Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran

Ali Naseri and Omid Azmoon[1]

[1] **Department of Information and Communications Technology, IHU University**
Tehran, Iran

Abstract

Attack to software, network and system is cause of computer security incidents. Computer Security Incident Response Capability (CSIRC) prevent from attacks by responding, predictive and safety quality management services. Computer Security Incident Response Team (CSIRT) provides these services. In this paper, modeling is proposed for deployment of CSIRT and structure for providing services is described. This model is implemented in a case study in a telecommunication company in a province of Iran and results are expressed.

Keywords: *CSIRC, CSIRT, Constituency, Computer Emergency Response Team (CERT).*

1. Introduction

Computer Security Incident Response Team (CSIRT) provides services and supports for preventing, handling and responding of computer security incidents like crash the services, malware distribution, unauthorized access, improper use and combined attacks [1]. CSIRT provide three services that are classified to responding services, predictive services and safety quality management services [2]. For efficient CSIRT operational framework, policymaking frameworks, quality assurance, flexibility and compatibility must be attended [3]. In this paper, modeling is proposed for deployment of CSIRT in awareness, support, disaster relief, and inhibition of the security environment of information exchange, technical services, including investigation of incidents and vulnerabilities, identification and assessment, counseling, education and information network security in the areas inside and outside of companies. The modeling process includes assessment, the steering committee, identify the entities involved in creating a CSIRT, the structure of the CSIRT, identify interactions with domestic and foreign institutions and the process is working and interactions. This model is surveyed in case study in a telecommunication company in a province of Iran and results are expressed. In continue, CSIRC is surveyed and then requirement for establishing of CSIRT is described. Next, model is proposed and case study is expressed and analyses.

2. CSIRC

2.1. Advantages

Aim of CSIRC is rapid and effective response to computer and network attacks. Therefore, CSIRC response to events by systematic process, evaluate security of infrastructures of hardware and software, help personnel for more effective and quicker services, prevent loss or theft information, use of incident information for future and more powerful protection, develop Standard Operating Procedures (SOP) priorities of organization and more quickly and efficiently respond, deal with legal issues occurred during the events [4].

2.2. Types

Different structures are proposed for CSIRT by missions, goals, requirement and services. Teams may be established in different sections like commercial, governmental, military, research and development, IT, … and have different structures like management, services, organizational model, … . Therefore, CSIRTs are divided by shape, size and function to internal, national CSIRTs, coordination centers, analysis centers, manufacturer's team and incidents response service. In first step, CSIRT responses to actual security incidents and decreases attack effects. Then statistics and reports of incidents in all fields are synchronized in order to determine security position of the organization and vulnerabilities. Finally, CSIRT play roles like protecting the systems, detecting, diagnosing and analyzing security damages, protecting against destructive activities, cyber security incidents coordination and effective response to computer attacks.

CSIRTs have different organizational models such as the available security teams, centralized model, and distributed model, combined and coordinating model. It is better to use centralized models in small organizations while combined model acts in the best manner for large and disperse covered organizations and centers.

Authority of CSIRT is at three levels, full, shared, no authority. First CSIRTs had no authority and commonly be national or academic type. In local CSIRTs, other levels of authority are needed [5].

2.3 Incidents Management

All processes and actions relating to incidents must handle by CSIRT include detect, triage, analyses and response. Incident management includes vast duties from services to functions such as handling vulnerabilities and harmful codes, training, security warnings and … . Incident response process has different stages include preparation, diagnosis and investigation, limitation, uprooting and restoration, activities and supports after removing the incidents [5] [6].

2.4 Implementation

For implementation of CSIRT stakeholders must be identified. Managers must Support, then plan of project are developed. Other steps are: Gathering information, Identification of constituency, definition of mission, funding, determination of level and range of services, determination of organizational model and authority and reporting structure, identification of required resources including staff and equipment and infrastructure, definition of interactions and interfaces, definition of roles and responsibilities, documentation of workflow, development of policies and procedures, development of implementation plan and request feedback, declaration of a formal CSIRT activities, definition of methods for performance evaluation, support for each element having a CSIRT [5] [6].

