectorial Shared Situational Awareness</li> <li>Point of Contact for Industry/Sector cyber incidents</li> </ul>	<ul style="list-style-type: none"> <li>Prevention and coordination of critical cyber incidents</li> <li>National Shared Situational Awareness</li> <li>Point of Contact at National level</li> </ul>
 <i>Authority on Incident Response</i>	<ul style="list-style-type: none"> <li>Distributed or Centralized</li> </ul>	<ul style="list-style-type: none"> <li>No or limited authority (only coordination and structured information sharing)</li> </ul>	<ul style="list-style-type: none"> <li>Depending on national strategy (typically limited)</li> </ul>
 <i>Relationship focus</i>	<ul style="list-style-type: none"> <li>Internal / external</li> </ul>	<ul style="list-style-type: none"> <li>Internal / external</li> </ul>	<ul style="list-style-type: none"> <li>External</li> </ul>
 <i>Primary communication tools</i>	<ul style="list-style-type: none"> <li>Phone, secure corporate mail / secure mail, web portal, Instant Messaging</li> </ul>	<ul style="list-style-type: none"> <li>Phone, secure mail / web portal</li> </ul>	<ul style="list-style-type: none"> <li>Phone, secure mail, web portal</li> </ul>

**Figure 2.** CERT types and their capabilities

### 3. CERT reference model

To achieve its mission and meet its objectives, the CERT has to adopt and develop a well-defined operational model. Four components are vital to build a first-in-class CERT that is able to effectively prevent, respond and manage cyber security incidents and emergencies (Figure 3).

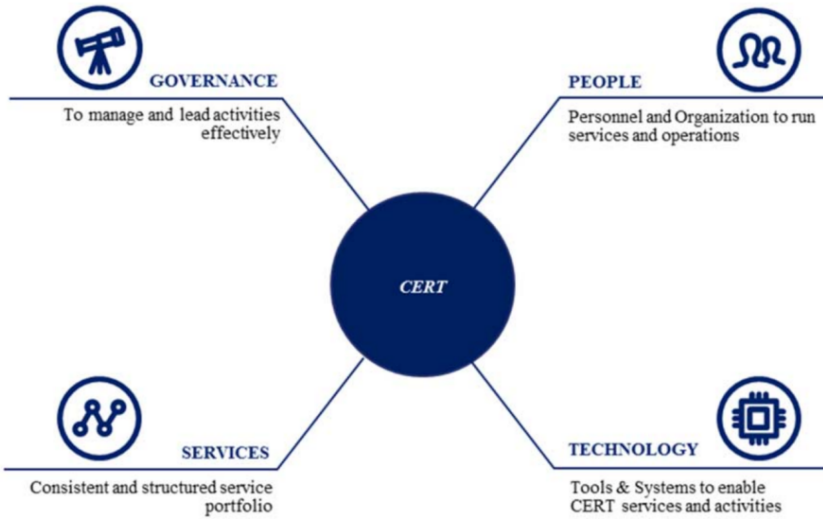


Figure 3. CERT reference model

### 3.1. Governance

CERT Governance should respond to specific metrics in order to be effective and continuously improved. Information on the number of engagements and the effectiveness of procedures to resolve incidents plays a paramount role in this area. The maturity of a CERT can be measured by e.g. the absence or abundance of intelligence gathered in the incident management process. Some indicators are essential to get along the maturing process of the CERT. These parameters need to be identified as early as CERT's inception, so that it would be possible to demonstrate the ability to target strategic goals timely and effectively.

The following diagram (Figure 4) summarizes, at a high level, a common approach to performance measurement applied to CERT.

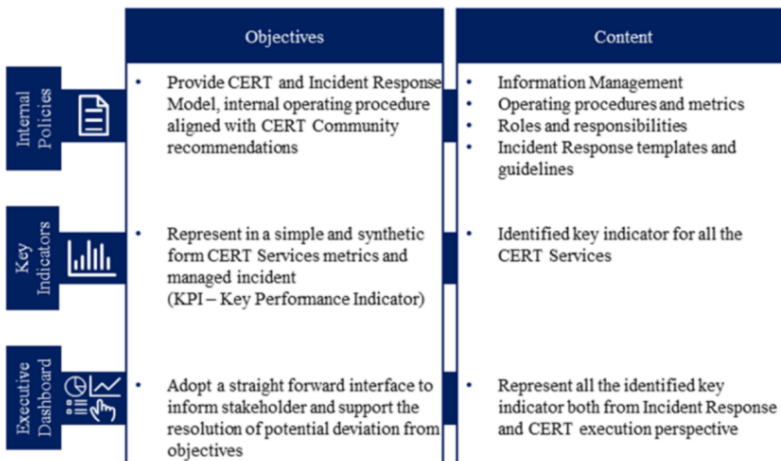


Figure 4. CERT governance model

### 3.2. People

The nature of work within a CERT is such that it exposes its human resources to stress for prolonged timeframes. Taking this into consideration, the selection of people who can manage the pressures of the job becomes one of the success factors of CERT performance.

One of the key pillars for CERT operation is the recruiting of dedicated people with the correct skillset. In addition to the standard background check, personal characteristics and skills should be examined for successful selection.

Figure 5 lists the additional skills and personal characteristics required for CERT staff.

Personal characteristics	Skills
<ul style="list-style-type: none"> <li>● Integrity</li> <li>● Diplomacy</li> <li>● Understanding of their limits</li> <li>● Time management</li> <li>● Attention to detail and subtle signals</li> <li>● Written and oral communication skills</li> <li>● Ability to follow policies and procedures</li> <li>● Ability to contribute to teamwork</li> <li>● Problem solving</li> <li>● Analytical and deductive skills</li> <li>● Ability to prioritize</li> </ul>	<ul style="list-style-type: none"> <li>● Good ICT skills</li> <li>● Understanding of ICT security principles</li> <li>● Understanding of the vulnerabilities and weaknesses of hw/sw components and human safety</li> <li>● History of the internet and its evolution</li> <li>● Information security risks</li> <li>● Network protocols</li> <li>● DNS</li> <li>● Network services and applications</li> <li>● Technological security countermeasures</li> <li>● Security of operating systems</li> <li>● Knowledge and ability to identify intrusion techniques</li> <li>● Cryptography: specifications, weaknesses, tools</li> </ul>

Figure 5. CERT staff skills

The organizational structure of the CERT is a critical aspect to support effective operations and proactivity. The number of critical events, analyzed sources, and Info Sharing relationships often influence the internal organization. The composition of CERT should contain people with a mix of technical, legal and communication skills. Figure 6 demonstrates a possible model of CERT.

