ANALYSIS OF ISSUES AND CHALLENGES IN ESTABLISHING AND OPERATING CSIRTs IN PAKISTAN

By
Hasnain Shafiq

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Islamabad, Pakistan, in partial fulfillment of the requirements for the degree of MS in Information Security

May 2023

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Hasnain Shafiq** Registration No. **00000327573**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ MS Policy, is free of plagiarism, errors, and mistakes, and is accepted as partial fulfillment for the award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and foreign/ local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: **Brig Imran Rashid, PhD**

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/ Principal) _____

Date: _____

DECLARATION

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and acknowledgments.

Hasnain Shafiq

May 2023

DEDICATION

This thesis is dedicated to

MY TEACHERS, PARENTS & SIBLINGS

for their love, endless support and encouragement

ACKNOWLEDGEMENTS

I am grateful to Allah Almighty for giving me strength to keep going on with this thesis, irrespective of many challenges and troubles. All praises for HIM and HIM alone.

I am very grateful to my Project Supervisor Brig Imran Rashid, PhD, Co-Supervisor Col Imran Makhdoom, PhD and GEC members who supervised the thesis / research in a very encouraging and helpful manner. They always guided me with their profound and valuable support that have helped me in achieving my research aims.

I would like to extend my feelings of gratitude towards my father Shafiq ur Rehman and mother Tahira Parveen for their endless support and towards Major Mubashir Raja and Captain Fazal Saadat for continuous guidance and motivation.

Finally, I would like to express my appreciation to all the people who have provided valuable support to my study and whose names I couldn't bring to memory.

.

ABSTRACT

CSIRT is a group of skilled people who have core knowledge of information security and cyber security incidents. CSIRT team prepares for and responds to the computer security incidents. Almost all organizations take their online security soberly and thus acquire services from CSIRT to control their level of online security. Every CSIRT assists their constituency when a security incident happens and proposes solutions and remediation methodologies to protect them in future. The establishment of CSIRT isn't an easy task to be developed by anyone, the detailed and hard activity requires expert people who specializes in this domain, understand the pros and cons for needed methodologies and processes. This research study describes the establishment of CSIRT and also the issues and challenges that people face while establishing CSIRT. Moreover, the concepts, methodologies, needs and limitations of existing techniques that people of developing countries have experienced are discussed. This research has highlighted CSIRT high level policies, Pakistan's cyber-crime law and presented the results of structured literature review investigating the business requirements for establishing a CSIRT. A survey has been conducted for CSIRT need and importance to achieve and understand the security posture of organizations working in the absence of CSIRT in Pakistan.

Keywords: CSIRT, Security Incident, Online Security

TABLE OF CONTENTS

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

Abbreviations

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CERC	Computer Emergency Response Centre
CIRT	Computer Incident Response Team
SERT	Security Emergency Response Team
IRT	Incident Response Team
CMU	Carnegie Mellon University
ICT	Information and Communication Technologies

Chapter 1

INTRODUCTION

Background

Today's world is all about information and informational assets. With the increase of business environment, the stakeholders of information assets are most relevant to their physical and online security. With the advancement in information technology more and more companies are dependent on ICT services. Soon with the passage of time, the companies including the big tech ones realized the need of IS governance or IS management for mitigating cybercriminal efforts to harm their informational resources. Using the modern technologies and service, it has been proven that even the big security infrastructure cannot guarantee the safety against criminal acts or commonly known as cyber-attacks.

To handle cyber-attacks Computer Emergency Response Team (CERT) was introduced in 1988 by the Coordination Center at Carnegie Mellon University (CMU). CERT is a registered trademark of Carnegie Mellon University. CSIRT and CERT are the alternative names of such group, although dozens of names are called for these groups around the world. The team includes group of expert people who specialize in field of IS and possess deep knowledge to handle computer security incidents. After realizing the significance of CSIRT, various countries have started creating their own CSIRTs for securing sensitive information and ICT traffic.

The history of Computer Emergency Response Team is linked with a famous malware known as Morris Worm which paralyzed a large number of internet connected users. In modern World, all big infrastructures and organizations have created and maintained their own CSIRT which thoroughly checks the security incidents and find means to respond back to the incident. Majority of the countries own their National CSIRTs, together with private organizations who are also providing their information security services to the companies, government agencies and academic institutions.

FIRST Organization

Understanding the need of CSIRT, FIRST had emerged as a global leader and premier organization in 1990 which specializes in incident response. Membership of FIRST has been taken up by both major and minor countries globally, providing incident response teams with the resources to respond to computer security incidents more effectively through the

acquisition of tools, best practices, and trusted communication channels with other member teams. First was developed with a motivation to bring together the CSIRTs operational all across the globe to one platform which aims to increase the dividends of incident management, prevention [1]. The aim of FIRST is to enable quick responses to incidents and to facilitate information sharing among the groups of teams that have become members of FIRST.

With the help and support produced by FIRST among the team members, a wide range of cyber-attacks have been resolved together with incidents and security vulnerabilities that have affected as many as millions of computer systems and connected networks to Internet of things.

Together with trust that FIRST has created among various teams coming from a distinct environments, culture and backgrounds; FIRST also provides some of the value added services which are listed below [1]:

- Annual Incident Response Conference
- Publications and Web Services
- Technical Conferences for Security Professionals
- Access to updated best practice documents
- Hands-on classed
- Special Interest Groups

1.1 Problem Area

In digital world, cyber-attack is an attempt to discover, alter, steal, destroy, expose or gain unauthorized access to information asset. A cyber-attack is an offensive methodology followed by the malicious minded people who targets computers, computer networks, infrastructures, mobiles, computers etc., to access data that is not intended for them. An attacker could easily get access to the sensitive information if the computer system or any asset that is holding the information is prone to cyber-attacks. Developing countries are although doing endeavors to create a platform if anyone didn't have yet where such cyberattacks should be entertained by the domain specialists in order to figure out the potential damage if caused or to investigate in depth about the incident, it's origin etc. and to respond back in a minimum time to effectively reduce the impact of incident.

CSIRT is an acceptable solution by the World to overcome the cyber incidents. Pakistan is among the developing countries where problems arise during the establishment of CSIRTs. The major complications create hurdles during educating departments belonging to

various domains about the importance of information security. Getting a mandate from Parliament is one of the most significant factors for data monitoring and compliance of information systems. After which, follow ups and capacity building of Government staff are also mandatory factors that influence the establishment of CSIRTs. Apart from these issues and challenges several other issues e.g. funding, lack of authority of CSIRT and deficiency of skilled people creates interruption in the establishment of CSIRTs. To learn about the issues, a survey should be conducted to analyze the root problems emerging during the establishment of CSIRT in Pakistan.

Problems in the absence of CSIRT

Problem arises when the cyber-attacks could not be controlled and cybercriminals could not be easily caught. There are hundreds of thousands of cyber-attacks happening on each day primarily targeting the huge tech companies to bring down the services and cause a potential damage whereas in the absence of CSIRT, these cyber incidents would not have stopped and the possible origin from where the attacks are launched would have not been identified. Information technology has brought easiness in life but the counter face is in fact far dangerous where the individual's personal data is on risk. The cyber-attacks haven't left any particular organization, the damage spread from big tech companies to hospitals, government agencies, and education institutions.

Giant companies have already hired information security consultants who regularly enforces information security management policies and cross verify the security checks which they have already implemented in their infrastructures. The need of information security management is most significant to restrain from cyberattacks. For this purpose a dedicated team should be produced to keep an eye on the information assets and propose a mandatory policy, plan and procedure to work against the cyber-attacks that could help the business to run faster and smoother.

1.2 CSIRT

CSIRT is a group of talented and expert people who are ready to handle cyber incidents within the organization at the right time. The need of CSIRT has deeply increased with the passage of time as the cyberattacks have gone viral. A huge number of educational, financial, medical and government institutions are hit by cyberattacks on regular basis which ends up making financial, reputational and data loss. CSIRTs have the responsibility of receiving,

evaluating, coordinating, and providing a response to security incidents. In case a cyber incident occurred it is the responsibility of CSIRT to consult its constituency and provide valid guidance and recommendation to handle the cyber-attack and also to protect themselves from further attacks [2]. The need of security is in demand for information assets, this is because a proper mechanism should be followed to handle cyber-attacks.

To protect the integrity of human identity and human valuable resources in an organization, CSIRT has already been established in majority of the developed countries to tackle the cyber-attacks.

ISO / IEC 27001:2013 Standard, which is one of the standards in the field of IS management, IS is defined as "protecting the confidentiality, integrity and availability of information, while features such as authenticity, accountability, unquestionable and reliable can be considered" [3].

Importance and Need of CSIRT

Today each organization is in need of CSIRT to tackle cyber threats. The risk to any organization depends on assets value, resources and reputation that the institution has preserved in market. After analyzing the traffic logs of certain organization, the responsible person generates an event that clearly highlights the incident that is forwarded to the next concerned authority where the incident is investigated in more depth. CSIRT has various group of people whose main concern is to give their best to run the organization smoothly by defeating cyber threats [4]. The mutual cooperation helps them to handle incidents in more efficient way as before. With all this, tools and technology also hold important position in combating cyberattacks.

Following is the group of members that play vital role in CSIRT:

i. Management

Management plays a fundamental role in building a CSIRT on national or on organizational level. These people are behind selecting the technical people whose job is to set up a required infrastructure for making the CIRT operational. Management has the authority to take a decision at any crucial point or give approval for new resources. Management focusses on effectiveness and efficiency that why their work includes developing a security policy, deploying in an organization and exercising it.

ii. Human Resources

In any organization disgruntled employees are always the biggest threat to that organization. In most of the cases employees are behind the incidents. The reason could be

anything despite of they are treated inhumanely. Once it's been confirmed after an internal investigation human resource takes required actions against the suspected employees. Moreover, human resources are meant to hire and handle employee's issues in an organization.

iii. Information Technology

Most of the companies have separate department for information technology and information security. The main difference between them is that IT people are meant to manage the network of an organization which is the backbone of any organization where the data of the people accessing the network is stored on the servers. Whereas the IS people's job is to make the data secure over the network. At the time of incident IT people work collaboratively with IS department to provide the best assistant to reduce the damage.

iv. Information Security

Information security members are trained to tackle cyber incident at the right time. They have the core knowledge of what is going on in the network and how to detect cyber incident. Besides handling the technical domain these people have the knowledge how to protect themselves from any loss. Their job role includes detecting cyber incident, access the extent of damage, containment, investigating the root cause i.e. forensics, and how to recover the normal state.

v. IT/Security Auditor

Many organizations and companies have hired information technology and information security auditors who plays a different but vital role in running the institution effectively. IT auditors are trained in the field of information technology and their job role is to observe whether the procedures are followed efficiently. They conduct the gap analysis in the organization where they investigate that the procedures are not appropriate for that they prepare set of rules and procedures to apply in the required areas where lack is been observed. Similarly, IS auditors learn about the organization's IS policy and thoroughly investigate security policy to find any loop holes in case the IS members or the management have left behind.

vi. Financial Auditor

Every organization needs a financial auditor who provides you a fiscal figure after the electronic incident has taken place. The fiscal figure is important to evaluate for insurance purposes. According to National Information Infrastructure Protection Act an organization needs a financial auditor to figure out the amount of loss a company has suffered [5]. Besides,

the incidents financial auditors are also required to evaluate the number of resources that are the required by the employees.

vii. Attorney

All well-established organizations and companies hire attorney to look after their legal proceedings. Building a CSIRT would also acknowledge the need of attorney. In case of electronic incident, after investigation the organization wants to take a legal action against the culprit, the attorney will proceed with legal advises and will carry out the whole proceeding. Attorney also supplies advices considering accountability issues if the customers are facing any kind of issues related to their information in the event of incident.

viii. Public Relations

The bigger companies and organizations always offer a good amount of time to closely pay attention of their customers' needs and suggestions to make their products better. Public relations are meant to share the organizational gestures with their customers. These people are professional and holds experience in what to deliver and what not with the customers or public media. When an incident occurs, public relations personnel hold a press conference or meeting with the people to disclose the internal findings and investigation reports.

ix. Security Guards

Security guards are generally meant to protect the physical infrastructure of an organization. The main assets of organization include the building of an organization that have the physical assets too and other financial and organizational piece of works i.e. documents. Any physical incident can take the organization down if the building collapses or any kind of theft happens within the organization.

CSIRT VS Security Team

CSIRTs are distinct from security teams within an organization's IT department. The security team's responsibility is to monitor the organization's network and systems on a daily basis, ensuring that all systems and information assets are kept up-to-date with the installation of patches and fixes to minimize security incidents. On the other hand, CSIRTs may have similar duties, but their main focus is to respond to security incidents, perform incident analysis and mitigation, and coordinate incident responses throughout the organization. CSIRT is a single point of contact for solving the security incidents, assists the organizational constituency in handling and preventing computer security incidents [6].

CSIRT Framework

Many people believe in adaptation to already developed policies and guidelines for creating their own CSIRTs, but it has been understood soon that no services, policies and guidelines can be appropriate for two CSIRTs. Each organization runs in a different environment making it difficult to inherit someone's code of conduct. In addition, teams with inflexible protocols are finding it challenging to adjust to the constantly changing landscape of incident response in the contemporary realm of computer security.

Following are the components of CSIRT which acts as the building blocks of CSIRT framework that make up the CSIRT vision [7]:

i. Constituency

- The constituency of a CSIRT refers to the organization or group of organizations, as well as individuals, whose incidents the CSIRT manages or coordinates.

ii. Mission Statement

- What do you do?
- What is the purpose?

iii. Organizational Structure

- What responsibility levels should be defined within CSRIT? How the coordination should be built within organization? How do you operate?

iv. Services

- How do you achieve your mission?
- What services you provide to your constituencies?
- What type of incidents do you handle?
- What type of activities do you perform?

v. Policies and Procedures

- Formal approach to respond to security incidents and response strategies.

vi. Resources

- What types of resources do you need to perform your mission?

vii. Funding

- How do you pay for the organization structure and services?

The components of CSIRT influence each other therefor influence CSIRT design. This example could be easily explained as; the mission is influenced by constituency and needs. Resources will influence organization model such that the diversified structure or

members of teams would hinder the working of CSIRT because of non-availability of CSIRT resources [6].

CSIRT Structure

An incident response team should be readily available to anyone who discovers that a security incident has taken place within the organization. It is the responsibility of CSIRT to analyze the security incident and respond to it to mitigate the damage and propose safety measures and restore the normal state. Various types of incident response team models are present which should be availed by constituencies depending upon the nature of services [8]:

Following are the possible structures for incident response teams:

1. Central Incident Response Team
2. Distributed Incident Response Team
3. Coordinated Teams

Three different staffing levels can be opted for to set up a CSIRT [9]:

1. Employees
   – Handling all incident activities by itself without consulting external party.
2. Partially Outsourced
   – Outsourcing certain amount of its activities to external parties for reducing work load.
3. Fully outsourced
   – Outsourcing all elements of its incident response related activities to external parties.

Team Selection

Organizations should consider following factors while selecting an incident response team:

1. 24/7 availability
2. Part-time Need
3. Employee Morale
4. Cost
5. Staff expertise

Issues in Outsourcing

1. Quality Work of third party
2. Division of Responsibilities
3. Sensitive Information revealed to third party

4. Lack of organization-specific knowledge
5. Lack of correlation between outsourcer and organization
6. Handling incidents at multiple locations

Maintaining incident response skills in-house (during the absence of outsourcer, problems may arise). Following screenshot shows the organizational hierarchy and the collaboration between CSIRTs.

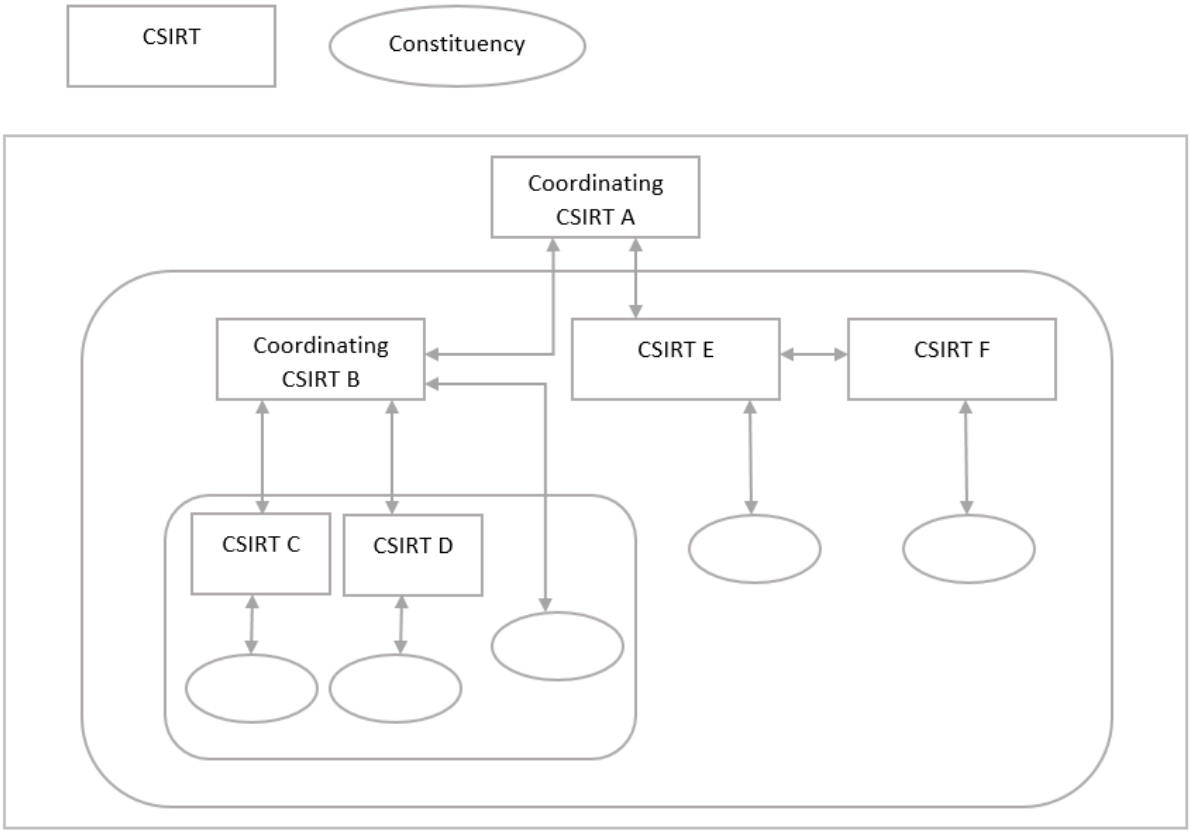


Figure 1. CSIRT Organizational Hierarchy

1.3 Categories of CSIRT

Following are the categories of CSIRT [6]:

1. Internal CSIRT

   - This is a particular CSIRT type which is focused on separate institution e.g. bank university, hospital, federal agency.

2. National CSIRT

   - Such type of CSIRT primarily focuses on every institution and provides information security services to overcome the problems.

3. Coordination Centers

- These centers are meant to provide coordination and facilitate the incident handling across various CSIRTs for a particular region or state.

4. Analysis Centers

   - These centers take data from various CSIRT centers, analyze the data and make an observation about trends and patterns in incident activities.

