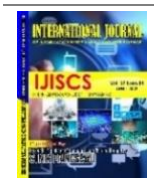

**IJISCS (International Journal of Information System and Computer Science)**
IJISCS, Volume 9, Number 2, August 2025
E ISSN: 2598-246X; P ISSN: 2598-0793, pp. 79-85
**Accredited SINTA 4 Number 79/E/KPT/2023**
https://jurnal.ftikomibn.ac.id/index.php/ijiscs

# ENHANCING CYBERSECURITY INCIDENT RESPONSE: A STRUCTURED APPROACH TO CSIRT ROLE ALLOCATION

*Corresponding author
hussam8830@gmail.com

**Hosamaldeen Hamd**
Information Technology Department, Gulf College,
HafrAlbatin, Saudi Arabia

**Article history**:
Received July 3, 2025
Revised July 16, 2025
Accepted August 4, 2025

**Keywords:**
Incident;
IR (Incident Response);
CSIRT

**Abstract**

The process of responding to cyber incidents requires professional skills and standardized methods. Incident responders often face challenges in determining who is responsible for addressing cybersecurity incidents. Consistence between incident response team members is crucial for two reasons: first, to eradicate and fix the incident effectively; second, to save time and effort. This paper proposes a model for distributing roles within an Incident Response (IR) team. Each member is assigned both basic and shared responsibilities to ensure comprehensive coverage. Three main roles are identified-Risk Analysis, Alerts and Warnings, and Security Consultant-which are designed as universal roles adaptable to teams of any size.

## 1.0 INTRODUCTION

The digital transformation of our lives, work, and social activities has led to an increase in cyber incidents and attacks. Preparing, planning, and mitigating security incidents while responding to cyberattacks must become an integral part of every organization's daily routine. One of the most critical steps in risk management is preparing an effective Incident Response (IR) team and clearly defining the roles of its members. These roles enable the team to address various types of attacks and system compromises, whether internal or external. Proper role distribution ensures that team members understand their responsibilities and can collaborate seamlessly during incident response operations.[8]

In addition to technical tasks, the IR team also handles logistics, such as writing reports and communicating with stakeholders. While specialists focus on resolving incidents, team leaders and communication specialists ensure that non-technical stakeholders receive timely updates. This paper addresses these challenges by proposing a structured model for role distribution within a CSIRT.[8]

## 2.0 INCIDENTS AND INCIDENTS RESPOND TEAM

### 2.1. Incident in cybersecurity

According to Rosencrance (2019), security incidents are events that indicate a compromise of an organization's systems or data or the failure of protective measures. Incidents can occur intentionally or unintentionally, caused by system users, employees, clients, or hackers. They may also arise from artificial intelligence (AI) systems or expert systems. The following section discusses the human actions that impact CSIRT operations.[8]

### 2.2. Incident Categories

Incidents are categorized based on their nature and target. Key categories include [6]:

- Cyberwarfare (CW): Attacks aimed at degrading, neutralizing, or destroying enemy combat capabilities.
- Hacktivism (H): Combining hacking and activism to exploit systems for ideological purposes.
- Cyber Espionage (CE): Targeted attacks on companies and institutions rather than individuals.
- Cybercrime (CC): Criminal activities involving networks and computers, including hacking and traditional crimes conducted online.

**2.3. Computer Security Incident Response (CSIR)**

CSIR relies on a team of professional cybersecurity analysts to respond to threats and manage their aftermath. CSIRTs consume and produce threat intelligence, ensuring appropriate technology and best practices are applied to counter network attacks. [1]

**2.4. Computer Security Incident Response Team (CSIRT)**

The CSIRTs will generally be the consumers of threat intelligence but can also be producers of threat intelligence from their internal sources.[7] CSIRT is a unit dedicated to guaranteeing that suitable technology and best systems management practices are utilized to counter attacks on networked environment and in addition to restricting harm and guaranteeing coherence of critical services despite effective attacks. Once an incident happens, participants of a CSIRT can aid its constituency in figuring out what happened and what moves need to be made to remedy the circumstances.[2]