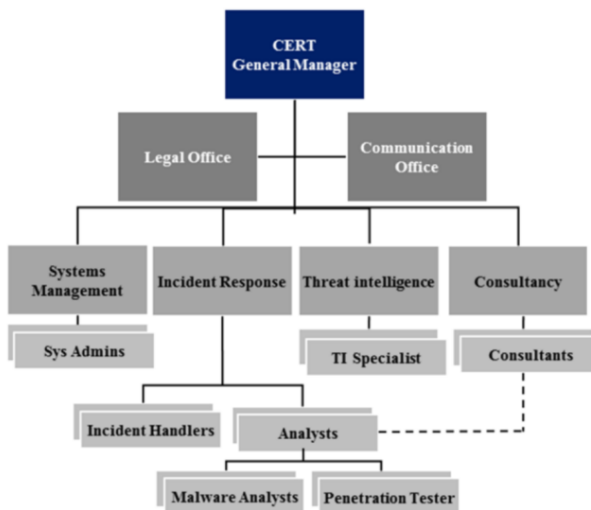


Figure 6. CERT organizational structure example

The size of the team depends on the amount of attacks and incidents the Constituency has to deal with. It can range from a few people to a team of 20 or more. Job rotation may be required with 24/7 shift work to allow regular presence of the team to respond to and analyze incidents. This allows limiting the exposure to cyber threats and the staff's stress coming from the incident response activities. It also increases the level of sensitivity and knowledge of all operational steps for running the service.

CERT will be expected to participate in conferences and regular courses for professional development and for increasing its knowledgebase.

### 3.3. Technology

Technologies in support of CERT are mainly aimed at accumulating, evaluating and sharing information in a controlled manner, ensuring necessary support for emergency incident response as well as in securing sensitive data and communication (Figure 7). Each component should be easy to use and resilient. It is worth considering splitting CERT related IT from the rest of ICT services as this limits and prevents operating disruptions. This may seem an uneconomic way of running ICT systems. However, in the event of a critical incident the recovery is much faster and more efficient with a separate set up.

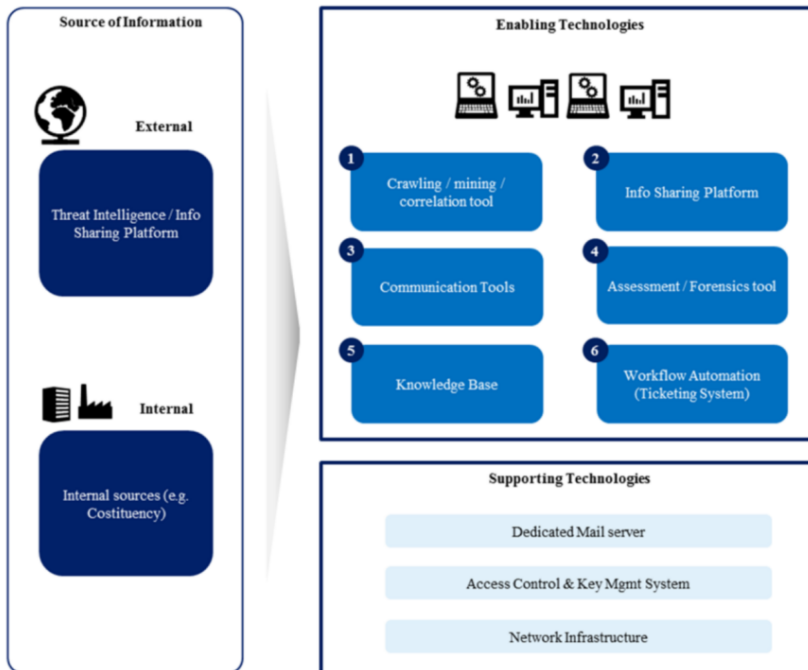


Figure 7. CERT enabling technologies

Among key enabling technologies, the CERT must consider adopting:

- **Crawling / mining / correlation tool:** threat Intelligence enabling technologies for collecting, searching, and analyzing information on threats, violations, etc.

- **Dedicated info-sharing Platforms:** technologies dedicated to the acquisition / exchange of information and their propagation towards the Constituency and security solutions aimed at prevention and monitoring;
- **Secure Communication Tools:** coordination and communication tools with adequate security levels (e.g. authenticated / encrypted communications);
- **Assessment / Forensics tools:** technologies supporting investigative activities and Digital Forensic;
- **Knowledge Base:** tools that support analysis and the definition of a standard modus operandi;
- **Workflow Automation (Ticketing System):** technologies that automate and track activities, in particular Incident Response ones;

#### 4. CERT services

A structured and well-defined service catalog tells internal and external stakeholders interacting with the CERT which capabilities can be leveraged. Core services are selected according to the missions, business needs, and available internal resources and can be grouped in three main categories:

- **Reactive services:** mainly consists of post incident analysis and coordination activities carried out to mitigate threats or attacks such as compromised hosts, malware, vulnerabilities or other type of cyber incidents;
- **Proactive services:** aimed to detect and intercept attacks and incidents before they might take place and prevent actual impacts on the production systems. The information collected, generated, analyzed, and correlated by the CERT is also disseminated to the constituency and the other stakeholders for protecting their assets and avoid being target of an attack;
- **Security Quality Management services:** includes services for the review and improvement of the security posture of the organization and the constituency<sup>1</sup>.

Each CERT may choose to develop and implement a different service portfolio, based on the strategic objectives and Constituency that has to serve. The most common core services a CERT may want to consider including in its portfolio and implement are detailed below.

##### 4.1. Incident Response

A key service of a CERT is Incident Management. Its phases, roles and responsibilities must be clearly structured to manage a cyber incident timely and effectively. This process is normally defined in five phases (Figure 8).