3. The Proposed Model of CSIRT

3.1 Needs

Needs and requirements are extracted from sessions by managers and directors and surveyed from experimental documents. Important and usual demands are: establishment of centralized and independent unit, establishment of strategic council, control of computer security incidents in the least time and minimize damage, prevention of accidents by secure systems and prediction of security attacks, risk analysis and evaluation of network status, the training of experts staff and increase skill of computer issues of personnel, attention for security incidents, provide ad hoc and periodic reports, evaluation of security tools and periodic test of permeability and security of applications, provide a copy of the configuration information of the company's equipment and update documents.

3.2 Structure

a. Missions: CSIRT missions are determined by sessions with directors and managers include: effective control of incident, prevention of incident, improvement of security by identification of risks and threats, network monitoring, preservation of data sources, promoting computer knowledge of user, attention of security of software, development of external stakeholders and provide security services for applicants by receive tariff, support and promote cyber security.
b. Types: Types are combination of internal by high priority and provide services for foreign applicants by low priority. CSIRT of Telecommunication Company can be converted to CERT, because of management of networks traffic of provinces and by support from government and security associations.
c. Sections and Services: With regard to missions, five sections are necessary: technical operations for incident control and response coordination, education and research for security consultation and training, technical analysis section for analysis incident and damaging codes, support section for development of security tools and maintenance and configuration, customers section for provision agreements service.
d. Model: Features of proposed model are: centralized unit of full-time professionals, distribution of number of employees in strategic positions in the organization and the city, addition and combination of reports by central team, high level analysis and provide strategies by central team, implement strategies by members of teams, faster response to incidents by distributed members of team, transfer skills and knowledge to areas of responsibility by distributed members of teams.
e. Requirements: Infrastructure and technical requirements are include: communication (like telephone and fax), equipment of CSIRT site (like emergency power system, CCTV, physical security, laptops, printers, digital cameras, audio recording and data storage for keeping records of accident, necessary software and applications), elements of network infrastructure (like valid IP addresses, domain, encrypted email system by PGP with filtering and capability of search for internal and external communications, a secure portal with important information of mission and recommendations and et al., secure configuration of network equipment such as routers for the screening of traffic using ACL, configure a firewall to control access to/from the network, computers and servers), suitable OS depends on skills of team members and type of network performance and costs vary due to the flexibility and generality, applications of incident response team (AIRT) (ability to pursue the incident with support built into the console and comprehensive incident management), technology and communication tools for transfer advice and warnings, virtual private and peer to