Some cybersecurity scholars argue that the best way to train efficient cyber security incident response teams (CSIRTs) is to ensure that training is designed to be pragmatic, with training activities that include role-playing, games, and simulation exercises. [3] Currently, CSIRTs fulfill different functions or areas in society or organizations, due to the constant growth of threats and ways of corrupting security, which is why it is necessary to know the standards, measures and functions that are applied in each sector [1]. Due to the size of the companies, it is not feasible to use an individual CSIRT, so private or public CSIRTs must be used to provide their information security services to the members that belong to their network. [4]

Constructing CSIRT now adays is not option or bias but essentially and critically need, and this is due to several reasons as follows:

- Reliability of cyber services 24/7
- increases of cyber crime
- quickness of cybers algorithms decryption.
- nor option from cyber except cyber
- etc.

## 3.0 TEAM CONSTRUCTION REASONS:

Cybercrime is an emerging form of transnational crime, and it is one of the fastest-growing areas of crime. contends that cybercrimes, such as confidentiality or privacy data breaches, could lead to the theft of personal data from millions of people across the globe [2]. Major CSIRT processes include preparation, detection, analysis, containment, eradication, recovery, and post-incident actions, the study of CSIRTs is different than cognitive expertise studies of individual analysts because CSIR is a distributed, team-based activity [2].

**3.1 Human actions:**

In the context of cybersecurity, human actions play an important role in the incident response team construction. for example, Employees' misuse actions, such as clicking on phishing links or downloading/sending malicious attachments, can lead to information system' breaches or malware infections. Proper training and awraness of traditional security methods will helps more of avoiding these problems and be safe, but applying this successfully, depends on too many reasons as follw:

- how many hours employees spent it on training
- how much money the organization also spent.
- controlong and monitoring methods used
- the importance of security to stakholder.
- CSIRT efforts in education and awarness.

- How long employees adhere to the training outcomes.
- Etc.

**3.2 Human incidents' types and methods:**

Human behavior is impossible to accurately predict or/and effectually monitor, more importantly, an insider is part of the organization, there for they are trusted to some extend and have legitimate credentials. Accordingly, it is almost impossible to spot a capable insider who is planning to undertake an attack and because human are creative, their harmful actions are is almost impossible to assure by automated means.[9] Cybersecurity Awareness programs can help reduce the likelihood of number of incidents, which maybe in form of workshop, digital news, signboards, incentives, and rewards, and too many creative methods.

**3.3 People/Employees help CSIRT:**

People play a crucial role in supporting incident response teams by contributing their knowledge, skills, and actions to help prevent, detect, respond to, and recover from cyber incidents. Here's how individuals/managers can assist incident response teams:

- participating in cybersecurity awareness programs and training sessions presented by IR team.
- Reporting unfamiliar Activity: If individuals spot anything unusual or suspicious, such as unexpected pop-ups, unusual system behavior, or unfamiliar requests for sensitive information, they should promptly report it to their organization's IT or security team.
- Adherence to Security Policies: This includes using strong passwords, updating software regularly, and applying security patches.
  - Data Protection and Privacy: Properly encrypting data, using secure communication channels, and limiting the sharing of sensitive information can help protect against unauthorized access.
  - Secure Software Practices: following coding best practices, conducting security testing, and addressing vulnerabilities.
  - Incident Reporting: Timely reporting can help mitigate the impact of an incident.
  - Backup and Recovery: Having reliable backups can aid in restoring systems and data after an incident.
  - Staying Informed: Keeping up-to-date with the latest cybersecurity trends, threats, and best practices.
  - cyber incidents and enhance overall security posture.

In summary, individuals have a significant role to play in cybersecurity incident response by reporting suspicious activities, and collaborating with incident response teams to minimize the impact of

## 4.0 PROPOSED CSIRT'S ROLES MODEL:

Essential roles of CSIRT generally are tow, reactive and proactive roles, which conceptually mean "before" and "after" accidents been happen, the reactive "before" role is the process of finding or expecting network's limitations and/or vulnerabilities that might be happens internally or externally, and the proactive "after" role is the process of remediating and handling effects of attacks or any reactions made after accidents.