---

<sup>1</sup> ENISA, CSIRT Services, <https://www.enisa.europa.eu/topics/csirt-cert-services>

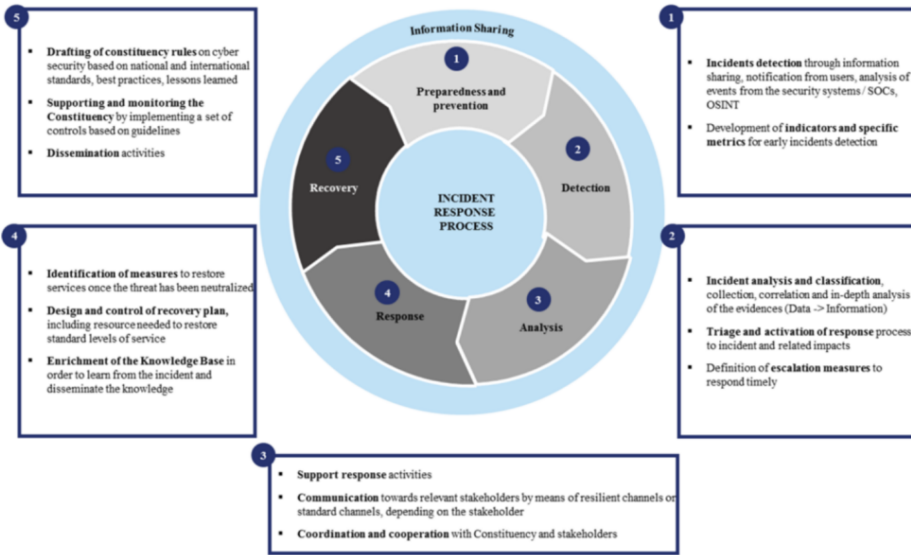


Figure 8. CERT Incident Response process

- **Preparation and prevention:** this phase involves establishing and training an incident response team, acquiring the necessary tools and resources, establishing incident response capabilities and processes to be ready to respond to threats and recover from incidents. It also includes establishing CERT’s communication strategy, defining communication staff member’s roles and responsibilities, disseminating rules, guidelines and procedures to communicate, cooperate and share information with CERT stakeholders.
- **Detection:** the detection phase commences at the onset of incident management. Internal and external sources and signals are encoded to enable the detection of incidents. Data from automated systems (i.e. SIEM), notifications from users, notifications / reports from external entities such as authorities, other CERTs and organizations are collected and correlated to identify any potential incident.
- **Analysis and Triage:** after an incident has been detected, the analysis process begins by classifying it. The key tool to be used here is the classification matrix, which helps to identify the “ordinary” incidents handled on daily bases by the SOC and those carrying more significant impact that need to be dealt by the CERT. If the incident is considered to be of a high-impact, i.e. at Level 2, 3, and 4, then the next phase of the process is triggered. Classification of the incident is key to determine the priority of the response.
- **Response:** the response phase should include pre-defined processes to mitigate the incident based on its classification. Key factors at this stage are the definition of communication procedures, stakeholders’ proactive involvement, the definition of roles, responsibilities, and common goals of the involved actors, and well-defined procedures and workflows.
- **Recovery:** once the immediate emergency has been resolved, CERTs must communicate short, medium, and long term plans according to defined procedures and tools. In this phase, the CERT gathers lessons learned on the incident and share them with Constituency / stakeholders, confirm that expected



results and response activities have been successful, and coordinate any follow-up activity to check corrective measure effectiveness through monitoring activities. The performance of the whole process, in terms of efficiency and effectiveness to identify improvements is also reviewed.

#### 4.2. Cyber Threat Intelligence

This capability is essential to mature incident prevention and management within the constituency. Cyber Threat Intelligence represents the critical element of a dynamic cyber security strategy that leverages multiple sources of information to have a better understanding of how relevant threat actors operate and the risks they pose to a specific organization based on actual vulnerabilities. The goal is to integrate information sources in the detection phase with the contextual knowledge of the Constituency and correlate with the team of analysts. Merging of this data through the intelligence and experience accumulated by the staff of the CERT allows identifying "weak signals" of imminent attacks, distinguishing the weakest or most sensitive points of Constituency. Figure 9 presents the intelligence building model employed by the FBI .

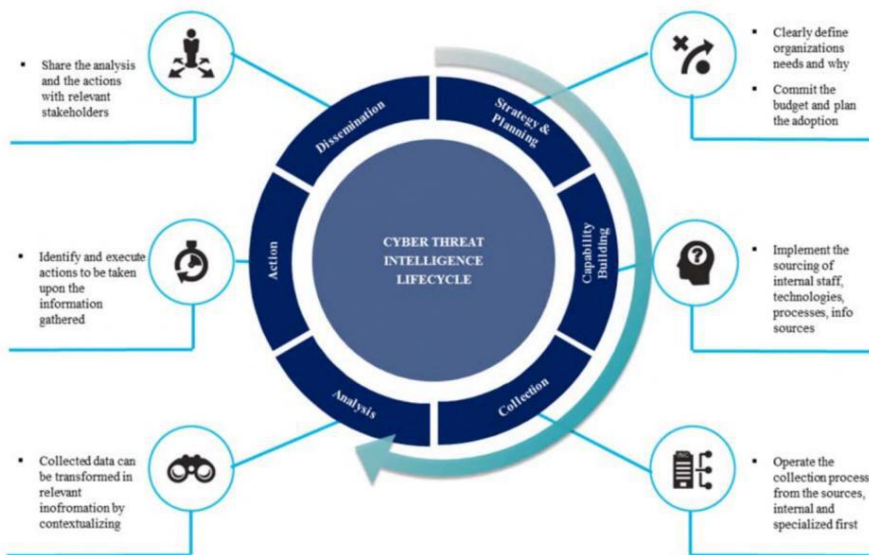


Figure 9. CERT Cyber Threat Intelligence process

The cycle begins with the acquisition of three types of Intelligence that differ from each other in terms of scope and mode of collection, acquired from open and closed intelligence source, Threat Intelligence Providers, and external stakeholders such as Government agencies, other CERTs or internal organizations:

- **Human Readable Intelligence:** new vulnerabilities, threats, malware, but also attack modes with impact on assets. They require analysts to identify preventive and monitoring measures;

- **Machine Readable Intelligence:** elementary feed (IP, URL, IoC) that might have an impact on the assets. They can be acquired from security solutions automatically;
- **Intelligence Acquired Through Active Research:** violations linked to information leakage, phishing, e-fraud, brand abuse, etc. They require analysis for validation and subsequent response and / or containment action;

Once acquired, specific enabling tools for analysts, such as inventory and CTI platforms designed to aggregate data from multiple sources and that put them into security solutions, are leveraged to identify information relevant for the Constituency (Figure 10).