5. Vendor Centers

   - These centers particularly dedicate their services to an organization; provides consultant in case an organization finds vulnerabilities or report an incident. Maintaining incident response skills in-house (during the absence of outsourcer, problems may arise). Following screenshot shows the organizational hierarchy and the collaboration

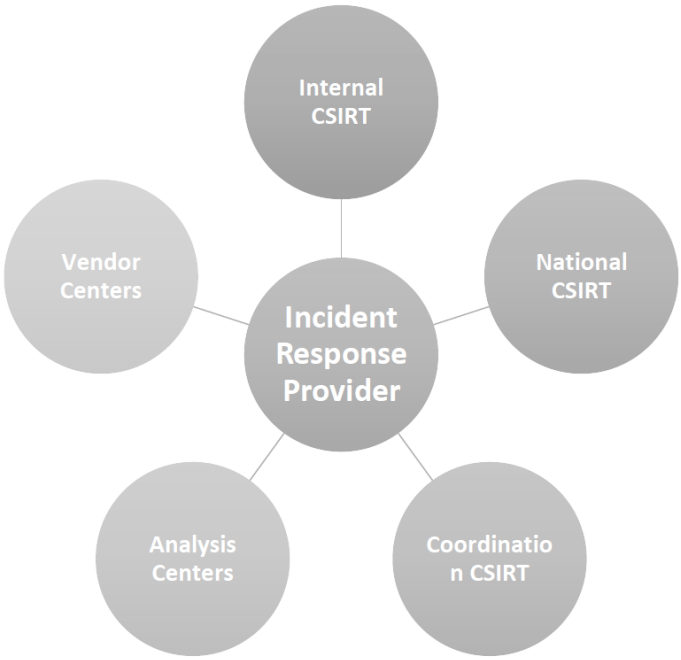


Figure 2. Categories of CSIRT

1.4 CSIRT Services

Following are the services [6]:

Reactive Services	Proactive Services	Security Quality Services
Alerts and warnings **Incident handling** •Incident analysis	**•Announcements** **•Technology watch** **•Security audit or assessments**	**•Risk Analysis** **•Business continuity and disaster**

•Incident response on site •Incident response support •Incident response coordination **Vulnerability handling** •Vulnerability analysis •Vulnerability response •Vulnerability response coordination **Artifact handling** •Artifact analysis •Artifact response •Artifact response coordination	**•Development of security tools** **•Intrusion detection tools** **•Security-related information dissemination** **•Configuration and maintenance of security tools, applications, and infrastructures**	**•recovery planning** **•Security consulting** **•Awareness building** **•Education/training** **•Product evaluation or certification**

Figure 3. CSIRT Services

Benefits of CSIRT

CSIRT team is a dedicated group to respond to cyber incidents to help organization in prevention and mitigation of potential incidents. Following are some of the benefits of CSIRT:

1. Incident Response
2. Threat Intelligence
3. Reduce cyber security risk in long run

Figure 4. Benefits of CSIRT

Apart from above listed benefits, CSIRT also provides a number of services that turn into benefits for their constituencies:

1. Centralized and exclusive response to cyber security incidents.
2. Helps organizational employees by providing expertise at any time to recover quickly from security incident.

3. Centralized coordination hub for discussing security incident matters within organization through the establishment of central contact point within CSIRT.
4. Provides centralized communication path with National CSIRT.
5. Retention of computer records in the event of a penal case against the organization
6. Coordination with other CSIRTS for obtaining real time cyber-attacks statistics to take measures to prevent cyber incidents.
7. Capacity building of organizational employees and raising awareness of security issues.

Technologies required for CSIRT

1. Security Information and Event Management (SIEM)
2. Vulnerability scanners and penetration testing tools
3. Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and wireless intrusion prevention
4. Firewalls and Next-Generation Firewalls (NGFW) which can function as an IPS
5. Log management systems (commonly as part of the SIEM)
6. Cyber threat intelligence feeds and databases
7. Governance, Risk and Compliance (GRC) systems
8. Security orchestration automation and response
9. Artificial Intelligence (emerging technology with profound results)

Areas not covered by CSIRT

The fundamental service of CSIRT is related to computer security incidents. Following are the types of incidents where a CSIRT doesn't provides its assistance:

- General IT incidents or problems.
- Physical security threats, such as bomb alerts, theft or suspicious activity.
- Human resource incidents, such as (cyber) bullying or disputes.
- Financial fraud.
- Criminal activities.
- Prevent strategy.
- IT service interruptions or downtime.
- GDPR breaches.

Phases of Incident Handling

The central body for handling security incidents in an organization is CSIRT. It can limit the damage from cyber incident by providing rapid response and suggesting recovery solutions to its constituency. CSIRT ensures that the work goes uninterrupted with minimum cost. Incident management includes:

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication
5. Recovery

Apart from listed responsibilities CSIRTs have the capability to understand the cyber incident by analyzing the attack patterns and keeping themselves aware by ensuring prevention in future from such cyber-attacks. CSIRTs analyze problems in detail and provide remediation/solution to other departments, works on capacity building and distribute alerts within organization on the latest risks and threats.

CSIRTs runs national cyber awareness system:

1. Offers current information on security events that have a significant impact on the wider community.
2. Current information on security issues, vulnerabilities, and exploits in a timely manner.
3. Weekly summaries of new vulnerabilities along with patch information.
4. Provide in-depth analysis on a new or evolving cyber threat.

Security Operation Center (SOC)

A SOC is an in-house IS team that facilitates on-going network activities and is responsible for monitoring and analyzing the organization security posture. The SOC team is a group of skilled people who make use of their knowledge with the tools and technology to detect, analyze and respond to security incidents. SOC focuses on described set of processes to tackle the security incidents in the early stages by taking effective measures to reduce the harm of any possible threat. A SOC is the central responsible body for protecting organizational assets from internal or external threats. The main responsibilities of SOC includes:

1. Monitoring, Detection, Analyze, Prevention, Reporting
2. Monitoring the security of users, systems, and applications
3. Creating and managing procedures
4. Integration of security products with other systems/tools

Apart from listed responsibilities, SOC is liable to monitor people, processes, and technologies by analyzing logs of various information assets to ex-filtrate data that is harmful to organization in any means. Some of the additional capabilities of SOC includes:

1. Malware Reversing
2. Digital Forensics
3. Cryptanalysis

Following are the components of SOC:

1. People
    - Formal Training
    - Internal Training
    - On-the-job experience
    - Vendor specific training
2. Process
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery
    - Lessons Learn
3. Technology
    - Monitoring (Incident Detection Management)

- Response (Protection/Forensics)

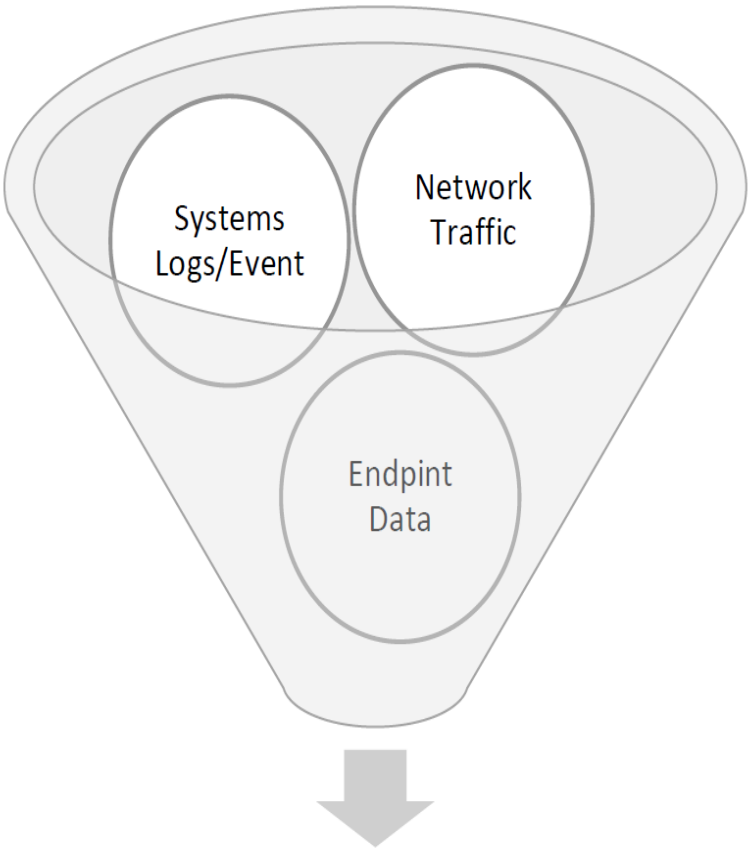


Figure 5. SOC Tiers

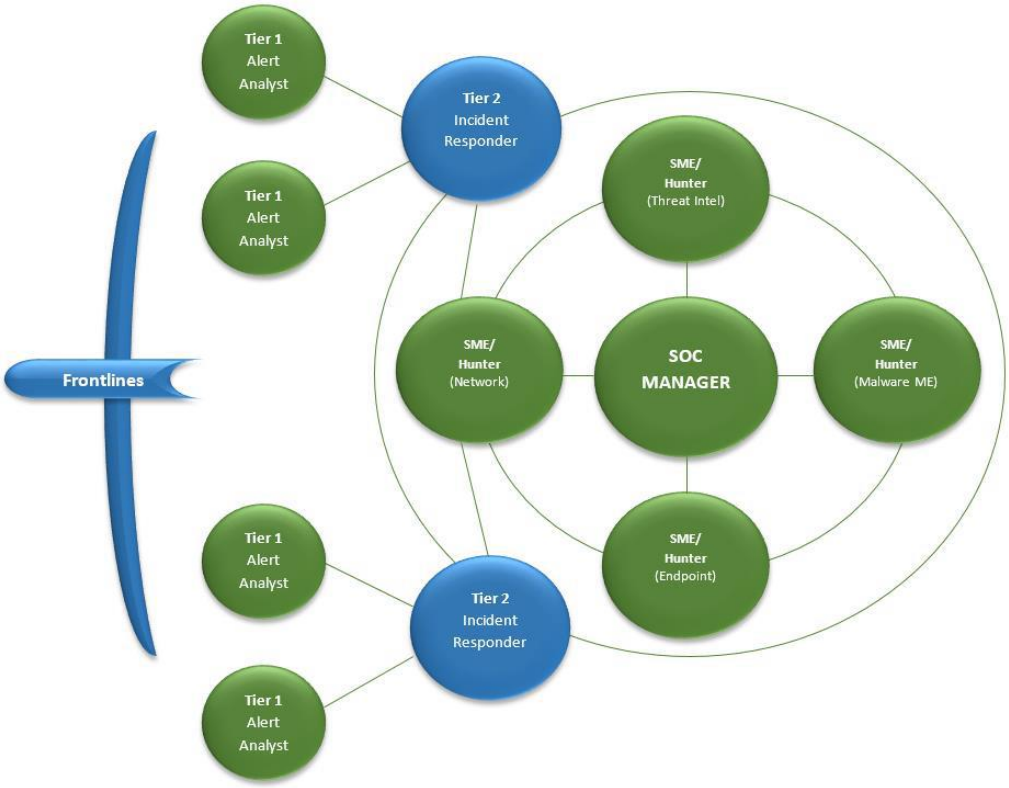


Figure 6. SOC Monitoring System

Comparison between SOC and CSIRT

Following table highlights the various differences between SOC and CSIRT:

Table 1: Comparison between SOC and CSIRT

SOC	CSIRT
SOC centralizes the roles responsible for protecting information security within the organization.	CSIRT is a centralized department within organization which specializes in incident management/handling.
SOC monitors people, process and technology involved in all aspects of cyber security.	CSIRT investigates security incident after it is detected. CSIRT analyse the incident by conducting forensics to rank alerts, coordinating and executing response strategies etc.
The goal of SOC is to oversee the appliances security, user security, governance, risk, compliance, policy, procedure creation and management, maintaining industry best	The main goal of CSIRT is to minimize the threat vector and control the consequence from the incident.

practices for information security.	
SOC is more concerned with incident detection.	CSIRT is more concerned with incident detection, analysis, response to security incidents and prevention.
SOC is a standalone body within organization, but in the absence of CSIRT, a SOC team can perform incident management.	The need of CSIRT is dependent on organization business needs and structure, however CSIRT may work under SOC.
SOC requires much more investment and budget to operate progressively as SOC comes first before CSIRT.	It is not mandatory to have a CSIRT for an organization. But if it is high-risk industry (e.g. finance, healthcare, government) than a formal and full time CSIRT is necessary.

1.5 High Level Policies of CSIRT

CSIRT approaches are vital to its activity. These are guidelines that the CSIRT staff must follow when carrying out tasks. They reflect the policies that the CSIRT upholds, oversee the operation and activities of the response center, and ensure the confidentiality, integrity, and availability of the CSIRT's data, assets, and other resources. Members of one CSIRT are responsible to ensure the quality of its services. Each CSIRT has polices which are central to its day to day operations.

The policies defined by CSIRT are serving as general guidelines for its employees and target community [34]. The guidelines are significant in explaining the specific nature of the services and how the CSIRT safeguards and preserves the confidential information that it handles.

FIRST (World's largest international forum of CSIRTs), has provided following necessary policies for a CSIRT that desires to become a member of the community.

Information Classification Policy

How CSIRT groups information and differentiates between sensitive, confidential, secret and public information.

Information Protection Policy

How to protect information according to its assigned.

Information Retention Policy

How long the CSIRT should keep records or other information in its possession.

Information Destruction Policy

How the CSIRT destroys information, records, media, devices, etc. to ensure that information is protected when its life cycle or the media containing it comes to an end.

Information Disclosure Policy

How and when the CSIRT may share or distribute information internally or externally.

Policy on Access to Information

Who can access CSIRT information, taking into account CSIRT staff, members of the target com-munity, or personnel from the CSIRT's parent organization (if it has one).

Appropriate Use of CSIRT Systems Policy

Acceptable use of CSIRT equipment and resources, specifically how, when and for what facilities and equipment can be used.

Definition of Security Incidents and Events Policy

Criteria that deter-mine the definition of a security event or incident and the classification of each by type and severity.

Incident Management Policy

How incident management occurs, including the type of incidents the CSIRT will answer, accept-able response times, and procedures to be applied, etc.

Cooperation Policy

What other entities the CSIRT will cooperate with and how it will do so, particularly other incident response teams.

Other Policies

In addition to the minimum policies required for a CSIRT, there may be others in order to improve the quality of services and the operation of the Center:

- Internet Use Policy
- Incident Reporting Policy
- CSIRT Communication Policy
- Personal Computer Security Policy
- Mobile Device Use Policy
- Telecommunications Equipment Security Policy
- Training and Education Policy
- Computer Network Security Policy
- Backup Policy
- Segregation of Roles Policy

- Change Management Policy
- Password Policy
- Email Use policy

1.6 Problem Statement

Following are the research questions to be investigated in this research:

1. What are the issues in establishing CSIRTs?
2. What are the issues in operating CSIRTs?
3. What are the challenges in establishing CSIRTs?
4. What are the challenges in operating CSIRTs?

1.7 Research Objectives

The broad objective was to study about the CSIRT. Following are the specific objectives:

1. How to establish CSIRT?
2. What is the need of CSIRT?
3. How to increase the effectiveness of CSIRT?
4. Understanding the CSIRTs, their structure, services, types, categories.
5. What are the limitations of CSIRT?
6. What are the issues and challenges of establishing CSIRT in developing countries?

1.8 Significance of Work and Potential Benefits

CSIRTs holds a huge importance in the cybersecurity era because of its potential benefits that an organization or a country can achieve. The history shows that a self-replicating malware which shut down 10% of Internet connected computers resulted in the establishment of CSIRT few decades ago. Today is a World of cybersecurity threats to everyone, CSIRTs play a vital role in facilitating industry-relationship confronting cyber-attacks. It is the need of society to acknowledge that each and every organization or institution is prone to some kind of cyber threat due to known or unknown vulnerabilities that are still present in their information systems but they are not aware of it or may be the weaknesses of particular systems they are using are not made public because of reputation and stakes of the big tech companies. Security industries are implementing new methodologies and systems to eliminate the threats and find the root cause and cybercriminals. The CSIRT is the actual

representation of combating cyber threats by providing the real time security and services that none of the other mechanism could provide to such a high extent.

The potential benefits are already experienced by the developed countries e.g. the European countries where the cyber ware (malicious actions by national or international states to attack and harm other countries infrastructure) is already running at its peak. In the era of cyber warfare, the European countries have successfully placed themselves in quite a safest zone where the probability of attack on them is slightly low as compared to the other countries where the cyber security is not taken into consideration. The European countries have brought together various CSIRTS that are operating in different regions to foster the collaborations and build strong relationships.

The focus on study of CSIRTs is highly needful in times where we don't have any sophisticated infrastructure to handle the cyber security threats and respond back to those threats in such a way that we get the information about the cyber-attack and the methodologies and techniques used by the perpetrators for harming our systems. Studying in depth about CSIRTs would be potentially benefit the under developed countries who are still behind in the long race to combat cyber threats. The benefits would ultimately result in analyzing the problems and challenges that constrain the organizations establishing CSIRTs for the very first time in region.

1.9 Novel Contributions

This research focuses on CSIRTs and the need that modern World requires. The growing security threats have increased the need and awareness in people about the need of cyber security. In this research document detailed information and primary knowledge is shared to facilitate the individuals or cooperate organizations in Pakistan to gain enough understanding about the issues and challenges that should be addressed prior to starting a CSIRT. Researchers of the developing countries also would be benefited with this research and would open up the door of ideas and methodologies while developing CSIRT in their countries. Limitations of one concept or idea encourages researchers to put their efforts best to evaluate and propose solutions. After reading this document, researchers would be welcomed to practice the concepts defined and revalidate while they establish CSIRT in their own places. The type of services is always under research and discussion to find ways and solutions to better assist one's constituencies.

1.10 Chapter Summary

This chapter highlights the necessity of information systems and communication technologies, which have become a crucial factor in the economic and social progress. The usage of Internet connected devices has grown in the past few decades shows that the security of network connected devices is becoming the main concern Worldwide. Seeing the need, many national and international communities have joined hands to overcome cyberattacks to make the Internet a safe place for all people across the globe. CSIRT was therefore introduced soon after a computer spreading malware was detected which compromised the security of thousands of computers across the globe. The much-needed information about CSIRT is discussed in great detail showing the various aspects and ultimate utilization of its services. CSIRT is the need of every company or country that understands the need of information security and optimizes the best practices to ensure the safety and availability at the right time. In many countries state departments are involved in sharing information security at the very low level just to spread awareness and need of information security. Countries are investing hundreds of millions to secure their cyber space by creating security teams to handle incidents and respond back to security incidents within the appropriate time.

Chapter 2

LITERATURE REVIEW

This chapter contains literature review about the establishment of CSIRTs, the effectiveness and the issues and challenges while establishing CSIRTs.

2.1 Major CSIRTs Operational in Pakistan

1. **National Response Centre for Cyber Crimes (NR3C) -** NR3C is a department of the Federal Investigation Agency (FIA) of Pakistan that is responsible for handling cybercrime-related cases in the country. It also functions as a CSIRT for the Pakistan government.
2. **Pakistan Computer Emergency Response Team (PakCERT)** - PakCERT is a non-profit organization that provides incident response services, cybersecurity awareness training, and vulnerability assessments to businesses and organizations in Pakistan.
3. **Information Security Department (ISD)** - ISD is the CSIRT of the Pakistan Telecommunication Authority (PTA). It is responsible for protecting the telecommunications infrastructure of Pakistan from cyber threats.
4. **National Telecom and Information Technology Security Board (NTISB)** - NTISB is a government agency that works to secure the country's telecom and IT infrastructure. It also functions as a CSIRT and provides incident response services to organizations in Pakistan.
5. **Higher Education Commission Cyber Security & Response Centre (HEC CSRC) -** HEC CSRC is a CSIRT that is responsible for protecting the IT infrastructure of higher education institutions in Pakistan.