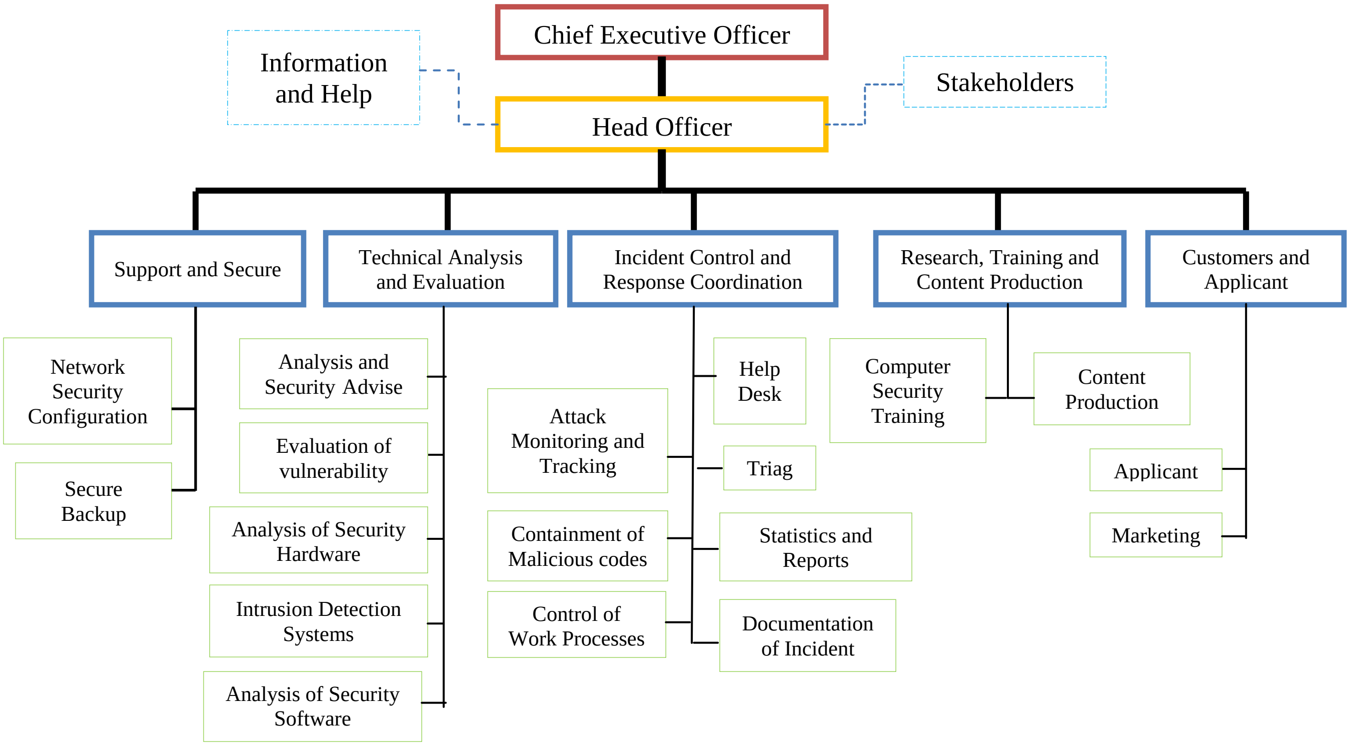
Chief Executive Officer
Information and Help
Head Officer
Stakeholders
Support and Secure
Technical Analysis and Evaluation
Incident Control and Response Coordination
Research, Training and Content Production
Customers and Applicant
Network Security Configuration
Secure Backup
Analysis and Security Advise
Evaluation of vulnerability
Analysis of Security Hardware
Intrusion Detection Systems
Analysis of Security Software
Attack Monitoring and Tracking
Containment of Malicious codes
Control of Work Processes
Help Desk
Triag
Statistics and Reports
Documentation of Incident
Computer Security Training
Content Production
Applicant
Marketing

Fig. 1. The Proposed Model of CSIRT Organization

peer networks, legal tools like TCT for Unix, development of backup systems for the last line of defense, development of tools and software(like firewall, Intrusion and Detection Prevention Systems (IDPS), network analyzer, detection and prevent wireless interference, logging events, spam and URL filtering, antivirus and antispyware).

4. Case Study: Telecommunication Company in a Province of Iran

In a province of Iran, managers of Telecommunication Company (TC), department of Information Technology (IT), department of Guard (GU), department of Data (DA) and Financial Section (FS) play role in creation of CSIRT. An internal CSIRT needs interaction with the authorities of physical security, constituency representatives, the organization information technology authorities, telecommunication section, media communication or public relations, business managers, legal consulates, law enforcement, human resources and security risks management section. In table 1, implementation of the proposed model of CSIRT for a telecommunication company in a provience of Iran is explained in detail.
Figure 2 shows CSIRT interactions of a telecommunication company at time of handling incident.

In diagnosis phase, signs of incident are reported by ICL users/data subscribers (by telephone, fax, email or on-line forms in TCL-CERT portal) to relief desk for users/subscribers in team central section. These signs are combined with reports of TCL-CERT laboratory software and equipment (such as warnings and the recorded incidents)/ status of operators and data department monitoring systems information (such as transfer and switch systems stoppage) and information technology department (such as applied programs incidents, servers and components of the network) /information obtained from public observations and security information and sent to triage phase after recoding in TCL-CERT database.
In triage phase, in case that the signs don’t indicate vulnerability or computer security incident, they are blocked (such as failure or noise of the subscribers cable communication or slow public traffic), otherwise, all gathered reports are classified and prioritized and sent to incident /vulnerability analysis phase after recording in TCL-CERT database.
Analysis phase is performed by incident/vulnerability analysis experts in assessment and analysis section in TCL-CERT laboratory. Determining type and estimating intensity of the incident and prioritization on the basis of the damaged sources sensitivity and its potential effects are the most important factors which are performed in this