- According to the European Commission there many requirements and skills for CSIRT or CERT as they mentioned (CERT is short for Computer Emergency Response Team) [5], in the following model' diagram I proposed most of the CSIRT roles/functions required for all members.
- This proposed model relies on distributing roles between IR' team members, according to their label and job position, and make them shared some roles to fill the gap if some team members absent or basically not found there.

is the process of finding or expecting network's limitations and/or vulnerabilities that might be happens internally or externally, and the proactive "after" role is the process of remediating and handling effects of attacks or any reactions made after accidents.

- According to the European Commission there many requirements and skills for CSIRT or CERT as they mentioned (CERT is short for Computer Emergency Response Team) [5], in the following model' diagram I proposed most of the CSIRT roles/functions required for all members.
- This proposed model relies on distributing roles between IR' team members, according to their label and job position, and make them shared some roles to fill the gap if some team members absent or basically not found there.

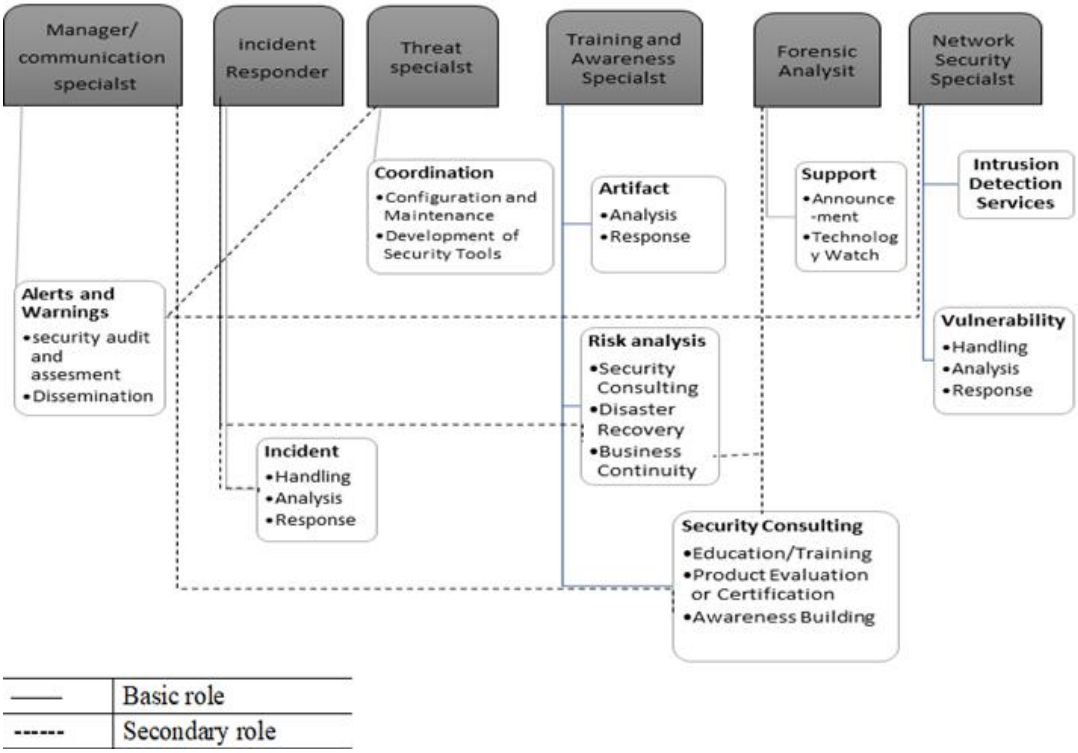


Figure 1 Proposed model of CSIRT roles distribution

**4.1 Role's distribution results**

For all job position there are important roles, these roles can be divided into basic and secondary functions, members of team may play the basic functions as well as the secondary functions at the same time, also may just play the basic functions according to the size and scope of the organization or according to the nature of the incident, here in the following tables is the results of functions distribution and relative job position.