The contextualization of intelligence requires a deep knowledge of the Constituency assets; this evaluation allows to understand what priority must be assigned to prevention and monitoring actions.

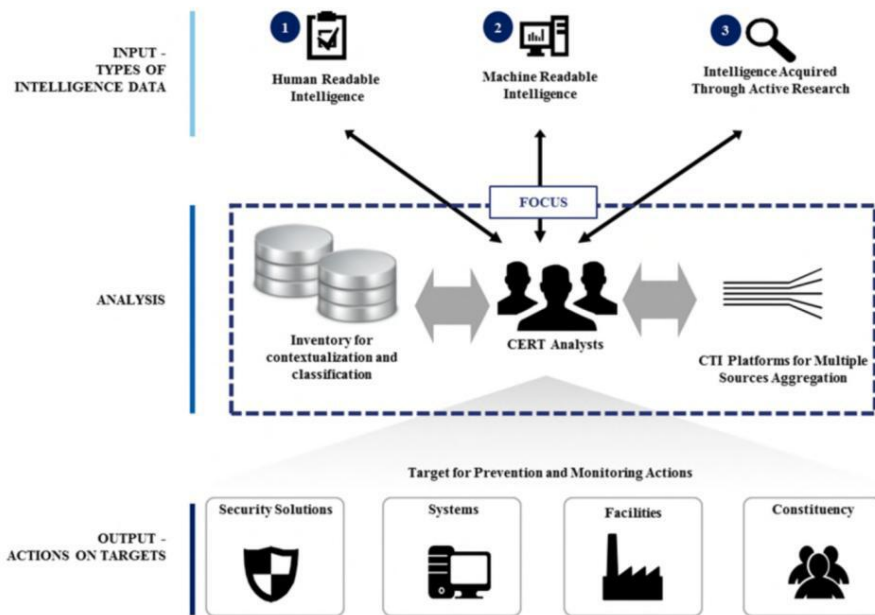


Figure 10. Threat Intelligence data acquisition and analysis

### 4.3. Information Sharing

Information sharing is the foundation upon which correct operations of CERT are built. This process must be able to follow the information throughout its entire lifecycle (input, processing, output), maintaining the adequate levels of classification. The process should be able to manage any change to the information occurring throughout the lifecycle. In order to achieve this, it is essential to refer to a clear map of involved parties, the classification policies, and the different information sharing means and methods adopted, both internally and to the Constituency.

The information sharing process consists of four consequential phases (Figure 11).

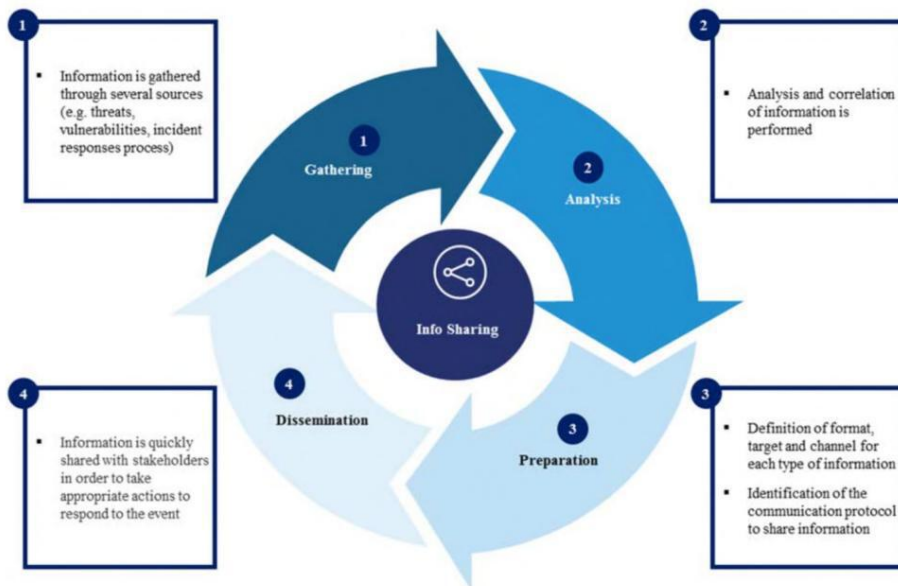


Figure 11. Information sharing process

All shared information should be classified according to an information confidentiality protocol. The Traffic Light Protocol is a common example of this. It provides a simple and intuitive schema for indicating when and how sensitive cybersecurity information can be shared within the global cybersecurity community of practice.

Information sharing initiatives may include:

- Dissemination of alerts, bulletins, advisors in which CERT sends information within the Constituency including description and technical details (e.g. IoC) on new threats and vulnerability using appropriate format using TLP protocol to classify the information;
- Periodic events such as meetings and workshops which can be limited to a subgroup of the Constituency / relevant stakeholders based on confidentiality of topics;
- Reports, which can be published through a CERT restricted area in which Constituency's members can log in to read or download the material.

#### 4.4. Red Teaming

Red Teaming Operations Services can be used to significantly raise the overall level of CERT cyber awareness.

Red Teaming Operations assess the cyber readiness and awareness of the CERT based on cyber threat scenarios derived from IT security assessments. With this process, it is possible to validate the materialization of the cyber threat scenarios on an operational level. Controlled incidents are executed based on predefined scenarios, like spear phishing and social engineering.