2.2 Academic CSIRTs in Pakistan

Many universities level CSIRTs are responsible for ensuring the security of university's computer networks and systems. The CSIRT also provides incident response services to other universities and research institutions in Pakistan.

1. NUST CSIRT
2. LUMS CSIRT
3. IIUI) CSIRT
4. QAU CSIRT

5. COMSATS University Islamabad (CUI) CSIRT

2.3 Khyber Pakhtunkhwa CERC

The Cyber Emergency Response Center (CERC) of Khyber Pakhtunkhwa (KP) is a government organization in Pakistan responsible for dealing with cyber threats and incidents in KP province. The center was established in 2014 under the Khyber Pakhtunkhwa Information Technology Board (KPITB). The main purpose of KP CERC is to provide a central point for receiving and responding to cyber incidents, such as cyber-attacks, hacking, and other forms of cybercrime. It also works to create awareness about cybersecurity among individuals, businesses, and government organizations in the province.

KP CERC has a team of cybersecurity experts who are responsible for investigating and responding to cyber incidents. The team works around the clock to ensure that incidents are dealt with quickly and efficiently. It also provides support and guidance to businesses and individuals on how to secure their computer networks and systems. The center has established partnerships with various organizations, including the National Response Center for Cyber Crimes (NR3C) and Pakistan Computer Emergency Response Team (PakCERT), to share information and resources and coordinate responses to cyber incidents.

KP CERC also offers training and awareness programs to individuals and organizations to help them understand the importance of cybersecurity and how to protect themselves from cyber threats. The Khyber Pakhtunkhwa Cyber Emergency Response Centre (KP-CERC) is a unique cybersecurity program that provides students with training and certification opportunities in the field of cyber security. The idea is to prepare a force which can defend the cyber frontiers of the country. Moreover, capacity building of IT staff is critical in safeguarding the government digital assets and citizen's data. Following services are currently offered by KP CERC:

- Penetration testing services for Government Departments
- Issue Advisories and Alerts
- Capacity Building Trainings around the issued Advisories and Alerts
- Awareness Trainings
- Developing SOP’s for Information Systems

2.4 Establishment of CSIRT

With the advancement in information technology the World has become a global village where everyone is connected to each other by some sort of medium showcasing the need of modern technologies. The information and communication technologies have revolutionized

the World by providing the ease to individuals and organizations to practice their routine manuals in an automated and better approach. In modern era, regardless of the business scale and diversity, everyone has joined the online World of Internet and started their living virtual lives for carrying out their daily routine work. These technologies have enabled people to access any information over the Internet and store their information there for sharing with other people. Although, this the opportunity has brought people nearer and have made their live easy in the accomplishments of their work but apart from the opportunities provided by the modern technologies, they have also made their information and lives vulnerable to the cyber threats. The cyber-criminals conduct intended malicious endeavors to harm their targets by causing damage to their business, by stealing their intellectuals or identities. These problems have emerged from the very start when the era of Internet was started and the technology was becoming more advanced. The security incidents are growing rapidly, without any contribution in handling them would end into data leakage, theft, fraud etc.

Hacking, denial of service attacks and malware outbreaks etc. are the most common examples of information security incidents. The information security incident is defined as:

"A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" [13]

With the increase in Internet security incidents, Internet community have recognized the need of information security mechanism to deal with the computer security incidents. It has been observed that handling incidents is not as easy as it seems to be. A group of experts should be needed at all times who specialize in their domains to have better approach in handling the incidents. Therefore, to establish an incident response capability, we need to establish incident response team [14].

A CSIRT is defined as:

"An organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents" [15]

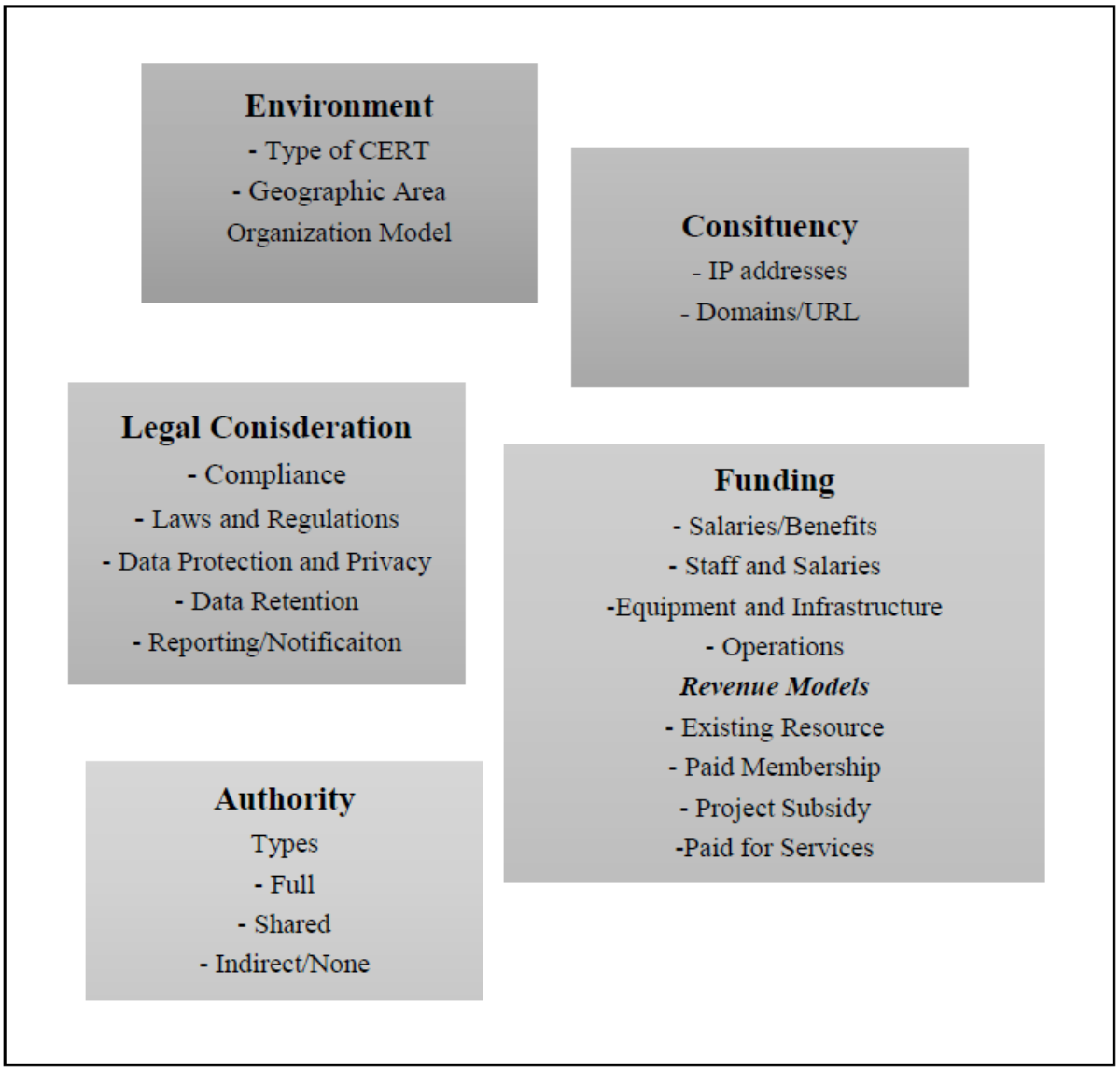
The team can be organized and should be called together on emergency basis when a cyber security incident occurs [16]. For better outcomes and support, incident response teams can organize incident response activates with other groups [14]; the sharing of information

always yields better results. CSIRT can also coordinate and facility academic institutions by conducting cyber security awareness campaigns and trainings [17]. [2] Provides a number of problems and challenges that the author has experienced in his life while establishing a national CSIRT in a developing country. According to the challenges described it has been observed that mandate which is also referred as mission of the CSIRT was unclear at the time of establishing the CSIRT. Lack of management support, choosing a revenue model, finding investment sources and interacting with the constituency (also other parties) are the main challenges. According to a service carried out it has been discovered that lack of management, lack of funding, unclear mission and authority were confirmed challenges [16].

To start establishing a CSIRT, the issues and challenges should be kept in mind. Although, enough guidelines and methodologies have been provided by the domain experts but one should understand where to start. A process and method should be followed while the establishment of CSIRT to handle the problems. Literature describes that successful provision of CSIRT services requires a holistic approach [18]. Following business requirements that aids in the establishment of CSIRT are described below which generally limits the establishment of CSIRT:

- Environment - This is the geographic region where CSIRT will serve and provides its services and operations. CSIRT could provide its services to military, academic institutions, government institutions, private organizations etc. CSIRT can operate in multiple teams where each team can serve more than one region [17].
- Constituency – "the group of users, sites, networks or organizations served by the team" [19].
- Authority – The nature of constituency decides the type of authority which the CSIRT members possess [20]. Authority is the business requirement which affects the services provided by the CSIRT e.g. incident tracing and incident detection activities could not be performed without the level of authority [20].
- Funding – This is one of the major requirement and challenge that most of the CSIRTs faces while in the establishment phase. Before providing services, an agreement should be signed by the two parties for whether the constituency would be willing to pay for services.
- Legal Consideration – Attorney
- Building CSIRT would also acknowledge the need of attorney. In case of electronic incident, after investigation the organization wants to take a legal

action against the culprit, the attorney will proceed with legal advises and will carry out the whole proceeding. Attorney also supplies advices considering accountability issues if the customers are facing any kind of issues related to



their information in the event of incident.

2.5 Relationships between CSIRTS

Depending upon the necessities, objectives and services CSIRTs are established with different shapes and sizes. Distinctive teams may be formed such business, military, organizational and academic, that have different needs and expectations of the constituency depends upon the type of services they are performing to clients. The inter-relations with other CSIRTs are deeply followed to achieve the better status and security. There are many CSIRTs operating in the World that are sharing information and modern methodologies and

process with each other. Efforts towards participation and coordination are the core of the CSIRT framework [21]. The coordination holds an importance while operating CSIRT. It is necessary to explain the services that the CSIRT would provide to its constituencies. It has been studied that with the evolution of needs and change in events the structure of CSIRT changes. The behavior and structure of a CSIRT are strictly dependent over each other. As the system (CSIRT) progresses with the passage of time the behavior of systems might change the dominant structure [22].

Organization should explain its structure likewise its services as this structure would describe the type of relationships that the organization establishes similar to the CSIRTS. Organizational structure is defined as "the network of relationships and roles existing throughout the organization" [23]. An organizational model refers to a hierarchical structure that establishes a framework for the system, including channels of authority, communication, responsibilities, and allocation of resources [21]. The organizational framework is also evaluated based on the objectives of the organization and serves as the link in which the work and processes are conducted. Through this way the number of employees in an organization can be noticed for delivering their services.

The organizational challenges are the main focus of the higher management. These challenges are the actual limitation that hinders the success and continuous flow of CSIRTs. These includes insufficient technical skills, mutual trust, lack of defined and agreed procedures for information sharing between different CSIRTS etc. [24].

2.6 Effectiveness of CSIRT

The effectiveness of CSIRT heavily depends on the factors that includes management and constituency. Although, many people believe that the effectiveness of CSIRT depends on the technological aspects e.g. cyber analysts, researchers, technical skills etc. [25]. CSIRT should develop a mechanism which should assess the practices that are followed during the operations of CSIRT. To establish efficient teamwork in EMS teams, the team members need to work together effectively in handling coordination, communicating risks, providing initial patient care, transferring patients, and documenting treatment [26]. One of the critical factor that uplifts the effectiveness of CSIRT is the ability of team members to function in a team [25]. The measure of effectiveness also focuses on the information security controls and the limitations which hinders their workflow. Several characteristics are the key factors that define CSIRT operations and environment [25]. Measures of effectiveness and efficiency

address two aspects of the outcomes of security control implementation: the strength of the outcome itself (effectiveness) and the promptness of the outcome (efficiency). CSIRT should be adaptive to changing environment and CSIRT should have the flexibility to meet unexpected incidents [27]. The measurements help the information security personnel to dive deep into the security controls implementation and re-define the information security policy that would help them to focus on the areas where much care is needed in order to fill the loop holes which could be targeted by the cyber criminals or hackers to ex-filtrate important information about the concerned organization.

Clearly defined metrics are crucial to determine which security practices are worth investing in. The CSIRT should establish a mechanism to assess the efficacy of its security practices and procedures, in collaboration with management and the constituency. The outcome of this evaluation can also lead to the enhancement of the processes of a CSIRT [27].

Following are the four basic elements which are responsible for the effectiveness of CSIRT: [7]

- Operational framework
  - Clear mission
  - Defined constituency
  - Organizational structure
  - Relationships with other organizations/CSIRTs
- Service and policy framework
  - Defined services
  - Defined Information Flow
  - Clear, comprehensive organization's policies
  - Defined process for collecting, recording, tracking and archiving information
- Effective quality assurance framework
  - Definition of quality systems
  - Specific measurements and checks of quality parameters
  - Reporting, auditing practices and procedures
  - Constituency and customer feedback
  - Balance, compliance and escalation procedures to ensure quality level
- Adaptability and Flexibility

- Ability to keep up with changing technologies
- Ability to adapt to real threats and future emerging threats
- Legal expertise and support

Following are some other factors which could increase the performance of CSIRT: [27]

- Communication Skills
- Collective Problem Solving
- Trust among group members
- Shared knowledge of expertise

Figure 8. Effectiveness of CSIRT

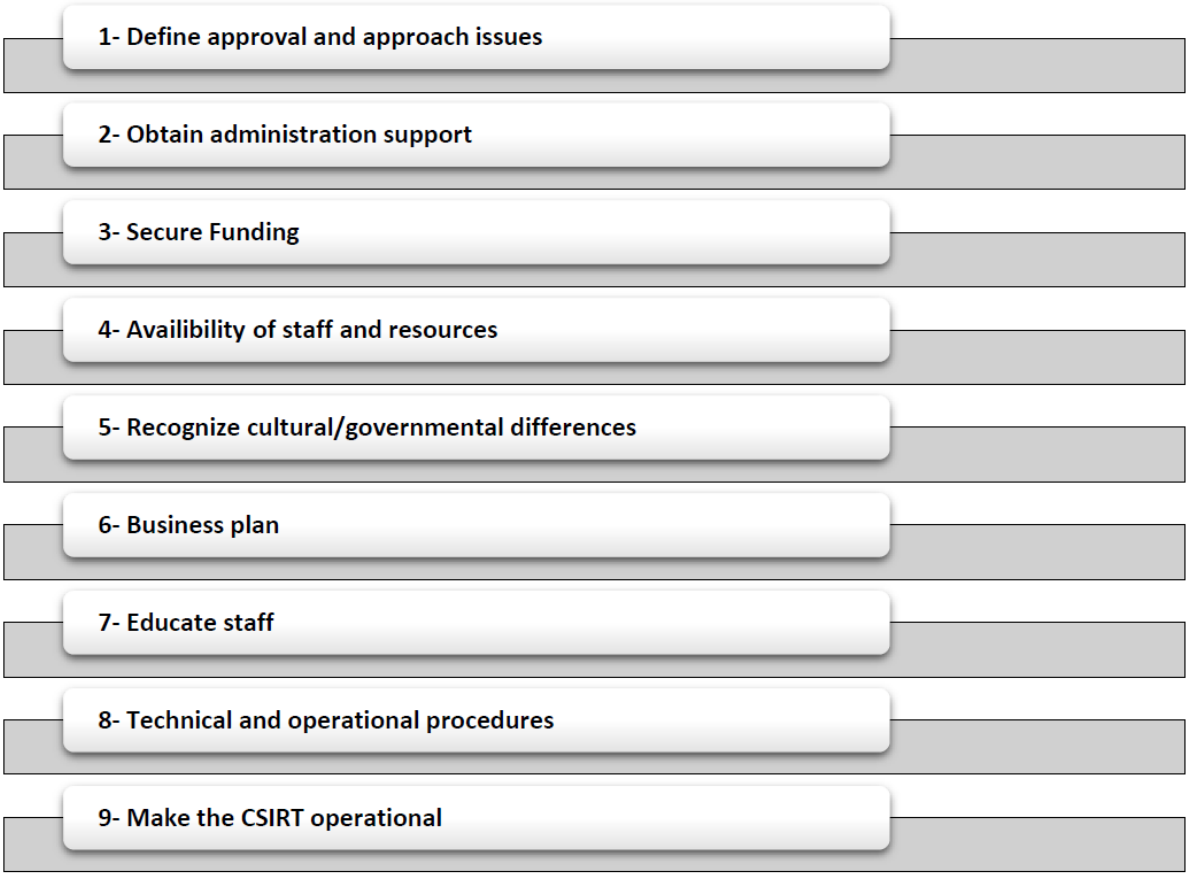
The effectiveness of CSIRT is dependent on the team work. If the team performs well in delivering their services, the better the CSIRT will progress. Trust among various domain members and the level of information sharing effects the progress of CSIRT. Team members should have the technical skills that are required to solve the problems. Adaptation to new technologies affects the performance and effectiveness of CSIRT.

The progress of a CSIRT can be evaluated by reviewing the design and implementation plans, assessing its capabilities and services, and gathering feedback from its constituency, both internally and externally. After identifying what works and what doesn't, the CSIRT team can develop improvement plans more effectively. The establishment of robust policies can help sustain and enhance the effectiveness of a CSIRT. Improvement in effectiveness of CSIRT can be fostered through the following guidelines: [27]

- Find ways to facilitate operational coordination among CSIRTs.
- Enhance cooperation between CSIRTs to promote information exchange, thereby maximizing the information available to CSIRTs.
- Share threat indicators with third-party organizations to encourage collaboration.
- Consider implementing regulations and/or legislation that compel organizations to act on CSIRT warnings and/or increase their liability to make them more accountable for taking warnings seriously.
- Explore measures to encourage cross-border information exchange, such as confidentiality agreements or methods to limit the liability of CSIRT incident response activities.

2.7 CSIRT Development Steps

Following figure shows the steps required for developing a CSIRT which are adapted by



CERT/CC [2].

Figure 9. Steps required for CSIRT Establishment

This article can serve as a guide for developing countries that are establishing a national/coordinating CSIRT or for those who are advising another country on the

establishment of their CSIRTs. Overcoming the problems and challenges in each step would help the organizations to establish an effective CSIRT. Every organization have some strengths and weaknesses, if the weaknesses turns into strength of the organization eventually the problems will be solved.

Table 2: CSIRT challenges during establishment

Ser	Proposed Steps	Identified Challenges
1	Define approval and approach issues	▪ incompetent competition ▪ delays in project implementation ▪ project termination ▪ un-clarity in mandate
2	Obtain administration support	▪ bad publicity ▪ emphasis on need
3	Secure Funding	▪ man, hours and budget should not be exceeded
4	Availability of staff and resources	▪ a CSIRT's technical needs may be against the host organization's ICT policy ▪ new recruits need specialized training ▪ a lot of equipment is needed
5	Recognize cultural/governmental differences	▪ lost stakeholder trust ▪ slow decision-making ▪ bureaucracy ▪ lack of openness ▪ political differences ▪ unnecessary delays ▪ costs and logistics of travelling ▪ maintaining foreign relations
6	Business plan	▪ trained and available ▪ selection of a revenue model ▪ selection of CSIRT services

		▪ determination of service hours ▪ number of staff members that are
7	Educate staff	▪ train technical staff ▪ risk of key personnel resigning
8	Technical and operational procedures	▪ incorrect understanding of processes ▪ procedures are not tested on real-life incidents
9	Make the CSIRT operational	▪ CSIRT is not fully announced ▪ constituency do not know how to interact with CSIRT

As discussed above, the identified challenges in each step causes problems in the establishment of CSIRTs. Solving these challenges would obviously be effective in the long run for the organization and continuity of the organizational business

2.8 Pakistan's Cyber Crime Law

Cyber law is any law that applies to Internet and its technologies, it is the part of any legal system that deals with Internet, cyber-space and their respective legal issues. Cyber law provides legal protections to people using the internet.