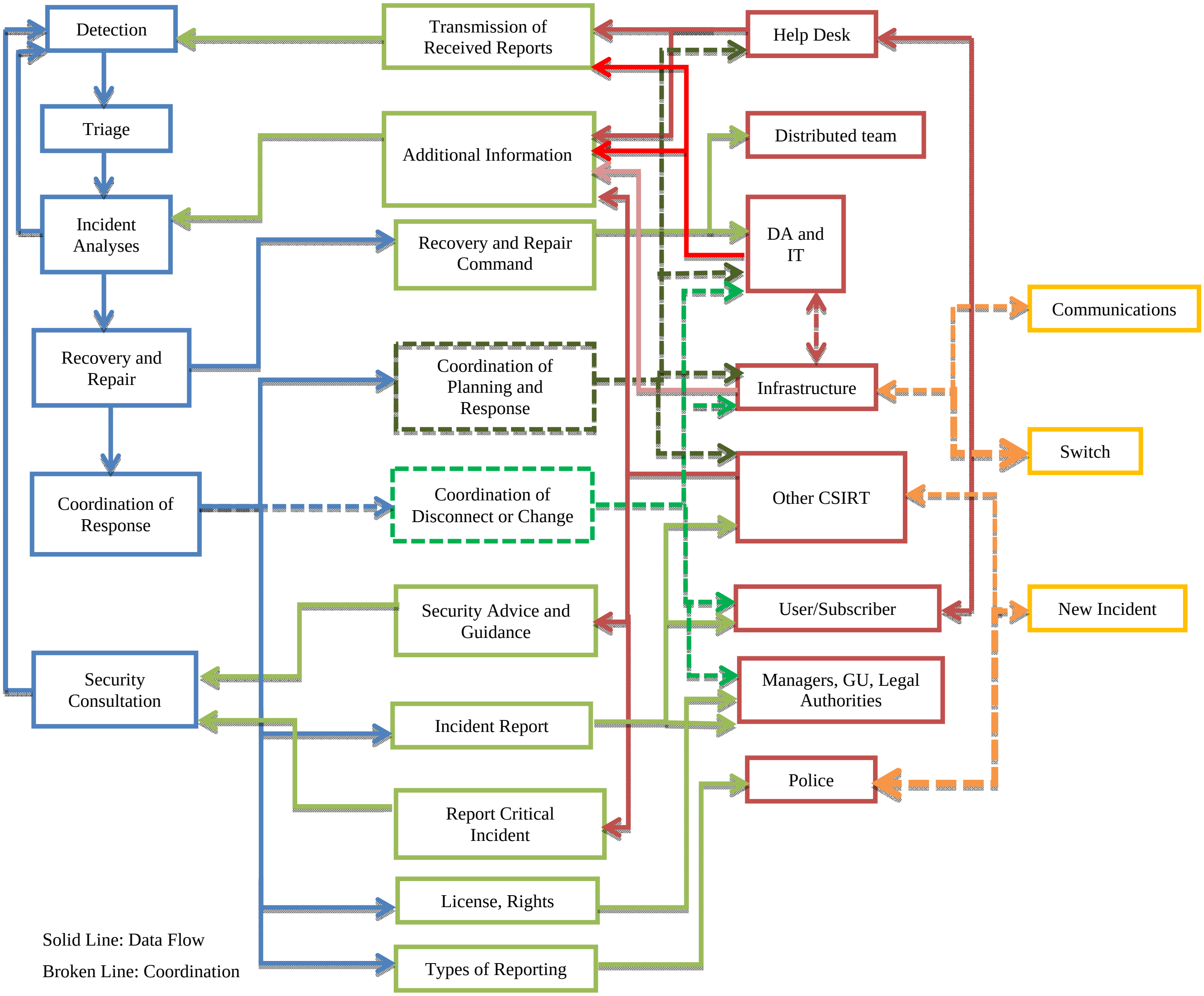

Figure 2: Flowchart of CSIRT in a Province of Iran

phase. If necessary, complementary information is obtained from relief desk of users or subscribers /data and information technology departments/infrastructural NOC/Maher departments or other CSIRTs of the province telecommunication colonies.

Response coordination section should coordinate with directors and authorities of a Telecommunication Company (for internal incidents) /common representative (for external incident), data and information technology departments /infrastructural NOC (if necessary) in case that execution of the response requires stoppage of the user /subscriber or changes in the related communication. Response is executed by distributed team members / data and information technology departments. Incident report is sent to contaminated user/ subscriber for information and in case that the incident requires legal follow-up, it is referred to legal unit of Telecommunication Company / Justice Administration.