Red Teaming Operations focusses on three core elements of Information Security:

- Cyber: represents the online world, the Internet as well as corporate Intranets and all other computer networks;
- Physical: the buildings, the desks, the safes, and the IT physical infrastructure;
- Human: represents the employees, customers, clients, third parties that bind the cyber and physical world together;

Red Teaming exercises are a cornerstone to build effective cyber defensive capabilities and are essential part of a CERT complete services portfolio. The key success factors are:

- Right business and technical mixture: red teaming exercises need to combine the right amount of technical and business understanding to become useful and representative;
- Thorough understanding of the context: for a red teaming exercise to be successful, it is necessary to gain a thorough understanding of the actor being simulated. Their objectives, means and methods need to be correctly designed into the exercise scenario in order to make the simulation realistic.
- Improvement of defensive capabilities: through Red Teaming exercises, the CERT Team can develop and improve expertise, training at the same time not only their technical skills, but also their ability to work with Incident Response and Info Sharing tools, following the pre-defined processes (CTI, IS, IR);
- Tailored threat driven scenario selection and execution: not some random attacks to random objectives. The best planning comes from in depth understanding of the constituency and of its risks, in order to translate them into scenarios that matter, combining risk and threat management approaches.

## 5. Common Organizational Models for CERTs

The organizational structure of the CERT is a critical aspect to support effective operations and proactivity. CERT authority and delivery model describe the control and governance that the CERT has over its own actions towards its constituents and existing organization, regarding computer security and incident handling functions.

In terms of responsibility and coordination, the CERT can position itself in different ways. It can operate with full authority, leading the constituency to perform the actions or the response steps necessary to enhance the security posture of the organization, or to recover from an incident. It can operate in a shared-authority regime, collaborating with the constituency to influence the decision-making process concerning what actions should be taken. Lastly, it can adopt a model that does not attribute authority to the CERT, limiting its scope to advisory actions to the constituency, without any decision-making power on its own.

Based on the authority model, the CERT can operate with a distributed, centralized or coordinating delivery models.

### 5.1. *Distributed*

For CERTs operating according to this model, the organization utilizes existing staff to provide a “virtual” distributed CERT, which is formally chartered to deal with incident response activities (Figure 12). Across the organization, individuals are identified as the appropriate points of contact for working as part of the distributed team based on their

expertise with various operating system platforms, technologies, and applications, or based on their geographic location or functional responsibilities.

There is no unique identified CERT, and incident response is handled by local system, network, and security teams as part of their day-to-day work.

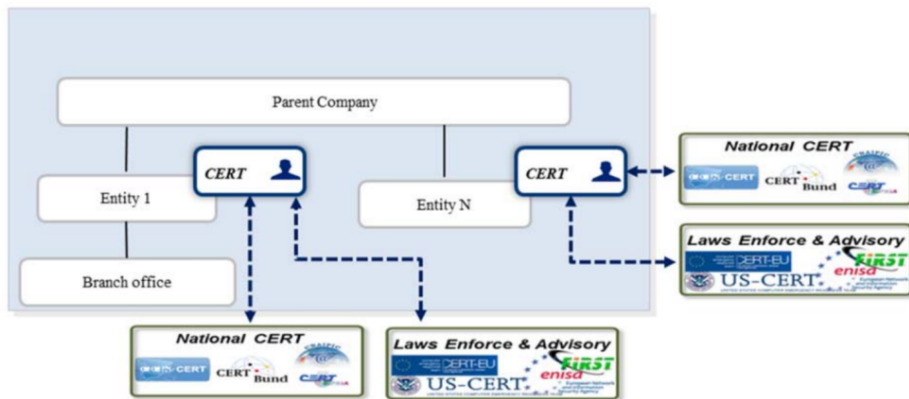


Figure 12. CERT Distributed model

For CERTs operating according to this model, responsibility for incident response remain at the local level, All Security processes and key Security technologies (like SIEM, IDS/IPS, etc.) are duplicated and locally managed.

The strengths of this model are that the staff is familiar with local systems and business functions (leading to an effective incident response) and reaction time can be faster at site, also thanks to the relationships and contacts with law enforcement and related agency which are based locally.

However, this model suffers of lack of a comprehensive view of security posture, a limited coordination and information sharing, difficulties in coordinating incident response for wider attacks and high expenses due to duplication of technologies and competencies.

## 5.2. Centralized

This model is a fully staffed, dedicated CERT that provides the incident handling services for an organization (Figure 13). In many cases, team members spend 100% of their time working for the CERT. However, this type of model could also be provided using part-time staff on a rotation basis. The team is centrally located in the organization and is responsible for all incident handling activities across the constituency or enterprise.

This model provides a very stable structure for building incident handling capabilities, support a clear mechanism for proactively managing organization's computer security risks, and defining the appropriate levels of prevention and mitigation activities.

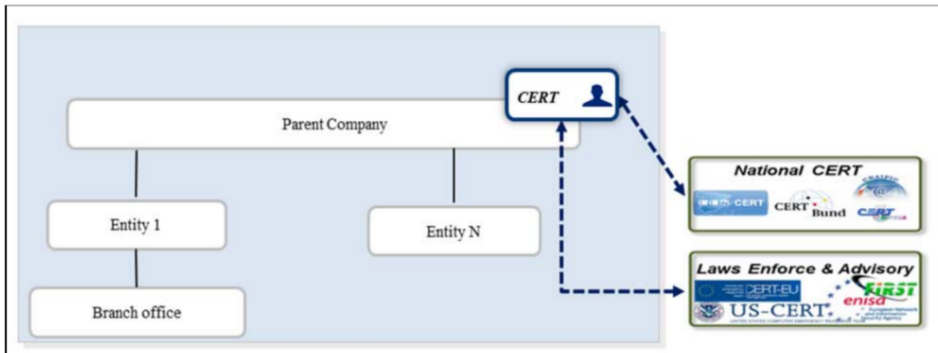


Figure 13. CERT Centralized Model

Responsibility for incident response is assigned centrally to CERT, which, at the global level, coordinates incident response and other security processes. In addition, key security technologies (like SIEM, IDS/IPS, etc.) are centrally managed with master/slave configuration.

For CERTs operating according to this model, a unique vision and cybersecurity strategy applied across the company and a comprehensive and overall view of security posture is assured, reducing spending in redundant staff and technology at the same time. The CERT acts as a single point of contact over law enforcement and other CERTs' communities.

However, especially in large organizations, it may be difficult to manage technology changes across geography and there could be a lack of local governance and accountability due to shared responsibility with local CTO/ICT departments leading to difficulties to enforce and standardize policies and eventually delays in incident response.