The promulgation of the following cybercrime laws in Pakistan was a response to the challenging situation created by the increased use of the internet, especially in relation to electronic commerce [35], [36].

1. Electronic Transaction Ordinance 2002 (ETO 2002)
2. Prevention of Electronic Crimes Ordinance 2007 (PECO 2007)

Both referenced laws were first IT applicable legislation made by national officials. Without going into the details of the enactments, it is crucial to note that this law was not enacted with the intention of punishing cybercrime-related offenses. Therefore, the limitations of this law are quite evident. As new ways of committing crimes emerged with the increased use of computers, none of them were included in this ordinance, which made it less effective. Consequently, most perpetrators evade the law, and judges cannot levy charges against them.

After observing the deficiencies in the Electronic Transaction Ordinance 2002 regarding cybercrime, a comprehensive law was introduced as the Prevention of Electronic

Crimes Ordinance 2007 (PECO 2007). The purpose of this ordinance was to address issues related to the misuse of technology. PECO 2007 provides some provisions for electronic crimes and devices to control the threat through effective legislation, but unfortunately, it did not attain the status of an Act and was revoked in 2009. Since then, cybercrime offenses have been dealt with under the ETO 2002.

The National Response Centre for Cyber Crime (NR3C) - FIA is a law enforcement agency that was established in 2007 after the introduction of PECO 2007. NR3C has expertise in digital forensics, technical investigation, information system security audits, penetration testing, and training. The unit has been involved in collaboration with officials from the police, intelligence, judiciary, prosecutors, and other government agencies. NR3C has also conducted numerous courses, workshops, and training/awareness programs for academia, print/electronic media, and lawyers. The latest initiative of NR3C is Digital Scouts, in which selected students from various private and public schools are trained to handle computer emergencies and raise awareness among their fellow students, teachers, and parents.

After 6 years, fortunately, cybercrime laws came under limelight again in 2014 due to vast coverage of cybercrimes. Prevention of Electronic Crimes Bill 2014 was introduced by IT Minister in National Assembly which was approved after few days which was sent for President Approval. On August 11, 2016, Pakistan's lower house, the National Assembly, passed a disputable cybercrime law called the Prevention of Electronic Crimes Act, 2016.

One of the major reasons behind the increase number of cyber violations is the absence of cybercrime law. Although, Prevention of Electronic Crimes Act 2016 was passed, still the federal government has failed to implement it. The law is being abused as substance like pornography, disrespectful posts, and sectarian hate speech is accessible via web-based networking media. The Federal Investigation Agency (FIA) is the skillful power and bound to capture the violators; be that as it may, due to non-execution of the law, the violators are still at large.

Here are some key provisions of the law:

- **Cyber Terrorism** - Any act committed through an electronic system with the intention of causing religious, ethnic, or sectarian hatred, or damaging the integrity of the country, will be considered cyber terrorism.
- **Unauthorized access** - Gaining unauthorized access to any electronic system, network, or database is considered a crime under the law.

- **Cyber Stalking** - Harassment and stalking through electronic means, including phone calls, messages, and social media, is a punishable offense under the law.
- **Identity theft** - Theft or misuse of another person's electronic identity, including email and social media accounts, is considered a crime under the law.
- **Electronic fraud** - Any form of electronic fraud, such as phishing, is considered a crime under the law.
- **Electronic forgery** - Creating, using or possessing any electronic device, software, or system for the purpose of committing electronic fraud or forgery is considered a crime under the law.
- **Penalty** - The law imposes fines and imprisonment for different offenses, with maximum penalties of up to 14 years of imprisonment and fines up to PKR 50 million.

The Prevention of Electronic Crimes Act 2016 also establishes a designated investigation agency, the Federal Investigation Agency (FIA), to investigate and prosecute cases related to cybercrime. The FIA can also block websites and take down illegal online content under the law.

2.9 International Incident Response Teams

According to FIRST (global forum of incident response and security teams) there are 483 teams in 92 countries [28]. All the security teams are concerned for providing various security related services to their registered constituencies. Most of the countries have multiple CSIRTs which are covering technical domain. Following table highlights security teams of various countries and the services they are offering:

Table 3: International Incident Response Teams

Name of Country	Team Name	Services
USA	USERT	Computer security incident handling, threat assessment, awareness and reactive and proactive services
Bangladesh	BRG e-Gov CSIRT	Cyber security incident handling, Digital Forensic Lab, Security consulting

India	CERT-In	Penetration testing, vulnerability assessment, threat modelling
Bhutan	BtCIRT	computer security incident handling, awareness and reactive services
Srilanka	Sri Lanka CERT/CC	Incident response, malware analysis, digital forensics, security assessment, threat alert
UAE	AeCERT, ADGovCERT	Incident handling, malware analysis, security awareness, threat modelling, digital forensics
Malaysia	MyCERT	Incident response, malware analysis, digital forensics, security assessment, threat alert
Indonesia	ID-SIRTII/CC	incidents handling, internet security awareness, handling network incidents
China	CNCERT/CC	Incident response, malware analysis, digital forensics, security assessment, threat alert
Egypt	EG-CERT	Threat assessment, penetration testing, malware analysis, digital forensics
Japan	JPCERT/CC	Security assessments, training services, forensics, security consulting
Mexico	CERT-MX	Incident Detection and Response
Qatar	Q-CERT	Incident response, malware analysis, digital forensics, security assessment, threat alert
Korea	KN-CERT	Incident response, malware analysis, digital forensics, security assessment, threat alert
Singapore	SG-GITSIR	Threat assessment, penetration testing, malware analysis
Thailand	ThaiCERT, TB-CERT	Penetration testing, incident handling, security audit
Turkey	TR-CERT	Network protection, Penetration testing, Cyber security consultancy, Forensics, Information Audit
Canada	CCIRC	Penetration testing, incident handling, security audit
UK	NCSC(UK),	Network protection, Penetration testing, Cyber

	Bunker	security consultancy
Israel	CERTGOVIL	Digital forensics, malware analysis, penetration testing
New Zealand	CERT NZ	Training services, Forensics, Information Audit
Russia	CERT-GIB, BI.ZONE-CERT	Penetration testing, Malware Analysis, Incident management
German	CERTBw,S-CERT	Network protection , Penetration testing, Cyber security consultancy, Forensics, Information Audit
Nigeria	ngCERT	Incident Detection and Response
France	CERT-FR	Incident Detection and Response
Brazil	CERT.br	Data leakage discovery threat intelligence digital fraud discovery
Australia	AusCERT	Vulnerability assessment, threat modelling, penetration testing, malware analysis
Spain	CCN-CERT, BCSC	Incident handling. Vulnerability handling. Training for professionals
Switzerland	GovCERT.ch	technical analyses, handling computer security incidents
Argentina	ICIC-CERT, BA-CSIRT	incident Detection and Response, penetration testing
Pakistan	KP CERC	Trainings, Awareness sessions, penetration testing, threat modelling

2.10 Limitations of Work Done

It's been more than two decades since CSIRTs have been established to help the victims to overcome their security weaknesses which are usually exploited by the malicious insiders. Although the effectiveness have not yet experienced to the level of satisfaction. Most of the CSIRTs are stilling providing reactive services which means that CSIRTs will provide their services when the attack take place. This is the limitation of CSIRT which should be handled with great devotion to take control of the ongoing cyber-attacks [22].The domain experts have growing understanding that the need of proactive services is very high [16]. Following limitations are derived from literature review in the context of CSIRT.

In [22], the author discussed that enhancement to the response process takes times to build whereas at the same time the incident response team has continuous pressure to prioritize the incidents and developing tools to enhance the handling of incidents. The author also discussed that capability trap is the major limitation to process improvement where the CSIRT personnel can't prioritize the magnitude of incidents in the time of intense pressure. However, author didn't mention the challenges that CSIRT may face during establishment phases.

In [29], the author discussed that trust between various CSIRTS is a major growing problem for which a survey among CSIRTS could produce better results that influence the effectiveness of cooperation between different operating CSIRTS and individuals of various CSIRTS lack knowledge and methodologies to share the findings and make a suitable relationship environment within and outside of the CSIRT. However, author didn't mention the issues that CSIRT may encounter during establishment and operations.

In [20], the author discussed five business requirements that includes CSIRT environment, funding, authority, constituency and legal considerations that should be satisfied before the establishment of CSIRT and also after the meeting the criteria for establishment the next phase would be to focus on determining the CSIRT services and staffing the initial team for operations. However, author didn't highlight how to operate a CSIRT.

In [2], the author discussed several problems and challenges while establishing a CSIRT which includes unclear mandate, funding, unclear business plan and CSIRT mission, etc. However, the limitations come into way when the problems and challenges described are not limited to each project, organization and country. The author didn't mention how each entity can face its own set of unique problems and challenges.

In [18], the author discussed that during the formation of CSIRT, limitation exists in the presence of inadequate plans, policies and procedures. Skilled people with background knowledge, communication skills, trusted staff and ability to solve problems is the only way to establish a successful CSIRT. However, author didn't describe the generic problems during formation of CSIRT.

In [30], the author discussed the positive effect of the management strategy that did not focus on attracting a higher number of frequent reporters, but retaining the most frequent reporters by reducing the turnover rate. The limitation however existed about the trend that is currently forming up by relying on external reporting more and its effect on the image and outlook of CSIRT instead of just dealing with the problem of funds.

In [25], the author discussed that no two organizations are alike that determines the likeliness of CSIRT for these two organizations. These differences could be due to CSIRT size, type, cultural differences and the type of attacks CSIRT's face on usual basis. However, research should be carried out about the factors that might change the development and implementation of strategies that impact the CSIRT effectiveness. The author didn't mention which factors should be taken into consideration while establishing a CSIRT for any organization.

In [31], the authors have had highly emphasized to develop a framework that enables responders to establish trust and achieve an effective collaboration response. A prototype implementation of workspace environment called the Palantir system provides collaboration access to tools and resources during investigation. Further research should be done in this area; a role-hierarchies, segregation of duties, well defined workflows, usability aspects of the workspace environment by improving interface enhancements for user interactions and evaluation of system in handling cyber incidents will used for validations and enhancements. However, author didn't highlight the methodology and procedures that should be followed during the CSIRT establishment and the framework working in CSIRT operations.

In [32], the author discussed few limitations that influence the effectiveness and working of CSIRT, in the view of some policy makers; cooperation with government and other law and enforcement agencies have been essential to facilitate the exchange of information and knowledge needed to reduce the attacks and provide effective responses to cyber incidents. Few other experts have pointed out that the culture and understanding of practitioner's impact the overall performance of CSIRT. However, author didn't explain how to setup CSIRT and what should be the roles and responsibilities.

In [33], the author has proposed an integrated framework to work collectively with various organizational units e.g. security teams, internal CSIRTS, Coordinating CSRIT etc. in order to fully address the needs of constituencies and deliver instant incident responses it is important to focus on the investigative aspects and communication with the stakeholders. However, the author didn't mention that in the absence of support and instant communication with the stakeholders can limit the prevention of reoccurrence of cyber incidents

2.11 Summary of Limitations

Table 4: Summary of Limitations

Reference	Year	Title	Limitations

[22]	2005	Limits to Effectiveness in CSIRTs	Theory of "Capability Trap" was discussed to understand why a CSIRT can experience problems improving to stay effective. A particular CSIRT was chosen for this study, due to which information gathered was limited.
[29]	2015	National CSIRTs and Their Role in Computer Security Incident Response	The scope of research study was limited to CSIRT's effectiveness, cooperation and factors that undermine trust in CSIRTs.
[20]	2015	Prerequisites for building a Computer Security Incident Response capability	The research study focused on evaluating CSIRTs business requirements, services. While study didn't reveal how to operate a CSIRT.
[2]	2010	Common challenges faced during the establishment of a CSIRT	The limitations described in this research study were mapped on ideal CSIRT. Problems and challenges described are not limited to each project, organization and country. The author didn't mention how each entity can face its own set of unique problems and challenges.
[18]	1994	Forming an Incident Response Team	The research document described the formation process of incident response team, the key roles, and responsibilities. Problems during the CSIRT development were not discussed.
[30]	2009	Preserving a balanced CSIRT constituency	The limitations existed in the trend that is currently forming up by relying on external reporting more and its effect on the image and outlook of CSIRT instead of just dealing with the problem of funds.
[25]	2015	Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based	The research study highlighted the factors needed that should be taken into consideration while establishing a CSIRT for any organization.

		Research	
[31]	2009	Palantir: A Framework for Collaborative Incident Response and Investigation	The research study discussed methodology and procedures that should be followed during the CSIRT establishment and the CSIRT operational framework. The framework was not able to share the issues, challenges during CSIRT establishment and their mitigations.
[32]	2015	CSIRT Basics for Policy-Makers	The research study was limited to CSIRT setup and what should be the roles and responsibilities of each individual.
[33]	2005	A Proposed Integrated Framework for Coordinating CSIRT	In the absence of support and instant communication with the stakeholders can limit the prevention of reoccurrence of cyber incidents. The research 43 study was limited to coordination among various CSIRTs.

2.12 Chapter Summary

This chapter describes the literature to dig deep into the work done by the researchers in the area of CSIRTs. The establishment of CSIRT is discussed in great detail to ensure that every possible information is highlighted. Various services provided by CSIRT shows the importance of its existence and the business requirements and components are also explained to ensure that an effective CSIRT could be established. There are various kinds of CSIRTs operating under FIRST which is the global leader providing best practices, solutions and methodologies to work effectively against incidents. The effectiveness of CSIRTs depends upon the type of services that are shared to its constituencies. While incident response teams capabilities and skills are highly required to run a successful and effective CSIRT. This chapter describes the limitations of CSIRTs in different phases and emphasizes to overcome the limitations by providing effective solutions and services to constituencies.

Chapter 3

Proposed Methodology

After detailed study about CSIRTs and literature review author of this research has found the necessary and unavoidable need of CSIRT within a private or a government institution for which he has used systematic literature review by the help of which he has evaluated the research done in the field of CSIRT and presented a fair evaluation of his research by means of a reliable and auditable methodology.

The summary of this study includes the evolution, need, understanding and the problems while establishing a CSIRT. Literature review shows the business requirements which turns to be the challenges while establishing CSIRT, whereas the effectiveness of CSIRT has also challenges to be encountered for improving the performance.

Various problems were discovered in each step of the establishment of CSIRT as described in detail in chapter 2, section 2.1.6, while these problems have been identified in the literature review too. This research document describes CSIRT from the very basic level to a maturity level by the help of which a non-technical person can understand the means, need and importance of CSIRT.

In this study, a solution has been proposed for the issues and challenges that might be faced during CSIRT establishment. Apart from the study, issues and challenges that frequently emerge in the development phase, author has also developed a strategy to ask the customers or people of various domains who are working or dealing in IT field to discover what type of issues and challenges they face in usual job routines related to cyber security. A quick and detailed survey in Pakistan will provide a huge amount of information which could be very essential for developing strategies and plans to tackle cyber threats. The audience for the survey may include: government, financial, healthcare, academic and telecom institutions. The business requirements which causes issues during the establishment of CSIRT will be dealt with effective policies, plans created by the domain specialists and the proposed procedures will eventually reduce limit of issues and challenges during the CSIRT establishment.

As defined above, the CSIRT heavily depends on the structure of the teams working in it. The relationships and trust factor increases the effectiveness of CSIRT, the shared information and problem-solving capabilities ensures the growth and progress in long run.

While the development of various teams also depends upon the technical knowledge and information factor, multiple group of teams can share their knowledge to remain up-to-date-about the current cyber security advancements.

3.1 Incident Management

Incident management involves incident handling and incident response. It includes the process of receiving, prioritizing and responding back to incidents and reports. According to NIST, following four (4) processes are included in incident handling:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident

The set of actions followed after a computer or network security incident is called incident handling. NIST's computer security incident handling guide states that only events with negative consequences are classified as security incidents. Such events can be:

- Unauthorized access to sensitive data
- Unauthorized use of system privileges
- System crash
- Packet floods
- Execution of destructive malware

Whenever dealing with incident handling, it should be kept in mind that incident handling is not about only intrusions. Malicious intruders in network, loss of sensitive data, unauthorized access to sensitive data, and loss of intellectual property all fall under the scope of incident handling.

As an incident handler, one’s job responsibility includes thinking from attacker’s perspective of damaging the company assets. Incident handler daily activities include discussing with other team members how an attacker managed to break into the system or network by finding all the loop holes. Incident handler should be aware of attacker’s techniques, tactics, and procedures and of course how an attacker operates during all stages of cyber kill chain.

Above mentioned incident handling processes are meant to be the roadmap for the incident handlers to follow the activities during the processes to better understand the criteria while handling and responding to incidents in future.

Figure 10. Incident Management

Preparation

The Preparation phase of the incident handling process includes everything related to an organization's incident handling readiness.

- Employees
  - A Skilled Response Team
  - IT Security Training
  - Security Awareness/Social Engineering activities, Cyber Drills etc.
- Documentation
  - Well-defined policies
  - Well-defined response procedures
  - Breach/incident communication plan(s)
  - Maintaining a chain of custody of actions
- Defensive Measures
  - A/V, (H)IDS, DLP, EDR, Security Patches
  - SIEM, UTM, Threat Intelligence
  - NSM, Central Logging, Honeypots, etc.

Incident management involves incident handling and incident response. It includes the process of receiving, prioritizing and responding back to incidents and reports. According to

Detection and Analysis

The Detection & Analysis phase of the incident handling process includes everything related to detecting an incident:

- Means of detection: Sensors (FW, IDS, Agents, Logs, etc.) | Personnel (Need to be trained)
- Information and knowledge sharing
- Context-aware threat intelligence
- Segmentation of the architecture

- Good understanding of / visibility in your network

An effective and actionable way to logically categorize your network is by considering the Following levels:

- Network perimeter
  - Firewalls, internet-facing NIDS, IPS, DMZ systems, etc. can assist such detection activities
- Host perimeter
  - Local firewalls or HIPS systems can assist such detection activities
- Host-level
  - A/V, Endpoint detection and response solutions can assist detection activities for data residing in the host.
- Application-level
  - Detection at the application level occurs by analyzing various logs that includes; application logs, service logs etc.