**4.2 Role Distribution:**

The proposed model divides roles into three main categories: Risk Analysis, Alerts and Warnings, and Security Consultant. These roles are distributed among team members based on their job positions, with shared responsibilities to fill gaps if some members are absent. Below are the results of the role distribution: [7]

**Table 1: Risk Analysis Role**

| Role | Incident Responder | Training Specialist | Forensic Analyst |
|---|---|---|---|
| **Basic Role** | Incident Handling, Analysis, and Response | Artifact and Risk Analysis | Support |
| **Shared Role** | Risk Analysis | Risk Analysis | Risk Analysis |

Table 2: Alerts and Warnings Role

| Role | Network Specialist | Threat Specialist | Manager/Communication Specialist |
|---|---|---|---|
| **Basic Role** | Vulnerability Handling, Intrusion Detection | Coordination | Alerts and Warnings |
| **Shared Role** | Alerts and Warnings | Alerts and Warnings | Alerts and Warnings |

Table 3: Security Consultant Role

| Role | Manager/Communication Specialist | Training Specialist | Forensic Analyst |
|---|---|---|---|
| **Basic Role** | Alerts and Warnings | Artifact and Risk Analysis | Support |
| **Shared Role** | Security Consultant | Security Consultant | Security Consultant |

Sharing threat intelligence is essential for monitoring changes in the threat landscape and predicting major cyber threats. The three primary roles—Risk Analysis, Alerts and Warnings, and Security Consultant—are interconnected and consist of multiple tasks. Achieving these tasks effectively enhances the overall incident response process.

**4.2.1 Risk Analysis Role**

Shared among Incident Responders, Training Specialists, and Forensic Analysts, this role includes:

- Disaster Recovery
- Business Continuity
- Risk Assessment
- Risk Countermeasures

**4.2.2 Alerts and Warnings Role**

Shared among Network Specialists, Threat Specialists, and Communication Specialists, this role includes Developing Training Programs, Awareness Campaigns, Phishing Awareness and Testing

**4.2.3 Security Consultant Role**

Shared among Managers, Training Specialists, and Forensic Analysts, this role includes Incident Assessment, Forensic Analysis, Root Cause Analysis, Continuous Monitoring

**4.3 Logistics Role**

After an incident occurs, responders assess its severity and notify stakeholders through structured steps. Notifications are tailored based on the recipient's role, Internal Recipients: Includes team members, managers, and executives. External Recipients: Includes customers, partners, and regulatory bodies.

**4.3.1 Second: What information could be shared, when and how:**

After responder or incident specialist select the actor who will be informed, notifications that should be transformed must be well prepared and well directed, through which channels and during which time, this information maybe technical like security commands or pieces of code, or general information reflecting impact and cost.

**Technical Details:**

For technical teams, the incident responder provides detailed information about the attack' nature, including indicators of compromise (IOCs), attack vectors, system's parts affected, and potential data breaches.

This helps more of understanding the incident's technical aspects and help more in containment and mitigation efforts, also gives clear and accurate situation for specialists who will take a decision of how to respond to these incidents and from which point they will start.

Technical information is just known by technicians and security specialists.

General Details, for manger/stakeholders or customer, responder send general information (report/notes), clearing potential impacts of cost and time to fixing this incident/s, also reflect them a wide picture of efforts and activities that technical team maybe apply, and the next planed steps.

For that, CISO or Team leader plays the role of coordinator and facilitator between IR team and Stakeholders.

**4.3.2 actions might be happened/avoid:**

Cybercrime is an emerging form of transnational crime, and it is one of the fastest-growing areas of crime. contends that cybercrimes, such as confidentiality or privacy data breaches, could lead to the

theft of personal data from millions of people across the globe. states that the cost and consequences of data breaches vary between the theft of personal information to trade secrets among others, with some companies facing additional problems such as customer retention issues following a data breach. [2]

## 5.0 RELATED WORK

The proposed roles distribution model for a Computer Security Incident Response Team (CSIRT) builds upon existing research and frameworks in the field of cybersecurity incident response. This section reviews relevant studies that have explored CSIRT structures, role definitions, and methodologies for enhancing incident response efficiency.