### 5.3. Coordinating

The CERT coordinates and facilitates the handling of incidents across a variety of external or internal organizations, which could include other CERTs. Coordinating CERTs usually have a broader scope and a more diverse constituency (Figure 14). What makes this model unique is the set of services provided and how they are tailored towards helping other organizations deal with incident handling issues.

Global CERT coordinates and facilitates incident and vulnerability handling activities across a broad, diverse, constituency. This coordination can involve sharing information, providing mitigation strategies and recommendations for incident response to the Local CERT.

Responsibility for incident response is shared between local and global CERT, with the global CERT coordinating local CERTs for incident response and other key security process.

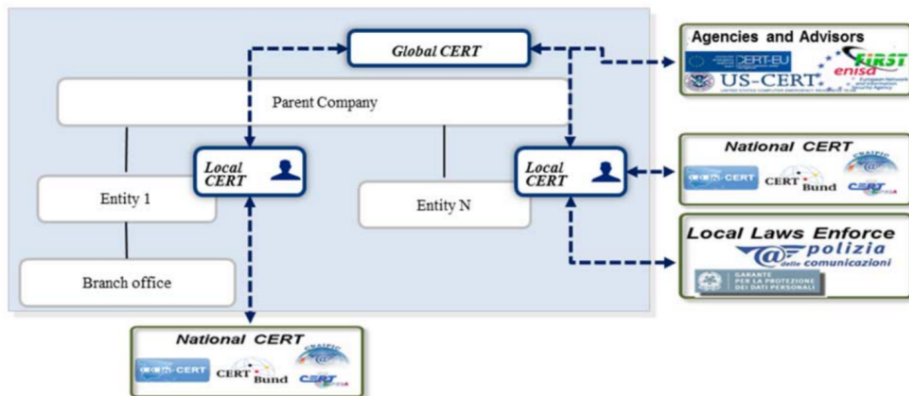


Figure 14. CERT Collaborating Model

For CERTs operating according to this model, a common set of shared security policies, standards and related processes have to be defined so to achieve the global strategy with effective local enforcement and incident response team whilst providing a central trusted point of contact towards the external cyber security community. The CERT has to establish a center to disseminate information about threats, vulnerabilities, and cyber security incidents (information sharing) in order to maximize the ROI by mixing local and global capabilities.

This model, however, requires a high effort to keep up standardized processes, technologies, procedures, etc. across geography and results may vary depending on the real local capability (primarily technical and organizational skills).

## 6. Conclusions

The definition and foundation of a CERT and its practices cannot be dictated by a narrow and rigid approach. A CERT is not a monolithic, fixed entity, but the provided capabilities shall be adapted and tailored to effectively allow the CERT to achieve its strategic goals and mission.

Four components are vital to build a first-in-class CERT that is able to effectively prevent, respond and manage cyber security incidents and emergencies. A Governance model, to allow achieving a high degree of effectiveness and ensure continuous improvements, the right people with the correct skillset, a structured and well-defined service catalog to present to internal and external stakeholders which capabilities can be leveraged and supporting technologies to automate the collection, analysis and sharing of information in a controlled manner.

The organizational structure of the CERT is also a critical aspect to support effective operations and proactivity and allow the required flexibility.

CERT authority and delivery model describe the control and governance that the CERT has over its own actions towards its constituents and existing organization, regarding computer security and incident handling functions. Based on mission,

Constituency and the available internal resources, CERTs can be set up upon different authority models (full authority, shared authority, no authority) and can operate with a distributed, centralized or coordinating delivery models.

## **References**

- [1] ENISA, CSIRT Services, <https://www.enisa.europa.eu/topics/csirt-cert-services>

The author(s) of this publication is/are solely responsible for its content. This publication does not reflect the opinion of the publisher. The publisher cannot be held liable for any loss or damage that may occur because of this publication.



# Information Sharing to Secure Cyberspace

Mark T. Maybury<sup>a,1</sup>

<sup>a</sup> *The MITRE Corporation*

**Abstract.** In an increasingly interconnected world, it is essential for all entities to have a common strategy involving each cybersecurity operations center, in order to increase the overall system's resilience.

The sharing of cybersecurity information is the first step to tackle when defining this common strategy, both at the sectoral and regional level. This is of particular relevance above all since it allows for the creation of a cybersecurity information-sharing ecosystem. Industries, Universities, Governments, private stakeholders and critical infrastructure providers are the main actors involved in this network. In general, the characterization of threats follows the information exchange (threat sharing) and is based on three fundamental aspects: cyber adversary tactics, techniques and procedures (TTPs).

In order to be effective, the common strategy should be principled, preventative, proactive and partnership-focused: it should not be abstract, but should follow a pragmatic approach by seeking to invest in affordable and effective solutions. In the near future, the human intervention will no more be necessary for the protection of computers: computers themselves will be responsible for acknowledging and sharing incidents, analytics and exercises, in order to increase their cyber resilience.

**Keywords.** Cybersecurity Information sharing ecosystem- Threat sharing- Common Cybersecurity strategy- Human-machine autonomy

## 1. Introduction

Our increasingly interconnected world faces an increasingly congested, competitive, and contested global commons [2]. Increases in advanced persistent threats, exponential growth in vulnerabilities and increasing dependency on critical infrastructure, industry and government on complex software systems is driving risk. Increased national efforts at cybersecurity resilience (e.g., [nccoe.nist.gov](http://nccoe.nist.gov)) together with over \$3 billion in venture capital invested in 2016 in cybersecurity promises new protections, along with some new challenges, such as investments in block chain. Modern Computer Emergency Response Teams (CERTs) must evolve to address increased threats, vulnerabilities and consequences, which have increased risk against national economic and military centers of gravity. Key stakeholders in cybersecurity information sharing include, but are not limited to end users, chief information security officers (CISOs), chief information officers (CIOs), computer security incident response teams (CSIRTs), chief privacy officers (CPO), cybersecurity program managers, regulators and a sprawling number of National Cyber Security Centers on the government side. This article discusses modern cybersecurity challenges and risk, cybersecurity information sharing policies and

---

<sup>1</sup> Vice President of Intelligence Portfolios, Director, National Cybersecurity FFRDC, The MITRE Corporation 202 Burlington Roads Bedford, MA 01730

organizations, effective cybersecurity policies and strategies and concludes with future directions.