Containment, Eradication and Recovery

- Containment is preventing an incident from getting worse (i.e., preventing the intruder from getting any deeper). Containment is divided into sub phases:
  - Short-term containment:
    - We should try to render the intrusion ineffective, without altering the machine's hard drive (we need to image it for forensic activities). To do so, we can disable network connectivity or
  - System Backup
    - Make images of the affected system for forensics activities. To preserve the evidence, you're not supposed to work on the original machine when investigating and you're also not supposed to analyze and work on the first image you take
  - Long-term containment:
    - If you are not still able to determine the attacker's actions or even motives, you may recommend leaving the machine intact and closely monitor the attacker's next moves. Critical systems can't

easily go down since they are related to core business processes or operations

- Eradication process includes eliminating intruder artifacts, understanding the root cause, attack vectors and TTPs in general, utilizing backups and improving. Important phases of eradication are eliminating attacker's residuals such as malware and improving defenses.
  - Eliminating attacker's residuals includes
    - Removing malwares such as backdoors, rootkits, malicious kernel-mode drivers, etc.
    - In case of a Rootkit, zero the drive out, reformat and rebuild the system for trusted install media.
    - Thoroughly analyze logs to identify credential reuse through Remote Desktop, SSH, VNC etc.
  - Improving defenses includes:
    - Configuring additional router & firewall rules.
    - Obscuring the affected system's position, establishing effective system hardening, patching, and vulnerability assessment procedures, etc.
- Recovery includes restoring and monitoring to make sure nothing evaded detection. Following key points explained should be employed:
  - Process System Recovery
    - Once the affected system is restored, ask the business unit to perform QA activities to ensure the system's running condition.
    - Also, ask the business unit to ensure the system includes everything needed for their operations.
  - Restore of operations:
    - A decision has to be made regarding when the restored system will enter production again.
    - Consult/coordinate with the business unit for this matter.
  - Monitoring
    - Once the restored system is back to production:
    - Keep a close eye for oversights. Stealthy backdoors may still exist.
    - Network, as well as host-based intrusion systems, should be utilized, looking for signs/patterns/signatures related to the original attack.

- Thoroughly analyze critical logs and events for signs of re-infection or re-compromise.

On account of the assortment of information sources, advanced digital forensic techniques can also be utilized for many reasons, for example, researching crimes and internal arrangement 48 infringement, reproducing computer security incidents, investigating operational issues, and recouping from recovering system harm [38].

Post-Incident Activity

In Post-incident Activity phase, incident handler reports the identified weaknesses, oversights, blind spots, etc., regarding both their processes and technological measures. Following the recovery phase, it is crucial for the incident handling team to create a comprehensive, precise, and objective report that documents the lessons learned during the incident handling process. This is not to say that the report should contain only the identified weaknesses, oversights, and blind spots. The insights gained from these lessons can facilitate enhancements not only in incident recovery, but also in the security operations, policies, and other areas of the organization [37]. Working processes and successful detection methods should also be included. Incident handler should focus his energy on improving his processes, technological measures and visibility.

Incident Response Policy, Plan and Procedure

Organizations running CSIRT should follow a coordinated, focused and formal approach to tackle the emerging threats hitting the running businesses by providing them incident response at the right time. This is all achieved by formulating policies, plans and procedures at the foremost to enhance the working performance of incident response

Policy

- Statement of management committee
- Purpose and objective of the policy
- Scope of the policy
- Organizational structure, roles and responsibilities
- Performance measures
- Prioritization or severity rankings
- Reporting and contact forms

Plan

Organizations should follow a sophisticated approach to respond to security incidents including an incident response plan that would ultimately help out the organization to boost their cyber incidents capability and will disclose the hidden approaches one uses to handle incidents. Incident response plan contains organization's mission, team structure, approach of dealing with incidents and the size of structure. The incident response plan should include the following key elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the people in the organization and also with other organizations
- Metrix for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Procedure

Procedures are the ultimate operations that are based on incident response plan. These are known as standard operating procedures because these are the representations of organization's approach towards incident handling that includes technical processes, checklists and the expertise of people working in long run to combat cyber security incidents. SOPs should be described thoroughly such that it should depict the organization's preparation towards incident response, moreover, SOPs should be created to maximize the usefulness and effectiveness of CSIRT.

Physical Location for Establishing CSIRT

The physical location for establishing a CSIRT can depend on various factors, including the size of the organization, the types of threats they face, and the resources available. Here are some factors to consider when choosing a location for a CSIRT:

1. **Proximity to IT Infrastructure**: It's important for a CSIRT to be located near the IT infrastructure they are responsible for protecting. This can help to reduce response times in the event of an incident and ensure that the team has access to critical systems and data.

2. **Accessibility**: The location of the CSIRT should be easily accessible by both internal staff and external stakeholders, such as law enforcement and regulatory agencies.
3. **Security**: The physical location should be secure and protected from potential threats such as physical attacks or natural disasters.
4. **Connectivity**: The location should have reliable internet connectivity to enable the CSIRT to communicate with other organizations and access threat intelligence sources.
5. **Availability of Skilled Workforce**: The location should have a pool of skilled cybersecurity professionals who can be recruited to work in the CSIRT.

3.2 Role if AI in CSIRT Operations

Artificial Intelligence (AI) can play a significant role in improving the efficiency and effectiveness of a CSIRT. Here are some examples of how AI can be used in CSIRT operations:

1. **Threat Detection**: Artificial intelligence can be leveraged to examine substantial amounts of information from diverse origins, such as system logs and network traffic logs, in order to detect anomalies and patterns that may suggest a potential security risk. Machine learning algorithms can be trained to identify known and unknown threats and prioritize them based on the level of risk they pose. Here are some ways AI can do it:-
    - **Machine Learning Algorithms**: Machine learning algorithms can be trained on large datasets of known threats to identify patterns and detect unknown threats. These algorithms can analyze data in real-time and provide alerts to CSIRTs when a potential threat is detected.
    - **Anomaly Detection**: AI-powered systems can use statistical analysis and pattern recognition to identify unusual behavior in network traffic or system logs that may indicate a security threat. This can help CSIRTs to identify threats that may not be detectable using traditional signature-based detection methods.
    - **Natural Language Processing (NLP)**: NLP can be used to analyze text-based sources such as social media and online forums to identify threats

and potential attackers. This can help CSIRTs to identify threats that may be discussed in public forums or social media before they are executed.

- **Predictive Analytics**: AI can analyze historical data and use predictive analytics to identify patterns and trends that may help predict future threats. This can help CSIRTs to prepare for potential threats and allocate resources effectively.
- **Autonomous Response**: AI can be used to automate incident response and take action to contain a threat automatically. This can help reduce the response time and allow CSIRTs to focus on more complex tasks.

2. **Incident Response**: AI can assist in incident response by automating repetitive tasks such as log analysis, incident triage, and notification. This can help free up human resources to focus on more complex tasks that require human judgment and expertise. Here are some ways AI can do it:-
   - **Incident Triage**: AI can be used to automatically prioritize incidents based on severity and the potential impact on the organization. This can help CSIRTs to focus their resources on the most critical incidents first.
   - **Log Analysis**: AI can be used to analyze system and network logs to identify the cause of an incident. This can help CSIRTs to quickly identify the root cause and take appropriate action.
   - **Threat Hunting**: AI can be used to identify and investigate potential threats before they escalate into incidents. This can help CSIRTs to proactively detect and respond to threats before they cause any damage.
   - **Autonomous Response**: AI can be used to automatically contain and mitigate incidents by implementing predefined response actions. This can help reduce the time it takes to respond to an incident and limit the damage caused.
   - **Chatbots**: AI-powered chatbots can be used to provide instant support to end-users who report incidents. This can help reduce the response time and allow CSIRTs to focus on more complex tasks.
3. **Vulnerability Management**: AI can be used to scan systems and applications for vulnerabilities and prioritize them based on the level of risk they pose. This can help CSIRTs to identify and remediate vulnerabilities before they are exploited by attackers. Here are some ways AI can do it:-

- **Vulnerability Scanning**: AI can be used to automatically scan systems and networks for vulnerabilities. AI-powered vulnerability scanners can identify and prioritize vulnerabilities based on their severity and the potential impact on the organization.
- **Patch Management**: AI can be used to automate the patch management process by identifying which patches are needed and automatically deploying them to vulnerable systems. This can help ensure that systems are kept up-to-date and protected against known vulnerabilities.
- **Risk Assessment**: AI can be used to assess the risk associated with vulnerabilities by analyzing data from multiple sources such as threat intelligence feeds and security incident logs. This can help CSIRTs to prioritize vulnerabilities and allocate resources effectively.
- **Predictive Analytics**: AI can be used to analyze historical data and use predictive analytics to identify patterns and trends that may help predict future vulnerabilities. This can help CSIRTs to proactively identify and remediate vulnerabilities before they can be exploited.
- **Intelligent Remediation**: AI can be used to automatically remediate vulnerabilities by implementing predefined response actions.

4. **Threat Intelligence**: AI can be used to analyze threat intelligence feeds and identify trends and patterns in the threat landscape. This can help CSIRTs to stay ahead of emerging threats and proactively defend against them.
   - **Data Collection**: AI can be used to collect and analyze vast amounts of data from multiple sources such as social media, dark web, and open-source intelligence. This can help CSIRTs to identify potential threats and attack patterns.
   - **Threat Hunting**: AI can be used to automate the process of identifying potential threats by analyzing large data sets and identifying patterns that may indicate malicious activity. This can help CSIRTs to proactively detect and respond to threats before they cause any damage.
   - **Threat Attribution**: AI can be used to attribute attacks to specific threat actors by analyzing attack patterns, malware signatures, and other indicators of compromise. This can help CSIRTs to identify the motives and capabilities of attackers and take appropriate actions.

- **Threat Prediction**: AI can be used to analyze historical data and use predictive analytics to identify patterns and trends that may help predict future attacks. This can help CSIRTs to proactively identify and mitigate potential threats before they can be exploited.
- **Threat Visualization**: AI can be used to create visualizations of threat data to help analysts better understand and interpret the data. This can help CSIRTs to quickly identify trends and patterns that may be indicative of malicious activity.

5. **Predictive Analytics**: AI can be used to analyze historical incident data to identify patterns and trends that may help predict future incidents. This can help CSIRTs to better allocate resources and prepare for future incidents.
   - **Behavioral Analysis**: AI can be used to analyze user and system behavior to identify abnormal patterns that may be indicative of an attack. This can help CSIRTs to proactively detect and respond to potential threats before they cause any damage.
   - **Threat Intelligence Analysis**: AI can be used to analyze threat intelligence feeds to identify emerging threats and vulnerabilities. This can help CSIRTs to prioritize their efforts and allocate resources effectively.
   - **Risk Scoring**: AI can be used to score and prioritize vulnerabilities and potential threats based on their severity and potential impact. This can help CSIRTs to focus on the most critical threats and vulnerabilities first.
   - **Malware Analysis**: AI can be used to analyze malware to identify patterns and characteristics that may be indicative of specific types of malware. This can help CSIRTs to identify and respond to new or unknown malware threats.
   - **Incident Prediction**: AI can be used to analyze historical data and use predictive analytics to identify patterns and trends that may help predict future incidents. This can help CSIRTs to proactively identify and mitigate potential threats before they can be exploited

3.3 Research Survey

This survey is being conducted to gather the statistics for information related to CSIRT. The information collected is solely used by Hasnain Shafiq (Student of MCS, NUST for his Master's Thesis). Following is the title of his thesis:

"Analysis of Issues and Challenges of Establishing and Operating CSIRTs"

Brief Introduction about CSIRT

CSIRT is a specialized group of people within or outside an organization whose responsibilities are to receive, review and respond to security incidents. The ultimate goal of CSIRT is to reduce the impact and control the consequences of an incident.

1. This survey study is filled by: _____ (optional)
2. Which type of organization you work for? Detection and Analysis
    - Government
    - Telecommunication
    - Financial
    - Academia
    - Others
3. What is your role in organization?
    - Director
    - Manager
    - Technical
    - Staff
    - Others
4. What is your experience in current organization?
    - 1-3 years
    - 4-7 years
    - 10+ years

Below questions are related to need and importance of information security

1. Does your organization give importance to inventory management?
    - Yes
    - No
    - Don't know

2. How do you ensure security of your critical assets?
    - Internal security analyst/CSIRT
    - Out-sourcing
    - Don’t know
3. How often your organization conducts risk assessment of assets?
    - Weekly
    - Monthly
    - Quarterly
    - Don’t know
4. How often your organization conducts cyber security awareness sessions?
    - Monthly
    - Quarterly
    - Annually
    - Never done
5. Who is responsible for information security within your organization?
    - CEO
    - Information Security Department
    - Everyone
    - Don’t know
6. Did your organization ever hire cyber security team?
    - Yes
    - Never used
    - No
    - Don’t know
7. Does your organization monitor and prevent unwanted traffic into your network via IDS/IPS/Firewall?
    - Yes
    - No
    - Never used
    - Don’t know
8. Has your organization ever encountered cyber-attack/incident?
    - Yes
    - No

- Don’t know

9. How your organization handles cyber-attacks/incidents? (Multiple answers allowed)
    - IDS/IPS/Firewall
    - Security Operation Center
    - Vendor CSIRT
    - Don’t know
10. Does your organization perform vulnerability assessment internally?
    - Yes
    - No
    - Out-sourcing
    - Don’t know
11. How your organization conducts security assessment [vulnerability assessment, penetration testing, digital forensics, malware analysis, risk assessment] of your organizational assets?
    - Internally hired security analyst
    - Out-sourcing/CSIRT/SOC
    - Never conducted security assessment
    - Don’t know
12. What sources your organization usually follows for security updates?
    - Public websites
    - Subscribed mailing list
    - Security Operation Center/CSIRT
    - Don’t know

Below questions are related to need and importance of CSIRT

13. Do you think CSIRT can help your organization in meeting your business objectives by securing your organization from security incidents?
    - Yes
    - No
    - Don’t know
14. Did your organization ever face the need of CSIRT for monitoring your valuable assets from cyber-attacks/incidents?
    - Yes

- No
- Don’t know

15. Does your organization has a CSIRT?
    - Yes
    - No
    - Don’t know
16. How much experience you think should be necessary for the Incident Response Team?
    - 1-3 years
    - 4-7 years
    - 10+ years
    - Don’t know
17. What type of CSIRT services would you recommend for financial, government, healthcare institutions?
    - Proactive
    - Reactive
    - Security Alerts
    - Don’t know
18. CSIRT often shares their research and findings via a website or another suitable medium. How much you are satisfied with the free public services?
    - Strongly agree
    - Agree
    - Strongly disagree
19. CSIRT also provides paid services where dedicated people continuously provides support and subscribed services to their constituencies. How much you are satisfied with paid services?
    - Strongly agree
    - Agree
    - Strongly disagree
20. What factors you think can enhance the effectiveness of CSIRT? (Multiple answers allowed)
    - Clear Mission
    - Defined services

- Skilled information security personals
- Don’t know

21. What factors you think can limit the effectiveness of CSIRT performance? (Multiple answers allowed)
    - No proper policies, procedures defined
    - Lack of CSIRT’s authority
    - Management of numerous security tools
    - Don’t know
22. Did your organization ever establish a CSIRT for your own business? If so, what type of issues/problems you have faced?
    - Unclear mission statement
    - Lack of resources
    - Budget constrain
    - Never had own CSIRT
23. Do you believe a national CSIRT can reduce the impact of cybersecurity attacks on public or private infrastructure?
    - Yes
    - No
    - Don’t know
24. Our company (xyz) is starting a CSIRT with the collaboration of FIRST (global leader and premier organization which specializes in incident response). Are you interested in availing our paid services?
    - Yes
    - No
    - Don’t know

3.4 Mapping Survey to Objectives and Research Questions

In order to achieve the meaningful results from the survey, the author has mapped questions of the survey that were asked from different organizations to the research objectives and response statistics are also listed below:

Table 5: Mapping Survey to Objectives and Research Questions

Q. No	Questions	Objectives of Questions	Mapping with Research Questions	Response Statistics

1	Does your organization give importance to inventory management?	Without effective inventory management, every component that is added to IT inventory becomes new point of vulnerability. IT inventory management requires that the hardware is fully tagged and tracked during the lifecycle, unaccounted and out-of-date software and hardware can be exploited easily. Proper and sufficient safeguards should be pre-implemented in order to protect from any cyber incident.	Q2, Q4	86% have mentioned that their organization gives importance to inventory management system.
2	How do you ensure security of your critical assets?	What type of services an organization has availed to ensure the security of their assets, whether they have hired internal information security team to maintain a check and balance of their information assets e.g. web applications, servers, network devices etc. or they are using services from third party.	Q2, Q4	76% of the organizations in Pakistan is utilizing internal security analysts/teams. While a minor number (11.6%) of organizations are still out-sourcing for ensuring the security of their assets.
3	How often your organization conducts risk assessment of assets?	How much organization takes its information security genuinely?	Q1	44.6% people are of the views that their organizations conduct risk assessment activities of critical or information assets quarterly.
4	Does your organization monitor and prevent unwanted traffic into your network via IDS/IPS/Firewall?	Does the organization is dependent on security monitoring tools, if so how much protection those signature based monitoring tools are providing to the end users/information assets?	Q1	83.5% organizations are monitoring and preventing unwanted traffic in their networks via automated security tools.
5	How your organization handles cyber-attacks/incidents?	What type of security controls, safeguards are used by organizations to prevent security incidents (this shows	Q1	78.3% organizations are handling cyber-attacks via automated security

		how much organization is interested in protecting its information assets)?		monitoring tools e.g. IDS/IPS/Firewalls or anti-virus software.
6	Does your organization perform vulnerability assessment internally?	Do organizations acquire third party services or always rely on internally hired individuals or security team. This shows how interestingly an organization takes the security measures for protection of their internal information assets.	Q1	71% have mentioned that their organizations are ensuring the security of their critical assets internally.
7	How your organization conducts security assessment [vulnerability assessment, penetration testing, digital forensics, malware analysis, risk assessment] of your organizational assets?	The objective of this question was to get insights about the number of organizations who have either hired internal information security teams for security assessment of their critical assets, getting third party services or never did security assessment. This Would help in understanding the need and importance of CSIRT in Pakistan.	Q1	64.5% organizations have internal teams for security assessment activities, while 19.8% out-source for conducting security assessment of their infrastructure
8	What sources your organization usually follows for security updates?	How keen organizations are regarding vulnerability disclosures/security updates/cyber security?	Q1	41% organizations usually follow updates recommended by security operation center. While 24% follows public websites and 14% are using subscribed mail services.
9	Do you think CSIRT can help your organization in meeting your business objectives by securing your organization from security incidents?	Do organizations have the understanding of CSIRTs (and their services) that is/are actively working in developed countries to protect the constituency's infrastructure? If so, then CSIRT should be established in Pakistan to deliver proactive services.	Q1, Q3	84.3% believe that CSIRT can help an organization in meeting their business objectives by securing their organization from computer security incidents.
10	Did your organization	Organizations in developing countries	Q1, Q3	70.2% organizations

	ever face the need of CSIRT for monitoring your valuable assets from cyber-attacks/incidents?	lack appropriate security controls, safeguards, skilled personnel etc., their infrastructure are more vulnerable to cyber incidents as compared to the organizations that are working in developed countries, since those organizations are utilizing the services of CSIRTs 24/7.		working in Pakistan have faced the need of CSIRT.
11	Does your organization have a CSIRT?	The objective of asking this question was to understand the challenges that any organization might have witnessed during the establishment of CSIRT for their own organization. This would help us in proposing a better solution to overcome the challenges that may rise in Various stages of CSIRT development. Moreover, a general stat about the number of CSIRTs working in Pakistan could be achieved.	Q3	Apart from security operation center, 42.2% organizations in Pakistan don't have CSIRT which makes them less secure compared to those who have utilized information security center services.
12	How much experience you think should be necessary for the Incident Response Team?	There are number of challenges that organizations may face during CSIRT operational phases. One of which is the capability of resources. Primarily, the skillset of resources is the major challenge that needs to be identified and overcome before putting the services in place.	Q4	46.3% organizations believe that 4-7 years of experience should be required for handling cyber security incidents.
13	What type of CSIRT services would you recommend for financial, government, healthcare institutions?	The objective was to achieve a stats about the number of organizations in Pakistan who are interested to avail the proactive services from a CSIRT. Since proactive services determines the efficiency of a CSIRT and discriminates it from any other ordinary information security team.	Q2, Q4	81.8% employers believe proactive security measures are more effective than getting an email alert or via any other medium.