This model is implemented and survey for 6 month and results are indicated in Table 2. Total member of CSIRT is 112 include 24 government employees, 6 responder, 30 coordinator, 12 leader, 30 member and 10 for other works. Reports are added and statistics extracted from them, 437 cases are happened, response to satisfaction is asked and categorized in 4 levels, percentage of satisfaction is summarized in Table 2. Response to importance of problem is asked too and categorized in 4 levels, percentage of importance is summarized in Table 2.

Table 1: Implementation of the Proposed Model by Telecommunication Company in a Province of Iran

Description	**Department in TC**	**Interactions of Internal CSIRT**
Telecom CSIRT, Entire company including applicants from the security services. Universities, Registration, Documentation and property records, Banks.	Internal TC: IT, DA, GU External TC: IT of ministries and universities and companies	Constituency Representatives
Provide infrastructures (transmission systems, switches, routers, etc.) Assignment of network services (Internet, Intranet, MPLS, PTMP, etc.) to subscribers (government and private) Management of Information Technology (Web, DB applications, anti-virus, firewalls, etc.)	DA, IT	IT
Provide telecommunications links	Telecom Infrastructure	Telecommunication
Report of incident Training Alert	Public Relations, Communications Portal	Media Communication and Public Relations
Marketing Financial support	Financial and Economic Managers	Business Managers
Rulings of computer crimes	Department of Justice	Legal Consulates
Inspection and follow-up enforcement by the police	Police, Protection Unit	Law Enforcement
Report of incident Presenting symptoms and progressive and provide additional information during the response	Employees, Users	Human Resources
Assessment of threat Identification of financial sector assets Determination of risk	Security Administration , IT, FS	Security Risk Management

Table 2: Statistical Results from Reports

Satisfaction Level	**4 (High)**	**3**	**2**	**1 (Low)**
Problems (437 cases)	203 or 46.45%	228 or 52.17%	5 or 1.14%	1 or 0.23%
Importance Level	**4 (High)**	**3**	**2**	**1 (Low)**
Problems (437 cases)	289 or 66.13%	145 or 33.18%	3 or 0.69%	0 or 0%

5. Conclusions

Computer Security Incident Response Team (CSIRT) prevent from attacks to software, network and system by responding and management services. In this paper, model for deployment of CSIRT is proposed and structure for providing services is described and implemented in a case study in a telecommunication company in a province of Iran and results are expressed.

References

[1] C.Alberts, A.Dorofee, G.Killcrece, R.Ruefle, M.Zajicek , "Defining Incident Management Processes for CSIRTs: A Work in Progress", CMU/SEI, 2004.

[2] J.Bailey, "Integrating a Leadership and Team Building Module in Community Emergency Response Team Training", Arkansas Tech University, 2009.

[3] G.Killcrece, R.Ruefle, "Creating and Managing Computer Security Incident Handling Teams (CSIRTs)", Software Engineering Institute, Carnegie Mellon University, 2008.

[4] K.Scarfone, T.Grance, K.Masone, "Computer Security Incident Handling Guide", U.S. Department of Commerce, National Institute of Standards and Technology NIST SP 800-61, 2008.

[5] M.West-Brown, D.Stikvoort, K.Kossakowski, G.Killcrece, R.Ruefle, M.Zajicek, "Handbook for Computer Security Incident Response Teams (CSIRTs)", Software Engineering Institute, Carnegie Mellon University, 2003.

[6] G.Killcrece, K.Kossakowski, R.Ruefle, M.Zajicek, "State of Practice of Computer Security Incident Response Teams (CSIRTs)", Software Engineering Institute, Carnegie Mellon University, 2003.

Ali Naseri is Professor of Department of Information and Communications Technology, and Chair for Faculty of Information Processing of IHU University. He has twenty years research experience in processing and computing fields and radar processing. Dr Naseri is also an advisor of Information and Communications Technology Ministry of Iran.

Omid Azmoon is Master engineer of Department of Information and Communications Technology of IHU University. He has ten years research experience. His researches have focused on data fusion in radars network. He currently works in Iran Communications Industries.