## 2. Challenges and Risk

Threat actors, from nation states to transnational criminals, have increased attacks targeted at exfiltration of intellectual property, identity theft, extortion via ransomware, attacks on integrity and destructive attacks on cyber physical systems. Figure 1 illustrates some of the largest data breaches including attacks against banks, social media accounts, tax systems, retail accounts, dating sites, logistics, voter databases and election systems. The scope and span of these attacks illustrate that cross-sector protection is essential and no industrial sector is a safe harbor. Attacks have occurred from a variety of vectors including insider threats, supply chain attacks, and engineer/employee error.

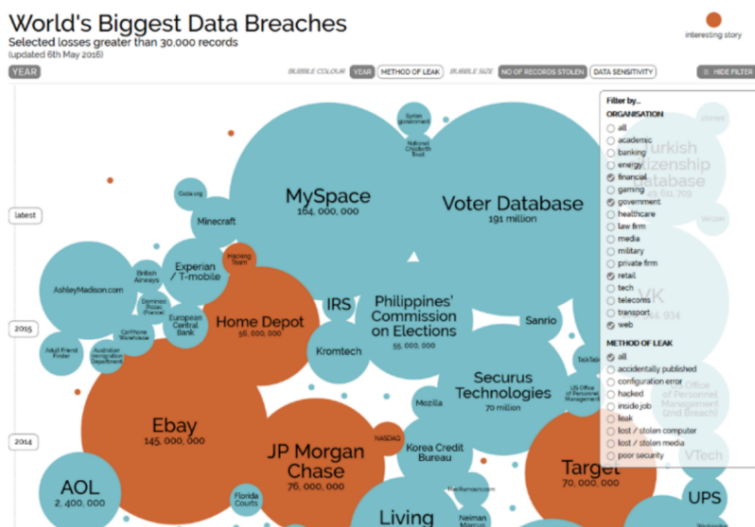


Figure 1: World's Biggest Data Breaches

Source: [www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks)

The quotes in Figure 2 illustrate some of the challenges faced by many cyber security operations centers. These include the difficulty of retaining very scarce but essential expert talent as cybersecurity adversaries can be highly skilled, resourced, and require an agile and expert human response. In addition, legal and policy restraints (e.g., privacy) often limit cyber defender's situational awareness. Assessment of systems can also slow transition and upgrading of security protections. And defenders often suffer from insufficient threat intelligence, information overload because of excessive false positives, over focus on compliance instead of risk management, and insufficient focus on genuine threats and sometimes a lack of awareness of what they should protect the most, i.e., the "Crown Jewels".

“We don’t bother filing requirements because the engineers will never deliver.”

“We can’t patch our sensors because of security won’t let us change version numbers.”

“Phishing campaigns? Our cloud email provider blocks those. We hope. We have no idea what’s coming at us.”

“All I do is look at the same false positives all day. Can’t someone fix this thing?”

“SSL break and inspect? We wish. The lawyers will never let us do it.”

“Oh those other analysts... I have no idea what they do all day.”

“I wish the boss would stop calling us to ask about the latest [threat report | shiny product | breach] everyday. It’s chewing up all our resources.”

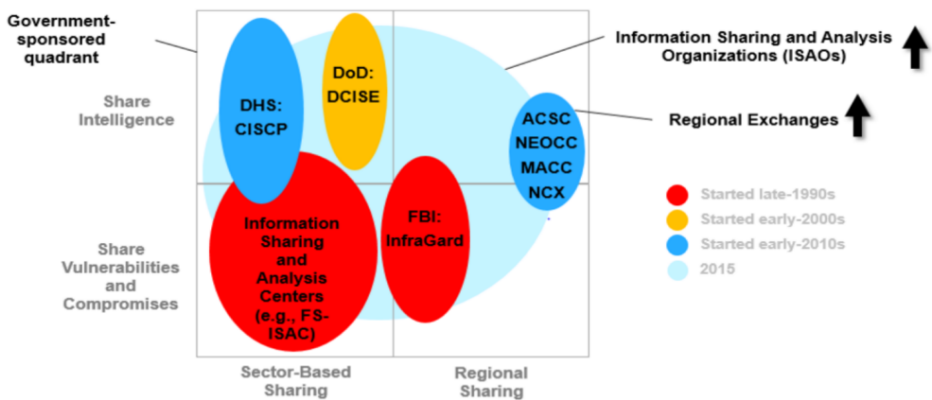
“It would be nice if I could spend some time actually catching bad guys and not dealing with the compliance police.”

“Our one good malware analyst bailed for better money. What are we going to do now?”

Figure 2: Some Cybersecurity Defense Challenges

### 3. Cybersecurity Information Sharing

Figure 3 illustrates the cyber information sharing landscape in the United States. The figure characterizes the kinds of information sharing organizations in terms of what they share and with whom they share it. The types of information shared can include intelligence about threats or vulnerabilities within systems being defended. The organization can either be focused on sector sharing or regional sharing. For example, the Department of Homeland Security’s Cyber Information Sharing and Collaboration Program (CISCP) and the Department of Defense’s Defense Industrial Base Collaborative Information Sharing Environment (DCISE) are both examples of intelligence sharing organizations within a particular sector. There are also sector specific organizations that focus on sharing vulnerabilities and compromises. For example, there are a number of Information Sharing and Analysis Centers (ISACs) in specific sectors such as the Financial Services ISAC (FS-ISAC) or the Electricity ISAC (E-ISAC). There are also organizations which share information across regions. For



• Cyber Information Sharing and Collaboration Program (CISCP) • Defense Industrial Base Collaborative Information Sharing Environment (DCISE) • Financial Services ISAC (FS-ISAC) • Advanced Cyber Security Center (ACSC) • Northeast Ohio Cyber Consortium • Mid-Atlantic Cyber Center (MACC) • National Cyber Exchange (NCX)

Figure 3: U.S. Cyber Information Sharing Landscape

example, the FBI’s InfraGard (infragard.org) is a partnership between the federal, state, and local law enforcement agencies and private sector institutions in industry and academia to share timely information with and among defenders to mitigate threats to US critical infrastructures and key resources. Other examples of regional information sharing organizations include Informational Sharing and Analysis Organizations (ISAOs) such as the Advanced Cyber Security Center (ACSC), the Northeast Ohio CyberConsortium, the Mid-Atlantic Cyber Center (MACC) and the National Cyber Exchange (NCX). These ISAOs provide cross-sector information sharing.