14	CSIRT often shares their research and findings via a website or another suitable medium. How much you are satisfied with the free public services?	The objective of asking this question was to figure out the interest of various organizations in availing CSIRT services if they didn't have yet. Sharing information about new cyber threats, vulnerabilities, advisories, are one of the primary services of CSIRTs to facilitate the constituencies. Overviewing the quality of free services can increase the number of constituencies.	Q4	91.8% agrees with the free public services. Although, paid services for dedicated resources to organizations are also offered by CSIRTs. 91.2% organizations are interested to enroll for paid services if they get opportunity to have a CSIRT in Pakistan.
15	What factors you think can enhance the effectiveness of Computer Security Incident Response Team (CSIRT)?	The objective is to figure out the factors that should be addressed in order to increase the effectiveness of CSIRT. Identifying the factors would help us to overcome the Problems that decrease the effectiveness of CSIRT services.	Q2, Q3, Q4	55.8% organizations believe that a clear mission of a CSIRT can make its services more effective while 65.8% mentioned defined services whereas 86.7% believe that skilled people of a CSIRT are the building blocks who enhance the effectiveness and also deliver quality services.
16	What factors you think can limit the effectiveness of CSIRT performance?	The objective is to figure out the factors that limits the effectiveness of CSIRT. Identifying and addressing the factors would help us in long run to overcome the problems that decreases the effectiveness of CSIRT services.	Q2, Q4	82.5% organizations believe that no proper defined policies, procedures can limit the effectiveness of a CSIRT. 40% mentioned lack of CSIRT's authority for services or agreement, 77.5% mentioned CSIRT effectiveness decreases if it lacks skilled personnel whereas 29.2% highlighted about management of

				numerous security tools can limit the effectiveness.
17	Did your organization ever establish a CSIRT for your own business? If so, what type of issues/problems you have faced?	Since Pakistan doesn't have a public/national CSIRT, the objective of this question was to understand what type of problems organizations might have faced if they have ever tried to establish a CSIRT for their own organization.	Q1, Q3	35.8% organizations voted that they never had a CSIRT. While the rest of the organizations have had different issues/problems while establishing a CSIRT for their organizations i.e. 20% have unclear mission statements. 20.8% have budget concerns whereas 23.3% have lack of skilled resources.

3.5 Chapter Summary

This chapter focused on understanding the problems that an organization may face during CSIRT establishment and operation. To solve this problem author has conducted a survey specifically in Pakistan to identify the issues and challenges that may hinder the establishment of CSIRT. Survey 59 results are mapped to objectives and research questions to obtain response statistics. For better understanding of CSIRT business it is important to know the challenges that CSIRT personnel faces during the day-to-day operations. Moreover, incident management was thoroughly discussed in this chapter. Each phase of incident management provides a depth of knowledge regarding the methodologies, tools and technologies required to perform incident handling in more effective way.

Chapter 4

Results and Analysis

In this chapter empirical data is analyzed and compared with the theoretical part. A survey was distributed among professionals of various organizations in order to effectively disclose the issues and challenges which may cause troubles during the establishment and operation phases of CSIRT. The survey was split into two parts; first part addressed the need and importance of information security within an organization whereas the second part was focused on the need and importance of CSIRT. The reason behind splitting of survey into two sections was very clear, in fact significant approach to understand how organizations working in Pakistan are addressing the need and importance of information security. The survey was filled by working employees of government, financial, academic, healthcare and telecom institutions. The overall respondent's number matched the figure of 121.

4.1 Frequency Analysis

Before proceeding with the statistics of survey outcomes, it is necessary to show the survey respondents (target audience) to efficiently achieve the analysis results. This survey is filled by people belonging to academia, cyber security services provider, financial, government, healthcare IT solution provider, IT services, private and telecommunication sectors. The overall analysis is based on the statistics obtained from people with different set of minds, working in different institutions with different methodologies and job roles. The statistical analysis would help to better understand the need and importance of CSIRT by asking series of questions related to information security and the set of policies and procedures different organizations run by in Pakistan to tackle the cyber security challenges. Below graph demonstrates the percentage of people who have provided their views on behalf of their organizations.

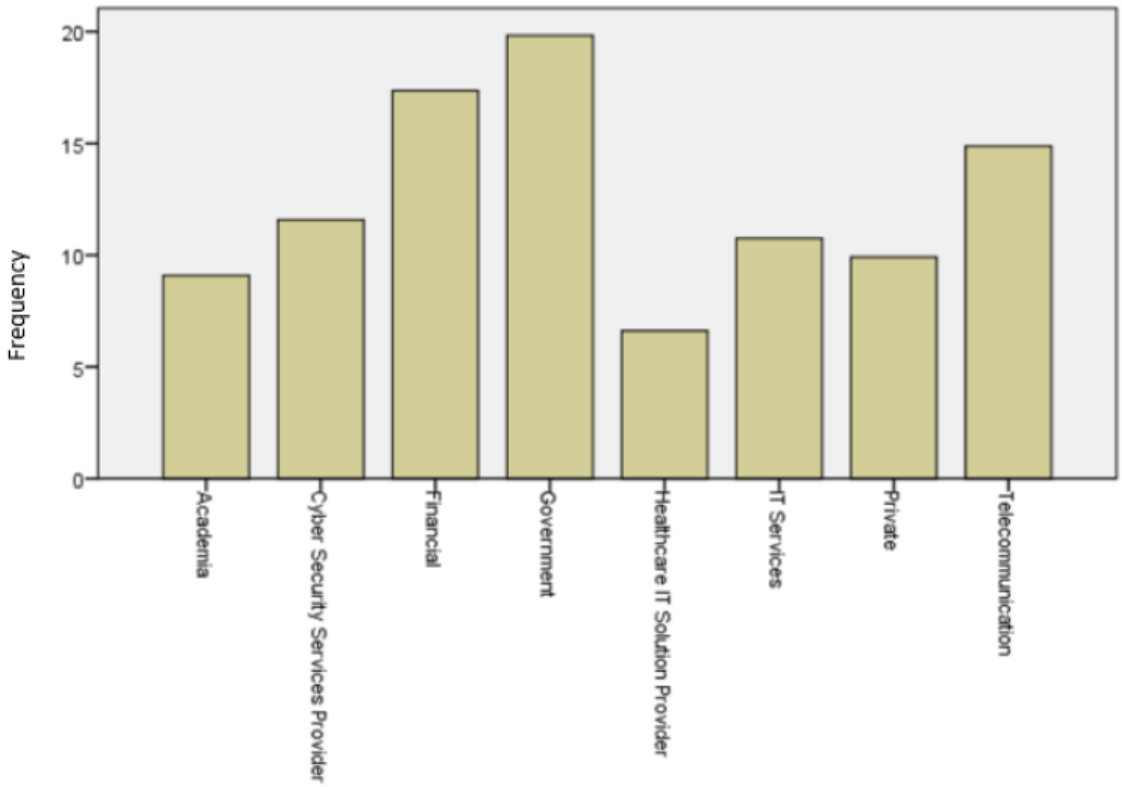


Figure 11: Type of organizations

Following table shows the frequency (number of organizations) with percentage.

Table 6: Types of organizations

Type	Frequency	Percentage
Academia	11	9.1
Cyber Security Services Provider	14	11.6
Financial	21	17.4
Government	24	19.8
Healthcare IT Solution Provider	8	6.6
IT Services	13	10.7
Private	12	9.9
Telecommunication	18	14.9
Total	121	100.0

Respondent's role in organization

Majority of the respondents on survey have technical expertise in related domain area. The below graph shows the percentage of respondents with various job roles whose point of views on this research survey may vary due to technical or managerial work backgrounds. However, the distributed background provides a real-world statistics which would be obviously used to analyze the results in more proficient way.

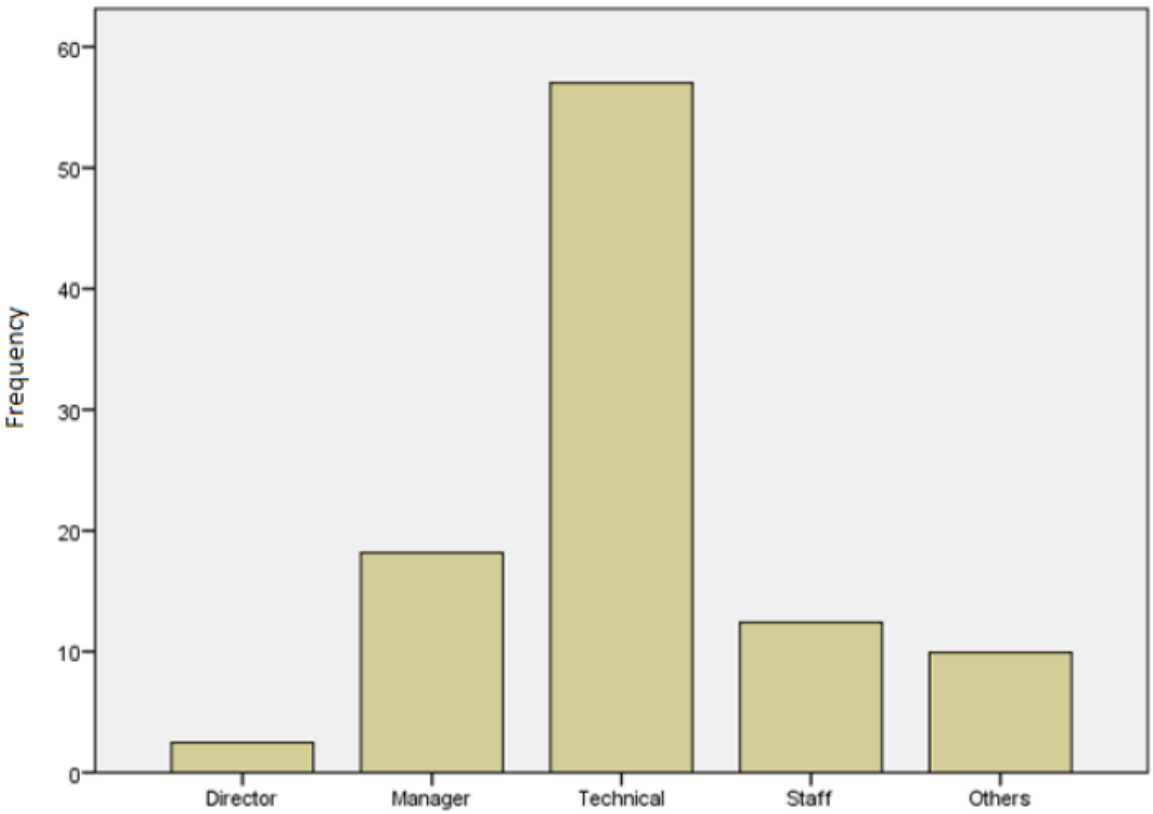


Figure 12: Respondents role in organization

Following table shows the frequency (number of respondents) with percentage of each role.

Table 7: Respondents role in organization

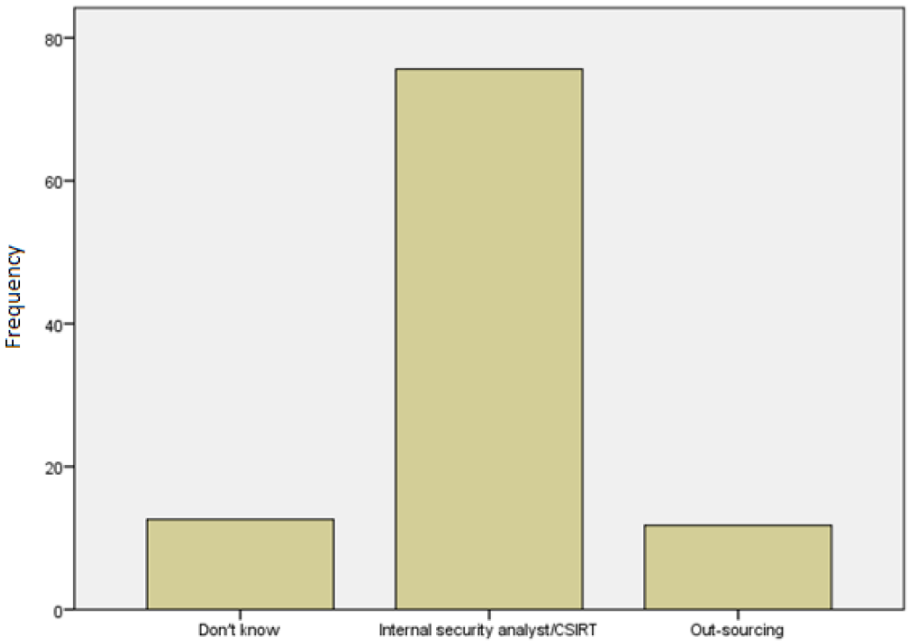
Roles	Frequency	Percentage
Director	3	2.5
Manager	22	18.2
Technical	69	57.0
Staff	15	12.4

Others	12	9.9
Total	121	100.0

Management of critical assets

The management of critical assets including their logical and physical security is the insurance of survival of organization. Majority of the organizations in Pakistan are dependent on internal security analysts/teams. While a minor number of various organizations are still out-sourcing for ensuring the security of their assets. Most of the organizations have network teams who are actively 63

working as internal security team responsible for making, running various security policies, procedures and also involved in security assessment of organization. Such organizations lack skilled people who should be dedicated for maintaining security of an organization. While there are few firms who have dedicated teams to put their best in order to ensure the security



of organizational infrastructure by all means.

Figure 13: Management of critical assets

Following table shows the frequency with percentage of each methodology.

Table 8: Management of critical assets

Methodology	Frequency	Percentage
Internal security analyst/CSIRT	92	76.0
Out-sourcing	14	11.6
Don’t know	15	12.4
Total	121	100.0

Responsible for Information Security

Most of the employees working in organizations despite of their work roles, they don’t have an idea about the protection of their organizational critical assets including personal information that may risk existence of data and may result in data disclosure to third party. Every organization if working in critical form of data for instance patient’s health information should implement strong information security controls in order to protect the identities of their clients which in this case are 64

patients. Most countries have strong information security laws which could end up putting a penalty on organization in case of data leakage due to poor information security controls.

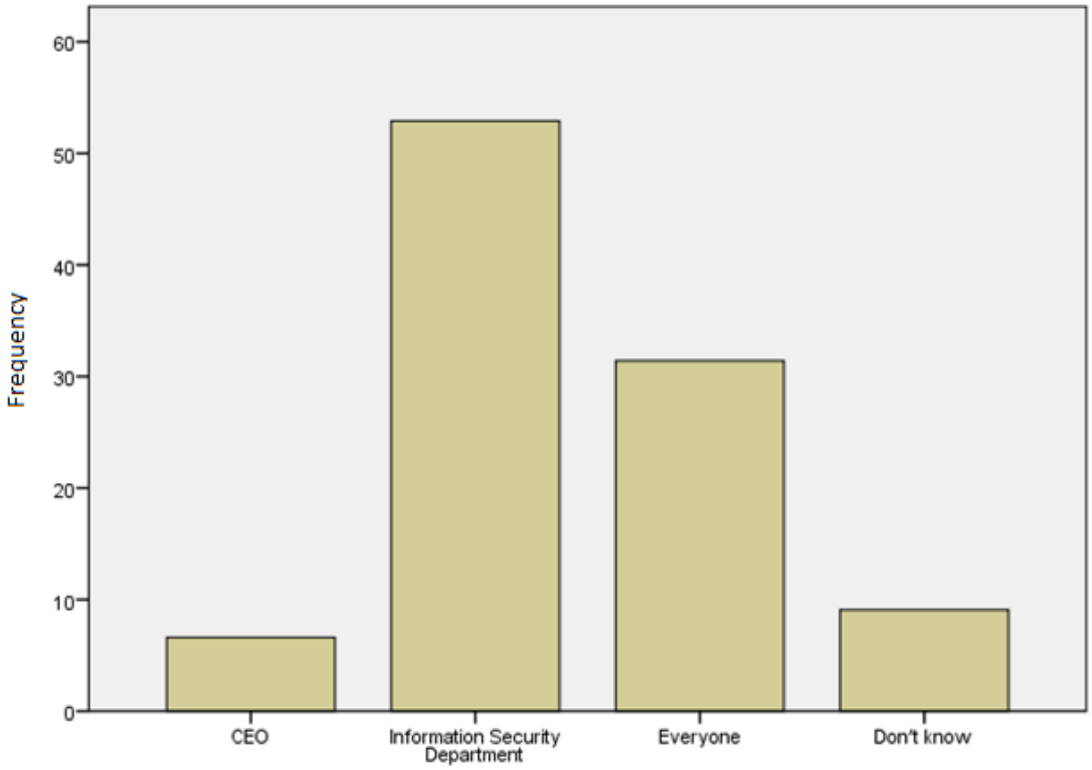


Figure 14: Responsible for Information Security

The above graph explicitly shows that majority of the organizations are still dependent on information security department which certainly lacks skilled employees to handle cyber incidents in more progressive and independent way Though each organization should impose the necessary learning by each employee to at least protect themselves from any cyber security incident. Following table shows the frequency and percentage of above graph.

Table 9: Responsible for Information Security

Responsible	Frequency	Percentage
CEO	8	6.6
Information Security Department	64	52.9
Everyone	38	31.4
Don’t know	11	9.1
Total	121	100.0

Monitoring and preventing unwanted traffic via IDS/IPS/Firewalls

Most of the organizations are fully dependent on the use of various traffic monitoring and preventing tools that looks the ingress and egress traffic which by itself segregates the legitimate and malicious traffic with the help of built-in mechanism (signature etc.). Malicious traffic allowed to enter network is the launch of successful cyber security attack and is also considered the first step. Asking various organizations about the security mechanism would help in determining whether organizations working in Pakistan do need CSIRT or not. Although, traffic monitoring tools do not have any direct relationship with implementation of CSIRT, these tools just help out in meanwhile forensics of any cyber security incident. Following figure shows that maximum organizations are fully dependent on traffic monitoring tools which could help them in monitoring malicious traffic but that doesn’t guarantee the protection of organizational critical assets.

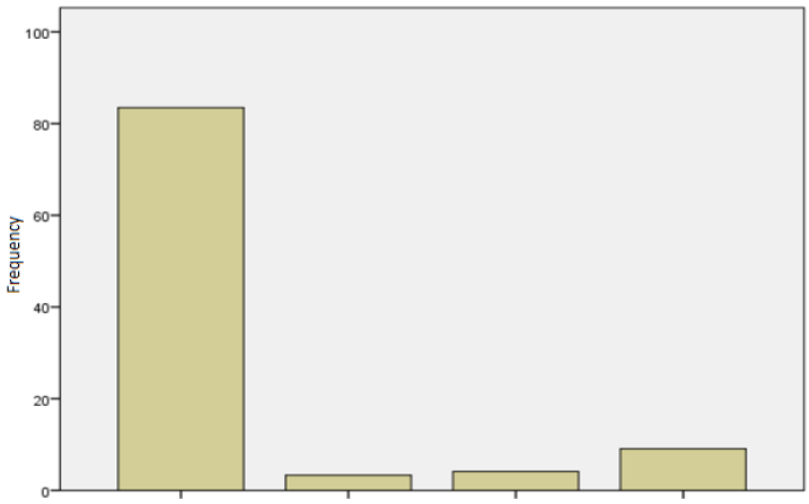


Figure 15: Monitoring Traffic via security tools

Below table shows the frequency and percentage of use of traffic monitoring tools.