1. CSIRT Development and Evolution: Ruefle et al. (2014) provide an in-depth analysis of the development and evolution of CSIRTs over time. Their work highlights the importance of structured roles and responsibilities within teams to ensure effective incident handling. This aligns with the current study's focus on defining clear roles for risk analysis, alerts and warnings, and security consulting.[13]
2. Role Distribution and Coordination: Bhaskar (2005) proposes an integrated framework for coordinating CSIRT activities. His research emphasizes the need for a balanced distribution of tasks among team members to avoid redundancy and ensure accountability. The current study extends this idea by introducing shared roles to enhance flexibility and adaptability.[11]
3. Security Incident Management: Goundar (2021) introduces foundational concepts related to security incidents and responses against cyberattacks. His work underscores the importance of proactive measures such as risk analysis and reactive measures like incident assessment, both of which are central to the proposed roles distribution model.[12]
4. Key Persons and Role Allocation: Botirov et al. (2021) identify key individuals involved in the information security incident management process and propose methods for distributing roles between them. Their findings support the inclusion of shared responsibilities in the current model to ensure seamless collaboration during incident response operations.[14]

By synthesizing insights from these studies, the proposed roles distribution model offers a comprehensive approach to organizing CSIRTs. It integrates theoretical foundations, practical considerations, and ethical guidelines to create a robust framework for modern incident response teams.

## 6.0 CONCLUSION

This paper proposes a model for distributing roles within a CSIRT, focusing on three primary roles: Risk Analysis, Alerts and Warnings, and Security Consultant. These roles are designed to be flexible and scalable, ensuring adaptability across organizations of varying sizes. By clarifying responsibilities and promoting collaboration, the model enhances the effectiveness of incident response teams.

## REFERENCES


[1] Nyre-Yu, M., Gutzwiller, R.S. and Caldwell, B.S. (2019) 'Observing cyber security incident response: Qualitative themes from field research', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), pp. 437–441. doi:10.1177/1071181319631016.

[2] Nyre-Yu, M., Gutzwiller, R.S. and Caldwell, B.S. (2019) 'Observing cyber security incident response: Qualitative themes from field research', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), pp. 437–441. doi:10.1177/1071181319631016.

[3] Angafor, GN, Yevseyeva, I, He, Y. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy. 2020; 3:e126. https://doi.org/10.1002/spy2.126Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Villegas-Ch., W.; Ortiz-Garces, I.; Sánchez-Viteri, S.Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. Computers 2021, 10, 102. ttps://doi.org/10.3390/computers10080102

[5] Retnowardhani, A., Diputra, R.H. and Triana, Y.S. (2019) 'Security Risk Analysis of bring your own device system in manufacturing company at Tangerang', TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(2), p. 753. doi:10.12928/telkomnika.v17i2.10165.

[6] Nasser, M., Ahmad, R., Yassin, W., Hassan, A., Zainal, Z., Salih, N., & Hameed, K. (2018). Cyber-security incidents: A review cases in Cyber-Physical Systems. International Journal of Advanced Computer Science and Applications, 9(1).
[7] Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. Elektrotechnik Und Informationstechnik, 132(2), 106–112. https://doi.org/10.1007/s00502-015-0289-2
[8] Bhardwaj, A., & Sapra, V. (Eds.). (2021). Security Incidents & Response Against Cyber Attacks. Springer International Publishing.
[9] Austin, G. (2020). Cyber security education: Principles and policies. Routledge Studies in Conflict, Security and Technology.
[10] Nyre-Yu, M., Gutzwiller, R.S., Caldwell, B.S. (2019). Observing Cyber Security Incident Response: Qualitative Themes from Field Research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting , 63(1), pp. 437–441.
[11] Bhaskar, R. (2005). A Proposed Integrated Framework for Coordinating Computer Security Incident Response Team. Journal of Information Privacy and Security .
[12] Goundar, S. (2021). Introduction to Security Incidents and Response Against Cyber Attacks. EAI/Springer Innovations in Communication and Computing .
[13] Ruefle, R., et al. (2014). Computer Security Incident Response Team Development and Evolution. IEEE Security & Privacy .
[14] Botirov, F., et al. (2021). Identification of Key Persons in the Information Security Incident Management Process and Distribution of Roles Between Them. Tehnika Fanlari Va Innovaciâ .