#### 4. Cybersecurity Information Sharing Ecosystem

Figure 4 illustrates at the macro level the cybersecurity information sharing ecosystem [3]. These systems incorporate organizations across industry, academia, government and non-profits. Using different icon colors, the figure illustrates how industry (orange), university (red), government (green), stakeholders (yellow) and critical infrastructure providers (black) work together to share cybersecurity information. Peer to peer sharing is shown with a dotted line, cyber threat intelligence sharing is shown in solid lines. The diagram shows relationships between ISACs, ISAOs, and CERTs, illustrating important interdependencies of threat, vulnerability, and incident sharing within and across sectors as well as emergency response and international partners.

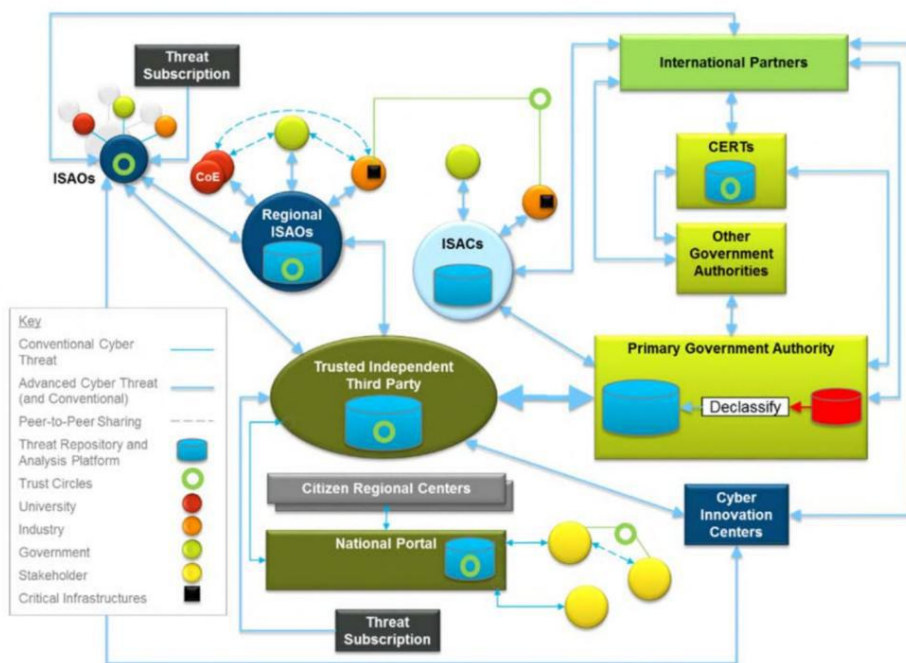


Figure 4: Notional Macro Sharing Ecosystem

### 5. ISACs and ISOAs

Figure 5 illustrates the current range of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISOAs). As show in color coding, ISACs and energy (red), finance (green), state (light green), retail (orange), defense (brown), health (purple), maritime (blue). The so-called life line critical infrastructures (finance, electricity, communications and water) were the first to be established. Additional ISACs where established in additional federal and industrial sectors (e.g., defense, transportation, chemical, food and agriculture, healthcare, natural gas). More recently new topics have emerged such as aviation, automotive, retail, and supply chain) as well as some state specific ones (e.g., Indiana, Arizona, Maryland, Southern California). Also, in recent years cross regional or cross sector Information sharing and Analysis Organizations (ISOAs) have been formed in areas such as legal, sports, and maritime security. For example, the Advanced Cyber Security Center [4] is a non-profit consortium across industry, academia, and government that focuses on cybersecurity research and development, education and thought leadership in New England to address advanced cyber threats.

ISACs originated in the late 1990s and President Obama issued the 2015 Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing and directing the Department of Homeland Security (DHS) to encourage the development of ISOAs. This included more efficient granting of clearances for private sector in critical infrastructures and more collaborating with ISOAs via the DHS National Cybersecurity and Communications Integration Center (NCCIC). It also resulted in establishing an ISAO Standards Organization Cooperative Agreement to the University of Texas at San Antonio (UTSA) with support from the Logistics Management Institute (LMI) and the retail Cyber Intelligence Sharing Center (R-CISC). The ISAO Standards Organization is a voluntary, transparent, inclusive and action oriented entity focused on creating practical voluntary standards and best practices.

## Information Sharing and Analysis Centers (ISACs) Information Sharing and Analysis Orgs (ISOAs)

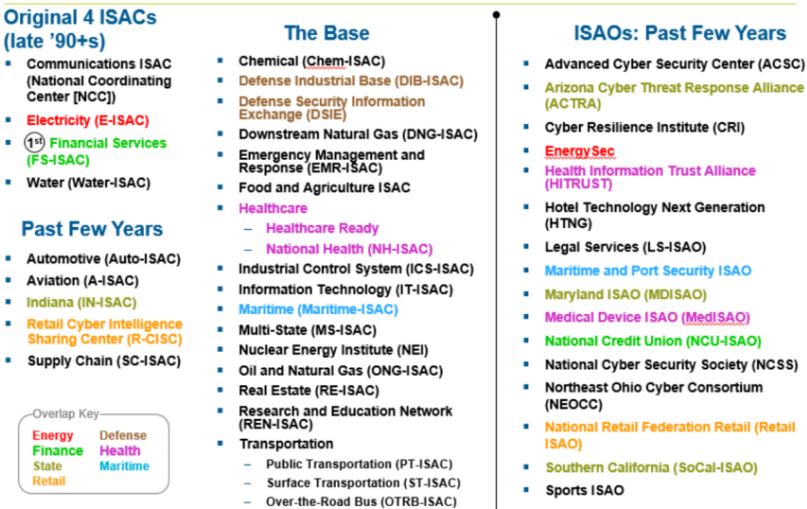


Figure 5: Information Sharing and Analysis Centers and Organizations