Table 10: Monitoring Traffic via security tools

Options	Frequency	Percentage
Yes	101	83.5
No	4	3.3
Never used	5	4.1
Don’t know	11	9.1
Total	121	100.0

Victims of Cyber Attacks

During the survey analysis it was disclosed that majority of the firms were became victims of cyber-attacks probably because of implementing weak or no cyber security safeguards. Although, no organization wants to disclose whether they were hacked or became a cyber-attack victim due to the fear of losing customers trust, reputation etc. or holding strong position in market. These firms don’t publish or share the cyber information with their customers in fact many organizations could have lost their customers personal or sensitive data in cyber breaches. Below figure shows a huge number who become victim, nevertheless there are people who still don’t know despite working in the same organization for years. Cyber-attacks happen on such organization because they don’t take information security or cyber security seriously resulting in loss of sensitive data disclosure, loss of reputation, loss of money etc. Spending on information security is worth it. Cyber incidents are happening in hundreds of thousands in numbers on daily basis, becoming a victim is far easy than thinking about it. Taking precautionary measures could help in protecting oneself or organization in long run.

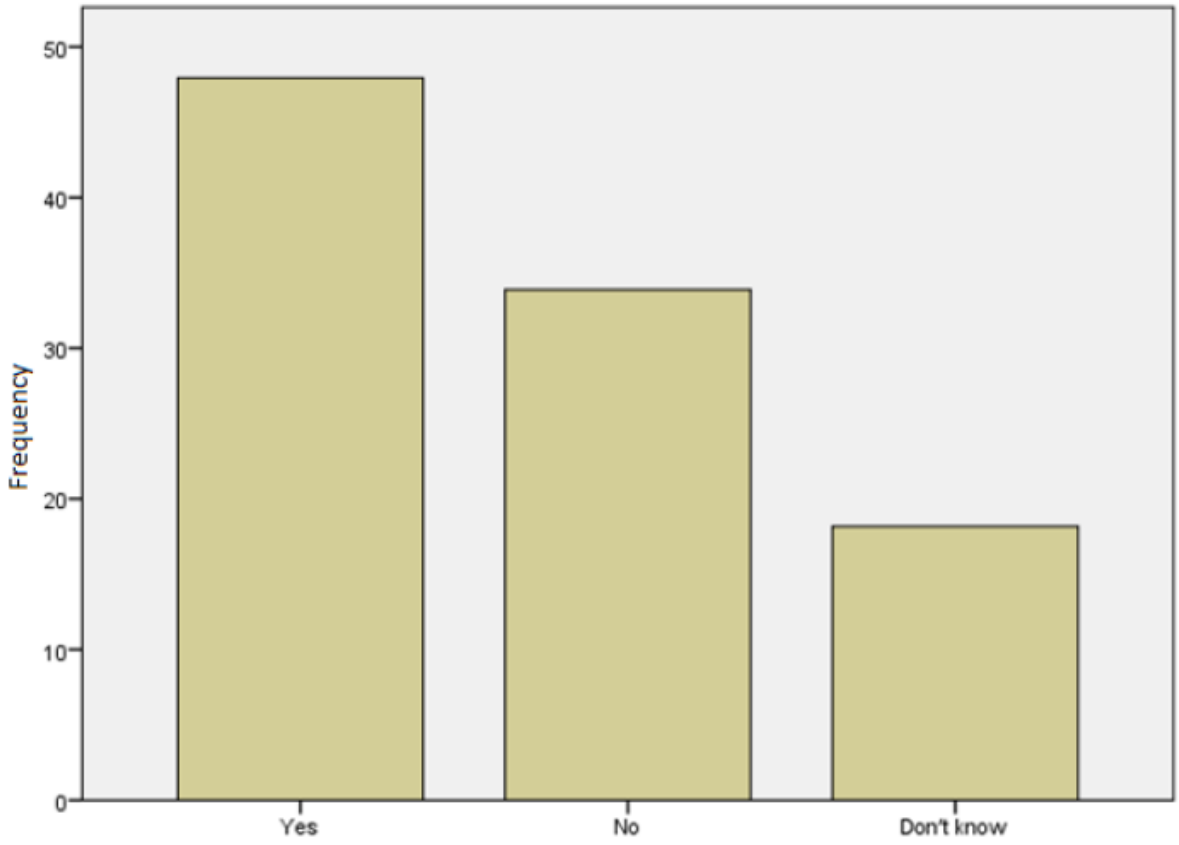


Figure 16: Victims of cyber attacks

Below table shows the frequency and percentage of organizations who become the victims of cyber-attacks.

Table 11: Victims of cyber attacks

Options	Frequency	Percentage
Yes	58	47.9
No	41	33.9
Don’t know	22	18.2
Total	121	100.0
Yes	58	47.9

Handling Cyber Incidents

Below graph shows that majority of the organizations are dependent on IDS/IPS/Firewall for maintaining security controls in their organization. Although there is no mechanism implemented which help in responding to cyber security incidents at the right time. Threat intelligence also plays an importance role in handling cyber incidents prior to happening by

analyzing the indicators of threats also available on threat intelligence platforms. The survey against handling cyber incident shows that various organizations don't have a proactive measure to handle cyber incidents. Despite very limited organizations are taking services from vendor organizations.

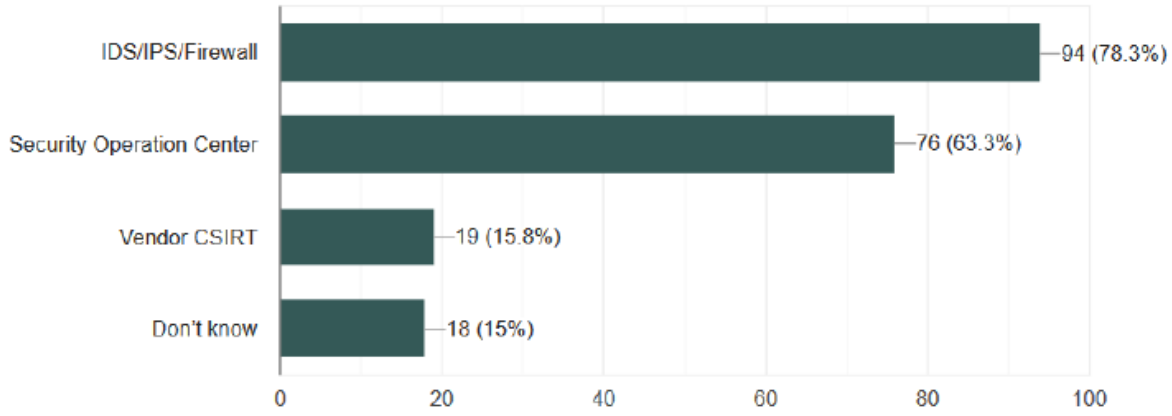


Figure 17: Methodology of handling cyber incidents

Importance of CSIRT

It is important to recognize that incident handling encompasses more than just intrusions. Incidents related to insider threats, service disruptions, and intellectual property loss are also part of incident handling. An effective incident handler should have knowledge of the methods, strategies, and procedures used by attackers. They should have a comprehensive understanding of the various stages of the cyber kill chain. This will allow them not only to anticipate attacks but also to recommend appropriate defensive measures. These are the needs of any organization in the world of threats to identify the challenges and make effective measures to incorporate information security controls in each phase of implementation and adaptation of information security management systems. The importance is already identified by people of various sectors and are aware of CSIRT services which help one organization in achieving its business objectives more efficiently by securing sensitive assets or data.

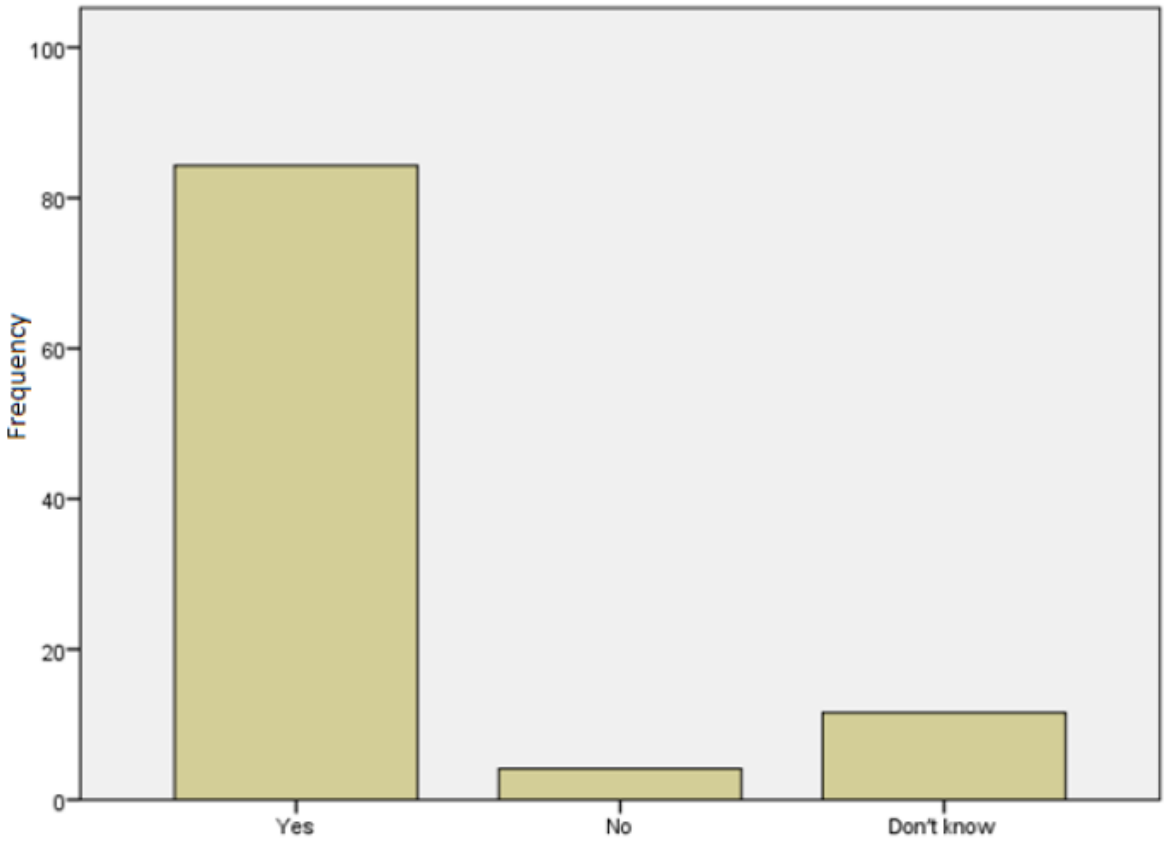


Figure 18: CSIRT security assurance

Below table shows the frequency and percentage of representatives of organizations who believe that CSIRT can help them in meeting their business objectives by protecting against cyber security incidents.

Table 12: CSIRT security assurance

Options	Frequency	Percentage
Yes	102	84.3
No	5	4.1
Don't know	14	11.6
Total	121	100.0

Factors Enhancing CSIRT Effectiveness

Respondents were asked question related to enhancing the effectiveness of CSIRT which would help out in determining the factors. Although, there are multiple set of rules and procedures to enhance the output of any CSIRT. Respondents came up with different viewpoints that helped in collecting useful collection which shows that majority of the respondents i.e. 86.5% believe that skilled information security personals are necessary to be

a part of CSIRT to enhance the effectiveness. Along with this, 65.8% believe CSIRT should define their services to constituencies in order to avoid any deadlock and 55.8% believe clear mission of CSIRT can enhance the effectiveness of CSIRT services and can work in long run with their constituencies.

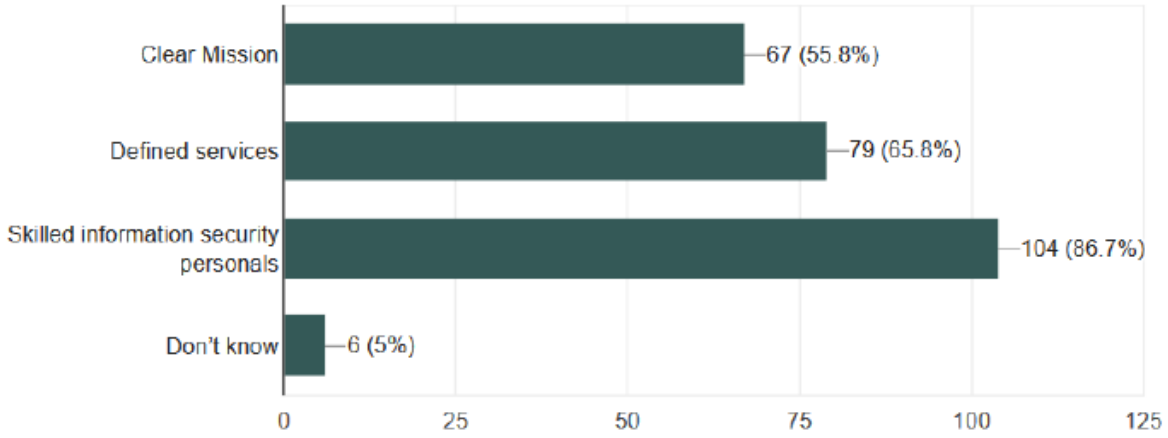


Figure 19: Factors enhancing CSIRT effectiveness

Factors Limiting CSIRT Effectiveness

It was observed that CSIRT has some limitations on the other hand too due to various factors. Respondents were asked to highlight the factors and came up with results such that most of organizations with 82.5% believe that no CSIRTs do not follow proper policies and procedures which in most cases are not defined. 77.5% believe that limitation factors include lack of skilled people which is truly one of the effective factors that can enhance the effectiveness of CSIRT. Employees with suitable skillset are difficult in market to be hired for the job role whereas 40% are of the views that CSIRT lacks authority in the absence of any high management which might result in the ineffectiveness of CSIRT operations. A smaller number of people i.e. 29.2% mentioned that using multiple tools for the same operations could result in the falsification of outcomes that limits the effectiveness of CSIRT operations.

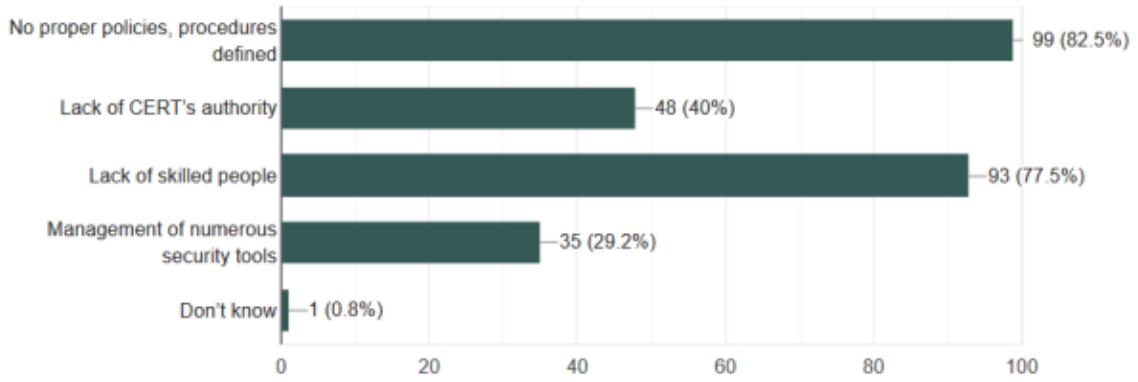


Figure 20: Factors limiting CSIRT effectiveness

Issues Faced During CSIRT Establishment

Target audience was inquired whether they had their own CSIRT for their private organization or not. 35% respondents answered that they didn't have any CSIRT or never thought to establish. With second number of 23.1% people thought that they lack resources for establishment which seems to be obvious reason behind no CSIRT. It is observed during the survey that 21.5% organizations didn't have handsome budget to continue the process of establishment. While 19.8% people didn't have any idea about the purpose or working of CSIRT to handle a standalone project.

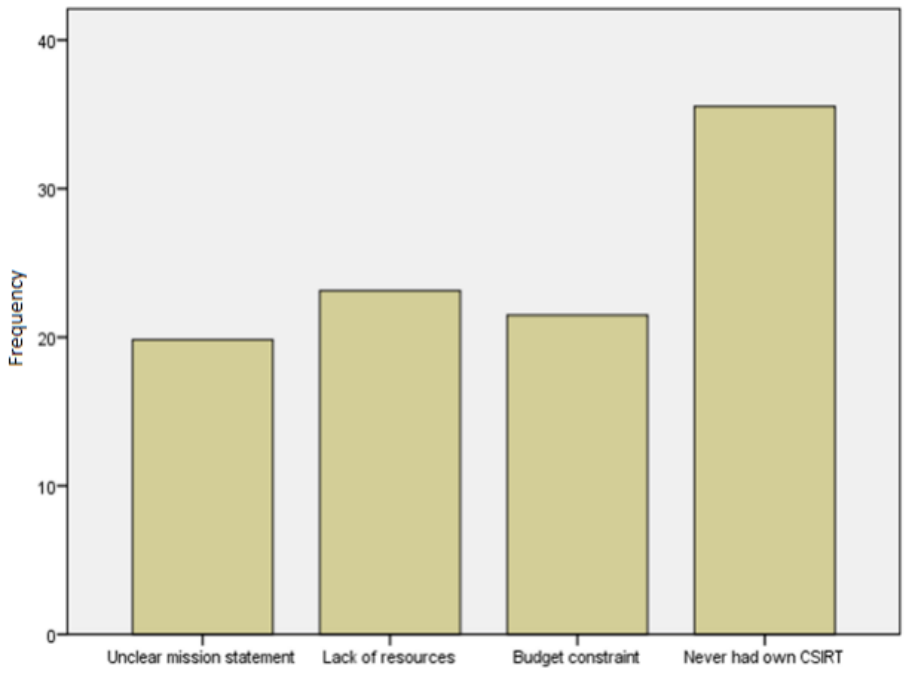


Figure 21: Issues faced during CSIRT establishment

Below table shows the frequency and percentage of organizations who faced issues/problems while establishing CSIRT for their organizations.

Table 13: Issues faced during CSIRT establishment

Options	Frequency	Percentage
Unclear mission statement	24	19.8
Lack of resources	28	23.1
Budget constrains	26	21.5
Never had own CSIRT	43	35.5
Total	121	100

4.2 Correlation Analysis

Correlation analysis validate the association among various variables. The aim of the correlation analysis in this study is to check the liaison between different variables that includes ensuring security of critical assets, need of CSIRT, encountered cyber-attacks, monitoring & preventing malicious traffic, National CSIRT reduce cyber-attacks. The analysis of the correlation between different variables provides insight into their strengths and weaknesses. The value of the correlation determines the outcome of the analysis. If the value is 0, it indicates that there is no direct relationship between the variables. Conversely, any value that is not 0 indicates either a positive or negative relationship. The positive or negative sign accompanying the value indicates the nature of the relationship. A positive sign indicates a direct relationship where an increase in one variable results in an increase in the other. On the other hand, a negative sign denotes an indirect relationship where an increase in one variable leads to a decrease in the other.

The values of the correlation table: 14 shows that there is a positive and significant relation between the variables. Analyzing the values one by one, we can see that encountered cyber-attacks by organization and CSIRT need faced by organizations has a value of $r = 0.283^{**}$ at $p < 0.01$.

Table 14: Correlation Analysis

S. No.	Variables	Mean	Std. Deviation	1	2	3	4	
1	Ensure security of critical assets	1.3636	0.69522	1				
2	Encountered cyber-attacks	1.7025	0.75988	0.175	1			
3	Need of CSIRT	1.4298	0.71678	0.202*	0.283**	3		
4	Monitoring & preventing malicious traffic	1.3884	0.93427	0.384**	0.070	0.122	4	
5	National CSIRT reduce cyber-attacks	1.2727	0.63246	0.076	0.084	0.291**	0.158	5

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Ensuring security of critical assets has positive relationship with monitoring and preventing malicious traffic with $r = 0.384^{**}$ at $p < 0.01$. Similarly, need of CSIRT and national CSIRT has a positive value of $r = 0.291^{**}$ at $p < 0.01$.

4.3 Summary of Data Analysis

Going through survey statistics that is conducted in various organizations of Pakistan, the author of this research document needs to analyze the obtained data in detail.

- In total respondents of 121, 86% have mentioned that their organization gives importance to inventory management system which has its own cons that is beyond the scope of this research document to discuss.

- 76% have mentioned that their organizations are ensuring the security of their critical assets internally that ultimately points to the capability of internal security team who are hired time to time to protect their assets.
- 44.6% people are of the views that their organizations conduct risk assessment activities of critical or information assets quarterly.
- Majority of the employees working in organizations have no idea about information security or the policies and procedures that one organization follows to keep itself at a safe distance from malicious intents.
- 19.8% people said their organizations didn't conduct cyber security awareness training in mean time that is one of the reasons that employees are exploited very easily.
- 52.9% employees believe that only information security team within organization is responsible for protecting information assets.
- 62.8% employees thought their organization hires external information security professionals for fulfilling the temporary needs e.g. to get compliant to certain standard.
- Cyber security incidents don't just leak data but pose serious threats to the existence of organization, those security incidents usually hit top level management who hold certain amount of confidential and sensitive information that could be used in lateral movement. In majority times those incidents are caused by weak organizational networks policies and safeguards.
- In cyber era, employers are still dependent on security monitoring tools, the survey results shows that 83.5% organizations are not following defense in depth policies such that they are making use of IDS/IPS/Firewalls which doesn't guarantee the protection against cyber-attacks.
- With the use of traffic monitoring tools, 47.9% organizations still have been hit by cyber-attacks.
- To remain up to date with malware families e.g. virus, worms, ransom wares, one organization has to practice proposed security measures that provides maximum level of protection against cyber security incidents. Those world class security standards or platforms for confronting with security threats are the means to protect identity, infrastructure, and sensitive information.
- Majority of the organizations in Pakistan are fully dependent and also taking dedicated services from vendor security operation centers that are by no means

free to acquire at all. Still 84.3% believe that CSIRT can help one organization in meeting their business objectives by securing their organization from security incidents.

- In the world of cyber warfare, 70.2% organizations working in Pakistan have ultimately acknowledged the need of CSIRT and believed that it can protect organizations from cyber damages that couldn't be achieved by using day to day security monitoring tools.
- Although, maximum organizations working in Pakistan doesn't know about CSIRT or their use to protect themselves.
- 81.8% employers believe proactive security measures are more effective than getting an email alert or via any other medium.
- CSIRT do offer public and private services which facilitates each and every organization despite of their work description.
- Pakistani organizations seemed interested in availing paid services for which 91.8% employees voted.
- 82.6% employers wanted or showed interest to have a national CSIRT in Pakistan that should be designated by one's country government or economy. National CSIRT have specific responsibilities in cyber protection for the country or economy.

4.4 Findings

Below table shows the response analysis with recommendations:

Table 15: Response Analysis and Recommendations

Q. No	Response Analysis	Recommendations (if any)
1	The huge number shows that organizations are keeping track of their assets which helps them to take precautionary measures before any breach happens. There still exists, 14% organizations who might have not ranked their organizational critical assets that could lead to a data breach.	Recognize the importance of inventory management in information security domain
2	The huge number shows that majority organizations have built their own information security teams where they look after their critical	Acquire third party services for getting external organization's security posture.

	assets. However, various service level agreements with external vendors also go in consideration.	
3	Near half number of organizations are conducting risk assessment quarterly which is likely a nice figure to be protected from external threats. But on the other side, half number of organizations are vulnerable to cyber-attacks.	
4	The high number shows that majority of the organizations are fully dependent on traffic monitoring tools e.g. IDS/IPS/Firewalls and have already taken precautionary measures for data security. While there are many organizations who are open to threats with no security measures at place.	Acquire proactive services
5	The high number shows that majority of the organizations are dependent on automated tools that primarily depend on signatures-based detections that usually fails in case of new threats. Network traffic monitoring tools alone cannot guarantee the integrity and confidentiality of data within network.	Acquire proactive services
6	The high number shows that majority of the organizations are performing vulnerability assessment internally, this could be due the fact that internal team knows the information security controls installed in organization more effectively than a third party.	Perform external security assessment to identify any missing loopholes if left by the internal security team.
7	It has been identified that organizations on large scale are not out-sourcing for conducting security assessment of their information assets. This shows the level of trust they have for external vendor organizations, may be due to fear of losing their sensitive information or weak areas.	

8	Near half of the organizations are protecting themselves against discovered threats via security operation centre which might be installed in their organizations while the rest are using public/mailing list which might put them at risk or due to any negligence or lack of knowledge to handle particular incident/threat.	Utilize services of an experienced personnel due to the fact that the security procedures could be breached any time due to negligence or unawareness of particular issue.
9	The huge number shows the importance of CSIRT in Pakistan, since CSIRT provides threat intelligence and threat hunting which is proactive approach and digital forensics that are frequently utilized in developed countries to maintain defense in depth.	
10	70% organizations acknowledged the need of CSIRT and believe it can protect organizations from cyber security incidents that couldn't be achieved by using day to day security monitoring tools. The need of CSIRT is dependent on business type/needs/objectives.	Utilize proactive services in financial, government, healthcare institutions
11	It is discovered that organizations working in Pakistan are mostly utilizing in-house information security teams. 42% organizations are vulnerable to external threats due to unavailability of any implemented security mechanism.	
12	Incident management domain lacks experts to work in incident handling process effectively. Primarily, skillset of people required for incident management is not up to the mark to compete sophisticated techniques, tactics, and procedures of adversaries.	capacity building of employees
13	Proactive security measures enable organizations to combat computer security incidents in more	

	effective way than reactive services. Proactive services are highly recommended for financial organizations, since these services are more than defined set of alerts.	
14	It has been found that IT, Government, Healthcare, Telecom, Academic institutions are interested in paid services of CSIRT if Pakistan has its own CSIRT. Apart from the paid services, CSIRT provides free alerts/emails, advisories to the subscribers to earn their trust.	
15	The statistics shows that organizations do have the knowledge regarding factors that can enhance the effectiveness of CSIRT. If the team performs well in delivering their services, the better the CSIRT will progress. Clear mission and trust among various domain members and team skillset effects the progress of CSIRT.	define proper policies, procedures, identify the tools required for incident management, employee should be aware of his roles and responsibilities
16	No proper documented policies and procedures can limit CSIRT effectiveness, each team member should be aware of its authority under the supervision of upper management and in their absence. The team should be skilled enough to work in strict environments and use of defined tools can overcome alert fatigue.	define proper policies, procedures, identify the tools required for incident management, employee should be aware of his roles and responsibilities
17	The response shows that majority of the organizations working in Pakistan do not own a CSIRT. While the distinct statistics shows that organizations might have faced various problems while establishing CSIRT for their organizations.	Need of information security awareness, capacity building of employees, trust sharing within different organizations

Answers of Research Questions:

1. **What are the issues in establishing CSIRTs?**

Organizations are lacking skilled resources and funding etc. Majority of the organizations are not aware of modern technologies to combat cyber-attacks. Lack of trust on external vendors led to usage of deprecated technologies for countering cyber-attacks. Moreover, un-clarity in mandate, lack of stakeholder's trust are the issues in establishing CSIRTs.

2. **What are the issues in operating CSIRTs?**

   Organizations face technical and operational issues including lack of skilled manpower, un-clarity in providing services, inter-department issues and lack of administration support, mandate and equipment. CSIRT's technical needs may be against constituency's ICT policy.

3. **What are the challenges in establishing CSIRTs?**

   A lot of equipment is needed for remote assistance. Administration support is highly required in CSIRT establishment which generally becomes a huge challenge to overcome. Moreover, clear mission, type of services and mutual cooperation among various domain members are the challenges in establishing CSIRTs.

4. **What are the challenges in operating CSIRTs?**

   Proactive services need to be provided to the constituencies for which trained employees are not available most of the times. Selection of CSIRT services, incorrect understanding of processes hinders CSIRT operations. No proper defined policies, procedures are also the challenges in operating CSIRT.

It has been understood from the research done so far that, most of the organizations in Pakistan are dependent on internally hired information security team who are only responsible for implementing and the maintenance of information security and the policies and procedures required in this area. Majority of the organizations lack potential technologies that are in high demand and actively used by the developed countries. Pakistani organizations are fully dependent on the use of security tools that includes IDS/IPS/Firewalls of legacy rules. These tools lack modern embedded technologies that could hinder a cyber-attack. Regardless of usage of highly expensive security tools, near 50% of the organizations in Pakistan become the victim of cyber-attacks. In this research, a survey helped to disclose the hidden and never asked questions from organizations about the need of CSIRT, near 85% organizations shown interest in having a CSIRT in their organization or on national level which could help them to protect their organization from any cyber-attack or espionage. It has been identified in the survey that skilled people are the only means to increase the

effectiveness in working CSIRTs and the lack of skilled people and undefined policies and procedures can make a huge hurdle in the establishment and operation phase of CSIRT. Meanwhile, Government of Pakistan has not implemented the newly proposed cybercrime law back in 2016. Without any legislation, no organization can put their efforts in maintaining and proposing cyber security services on national level. Although, cybercrimes are not justified by any means but still organizations need accepted legislations by the parliament to carry out their services and establish a private or national level CSIRT to protect and share remedial services to the constituencies.

4.5 Business Model of CSIRT

Till here, this research document has covered what a CSIRT is, what is the framework of CSIRT, defining the mission statement and the services it provides to its constituency. The next step is to define the business model of a successful working CSIRT.

1. Financial Model

Ideally, funding should align with the requirements of the constituency. However, in practice, the range of services that can be offered must be adjusted to fit within a specific budget. Therefore, it is more pragmatic to begin the planning process by considering financial matters.

- **Cost Model**

The costs are primarily influenced by two factors - determining the service hours and the number and quality of staff to be employed. It is plausible to consider a scenario where both proactive and reactive services are provided during office hours.

- **Revenue Model**

A revenue model should be properly approved and implementation should be fulfilled so the planned services be financed accordingly.

For this purpose, following scenarios should be taken into consideration.

- **User of existing resources**

  Maximizing the use of existing resources within the organization can bring significant benefits by reducing the need to hire additional staff and thereby controlling expenses.

- **Membership fee**

  You can offer your services to your constituency by charging them an annual or quarterly membership fee. Any additional

services that are requested by them, such as penetration testing, consultancy services, or security audits, would be charged separately.

- **Subsidy**

  Applying for project subsidies provided by government institutions is worth considering, as nowadays most IT projects are supported by the government.

2. Organizational Model

The appropriate structure of a CSIRT greatly relies on the current structure of the hosting organization and its constituency, as well as the availability of experienced professionals to be employed on either a permanent or as-needed basis. A typical CSIRT defines the following roles within the team:

- General Manager
- Staff
- Operational Technical team
- External Consultants

It is also necessary to have a legal advisor during the starting phases of CSIRT. This would raise the cost of the company but it will help CSIRT in time saving and legal troubles.

Following are few organizational models in use by operational CSIRTs;

1- **The independent business model**

The CSIRT is established and operates as a separate entity, having its own leadership and staff.

2- **The embedded model**

If a CSIRT is to be established within an existing organization, such as an IT department, this model can be employed. The CSIRT would function as an autonomous entity, led by a team leader who would be accountable for all of the CSIRT's operations.

3- **The campus model**

Academic and research CSIRTs often adopt the campus model, which is suitable for organizations that consist of multiple universities and campus facilities spread over a region or country.

4- **The voluntary model**

This organizational model depicts a loosely organized community of specialists who voluntarily come together to offer advice and support to one another and

others. The effectiveness of this model heavily relies on the motivation of the participants.

3. Developing an Information Security Policy

The IS policy of a CSIRT is tailored according to the type of CSIRT. This policy not only outlines the desired state of operational and administrative processes and procedures, but also needs to comply with relevant legislation and standards, particularly with regards to the liability of the CSIRT. National laws and regulations typically govern the activities of a CSIRT.

4.6 Chapter Summary

This chapter thoroughly discussed the survey statistics gathered during the research duration. A summary for each survey question is explained in detailed. Moreover, findings have been generated and response of survey results have been analyzed. At the end of this study, the author has also discussed the business model of CSIRT in order to continue the research to the next level. Business model explained shows the requirements needed in order to run a successful CSIRT.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

This research document has described about the framework of CSIRTs and its various components. The research is fully focused on the CSIRT problems faced during the establishment and operations in Pakistan. Literature review is conducted to know about the work done in the field of incident handling and the measures taken collectively by various organizations in developed countries to overcome the problems, since in developing countries e.g. in Pakistan these problems are not yet recognized or solved. This research has established a baseline to identify the issues and challenges during the CSIRT establishment and operations in Pakistan. To conclude this, the major complications that creates hurdles during educating departments belonging to various domains about the importance of information security, getting a mandate from Parliament is one of the most significant factor for data monitoring and compliance of information systems. After which, follow ups and capacity building of Government staff are also mandatory factors that influence the establishment of CSIRTs. Apart from these issues and challenges several other key factors e.g. funding, lack of authority of CSIRT and deficiency of skilled people creates interruption in the establishment of CSIRTs. Increasing volumes of computer security alerts based on legacy software and technologies, competition for skilled analyst and lack of knowledge transfer between analysts, budget constraints with security incidents becoming more costly, legal and regulatory compliance, and lack of CSIRT's authority, less number of resources, no proper policies and procedures defined are the main issues due to which organizations are unable to establish CSIRT on broader level. According to some policy-makers, it has become crucial for CSIRTs to collaborate with government authorities to identify the source of cyber-attacks, in order to promote the sharing of information and knowledge to mitigate vulnerabilities and respond to such incidents effectively. Despite all the problems highlighted during the course of this research, organizations in Pakistan are still motivated and have already acknowledged the need and importance of CSIRT in Pakistan.

5.2 Future Work

This study identified the necessary steps required for establishment of CSIRT as well as the issues and challenges that might be encountered during the early phases of establishment. Future work needs to be done to resolve the issues and challenges that emerge during the development cycle of CSIRT. A working framework is required to be built upon which a private body or national CSIRT should be implemented. Training, awareness, capacity building and modern technologies use should be strongly encouraged. Moreover, legislation should be properly implemented by the government of Pakistan so that cyber-crime should be dealt in effective way.

References

[1] "FIRST - Improving Security Together." [Online]. Available: https://www.first.org/.

[2] M. Grobler and H. Bryk, "Common challenges faced during the establishment of a CSIRT," in Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010, 2010, pp. 1–6.

[3] ISO/IEC, "ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements," Inf. Technol. — Secur. Tech. — Inf. Secur. Manag. Syst. — Requir., vol. 2013, no. ISO/IEC 27001:2013, p. 38, 2013.

[4] Michelle Borodkin, "Computer Incident Response Team."

[5] J. Kyl, "S.982 - 104th Congress (1995-1996): National Information Infrastructure Protection Act of 1996," 1996.

[6] Moira J. West-Brown, Don Stikvoort, and Klaus-Peter Kossakowski, Handbook CSIRTs. 1998.

[7] U. Georgia Killcrece (Carnegie Mellon University), Robin Ruefle (Carnegie Mellon University, Creating and Managing CSIRTs. 2004.

[8] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide - Google Search," 2012.

[9] "Key Roles and Responsibilities for your Incident Response Team (3/5)," 2018. [Online]. Available: https://www.hitachi-systems-security.com/blog/roles-responsibilities-incident-response-team/.

[10] "CSIRT — IT Help and Support." [Online]. Available: https://help.uis.cam.ac.uk/service/security/csirt.

[11] Maliha Alam and Mehreen Shahid, "CSIRT Guide."

[12] "KP CERC | KPITB | Khyber Pakhtunkhwa Information Technology Board." [Online]. Available: http://kpitb.gov.pk/projects/kp-cerc.

[13] SANS, "Information technology - Security techniques – Information security management systems - Overview and vocabulary," Standards South Africa, Standard 27002," 2009.

[14] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek, Organizational Models for CSIRTs. 2003.

[15] C. J. Alberts, A. J. Dorofee, G. Killcrece, R. M. Ruefle, and M. T. Zajicek, “Defining Incident Management Processes for CSIRTs: A Work in Progress,” Oct. 2004.

[16] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, “State of the Practice CSIRTs.” 2003.

[17] ENISA, “Good Practice Guide for Incident Management,” 2010.

[18] Danny Smith, “Forming an Incident Response Team,” 1994.

[19] Nevil Brownlee, “Expectations for Computer Security Incident Response.” .

[20] R. Mooi and R. A. Botha, “Prerequisites for building a Computer Security Incident Response capability,” in 2015 Information Security for South Africa (ISSA), 2015, pp. 1–8.

[21] Y. M. Wara, “A Guide to Establishing CSIRT For National Research and Education Network (NREN).” 2015.

[22] Johannes Wiik and Jose J. Gonzalez, “Limits to Effectiveness in CSIRTs,” 2005.

[23] R. Teixeira, X. Koufteros, and X. D. Peng, “Organizational Structure, Integration, and Manufacturing Performance: A Conceptual model and Propositions,” J. Oper. Supply Chain Manag., vol. 5, no. 1, p. 70, Jun. 2012.

[24] ENISA, “Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organizational Aspects — ENISA,” 2017.

[25] J. Steinke et al., “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” IEEE Secur. Priv., vol. 13, no. 4, pp. 20–29, Jul. 2015.

[26] First Responder: Your First Response in Emergency Care - David Schottke, American Academy of Orthopaedic Surgeons - Google Books. 2007.

[27] M. Bada, S. Creese, M. Goldsmith, and C. J. Mitchell, “Improving the Effectiveness of CSIRTs.” 2017.

[28] “CSIRT Services Framework Version 1.1.” [Online]. Available: https://www.first.org/education/csirt_service-framework_v1.1.

[29] Robert Morgus, Isabel Skierka, Mirko Hohmann, and Tim Maurer, “National CSIRTs and Their Role in Computer Security Incident Response,” 2015.

[30] Johannes Wiik and Jose J. Gonzalez, “Preserving a balanced CSIRT constituency.” 2009.

[31] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, and R. Butler, “Palantir: A Framework for Collaborative Incident Response and Investigation,” in Proceedings of the 8th Symposium on Identity and Trust on the Internet - IDtrust ’09, 2009, p. 38.

[32] Isabel Skierka, Robert Morgus, Mirko Hohmann, and Tim Maurer, “CSIRT Basics for Policy-Makers,” 2015.

[33] R. Bhaskar, “A Proposed Integrated Framework for Coordinating CSIRT,” J. Inf. Priv. Secur., vol. 1, no. 3, pp. 3–17, Jul. 2005.

[34] "Best Practices for Establishing a National CSIRT", [Online]. Available: https://www.sites.oas.org/cyber/Documents/2016 - Best Practices CSIRT.pdf

[35] "Pakistan: National Assembly Passes New Cybercrime Law." [Online]. Available: https://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/

[36] "The Prevention of Electronic Crimes Act, 2016." [Online]. Available: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

[37] Michael Bartock, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, Karen Scarfone "Guide for Cybersecurity Event Recovery".

[38] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, "Guide to Integrating Forensic Techniques into Incident Response".