Proposed Roles Distribution model for a Computer System Incident Response Team (CSIRT)

Hosamaldeen Hamd
Assistant Professor, Department of Computer Science and Information
Gulf Colleges for Humanities and Administrative Sciences, KSA

ABSTRACT
The process of responding to cyber incidents require professional skills and standard methods, incident's responder find themselves facing a problem of determining who is responsible to act with the accidents, the consistent between incidents response team heavily required, first to eradicate and fix the incident and/or second, to save time and efforts, in this paper, roles of incident response team were distributed and assigned between the team members, everyone in the team defined his basic and shared role between himself and the other team members, three main roles has been assigned and determined as a comprehensive roles for any response team size which are(risk analysis, alert and warnings, and security consultant)roles.

Keywords
Incident, IR incident response, CSIRT, roles

1. INTRODUCTION
The digital transformation of our lives, our work and our social activities is likely to results in more incidents and attacks, there for, preparing, planning, and mitigating security incidents and response to the cyberattack must become part on an organization and every individual' daily routine in the "new normal".[8]

one of the most important steps in our risk management plan in the organizations, and considered critical, is the preparation of incident response team, its member role, is to deal and operate with varieties of attacks and system compromises actions which may be happened internally or externally, incidents response plan depends on the methods of roles' distribution between team members and describes them how to responds effectively to incidents.

Member's roles interconnected each other and sometimes shared the same role, for that, they need to following clear road map to determining and differentiating between roles or to do same roles according to the needs.

Incident response team have a logistics role also, not just the professional things, they are also responsible of writing reports and notes to stakeholders and others, who connected the information system/organization network, while specialists and professionals works on incidents, team leader and communication specialist work on sending reports and notifications to non-technical.

2. INCIDENTS AND INCIDENTS RESPOND TEAM
2.1 Incident in cyber
According to Rosencrance (2019) "security incidents are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed [8].

So, incidents are any events that compromised the CIA' goals of security.

2.2 Incidents makers
Incidents intentionally or unintentionally happens, anyhow, there are different actors who doing these incidents, maybe system users, employees, clients, and hackers play this role, all of them considered human' actions affect the system architecture or content, AI and experts' system also makes incidents sometimes, in the following, author discuss the human side to represent how CSIRT affected by their actions.

2.3 Incident Categories
Incidents generally separated into different types, and the targeted victim of attack affect more of categorizing incidents, here are main categories of incidents according to [6] as follow:

- **Cyberwarfare (CW):** "using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability".
- **Hacktivism (H):** "is the convergence of the hacking process and activism where hacking refers to the operations that exploit computers in ways that are unusual or often illegal, normally with the help of certain software".
- **Cyber Espionage (CE):** is the arm of the corporate high-tech crime. It mainly involves attacks on companies and institutions and not individuals. Cyber espionage does not always necessarily occur on a large scale.

Cyber Crime (CC): Involves all criminal act which deals with the networks and computers (hacking). Additionally, traditional crimes that are conducted

2.4 Computer Security Incident Response (CSIR)
Computer Security Incident Response (CSIR) is based on the need for a functioning team of *professional* cybersecurity analysts to respond to cyber threats and handle their aftermath [1]

2.5 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. 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. 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.

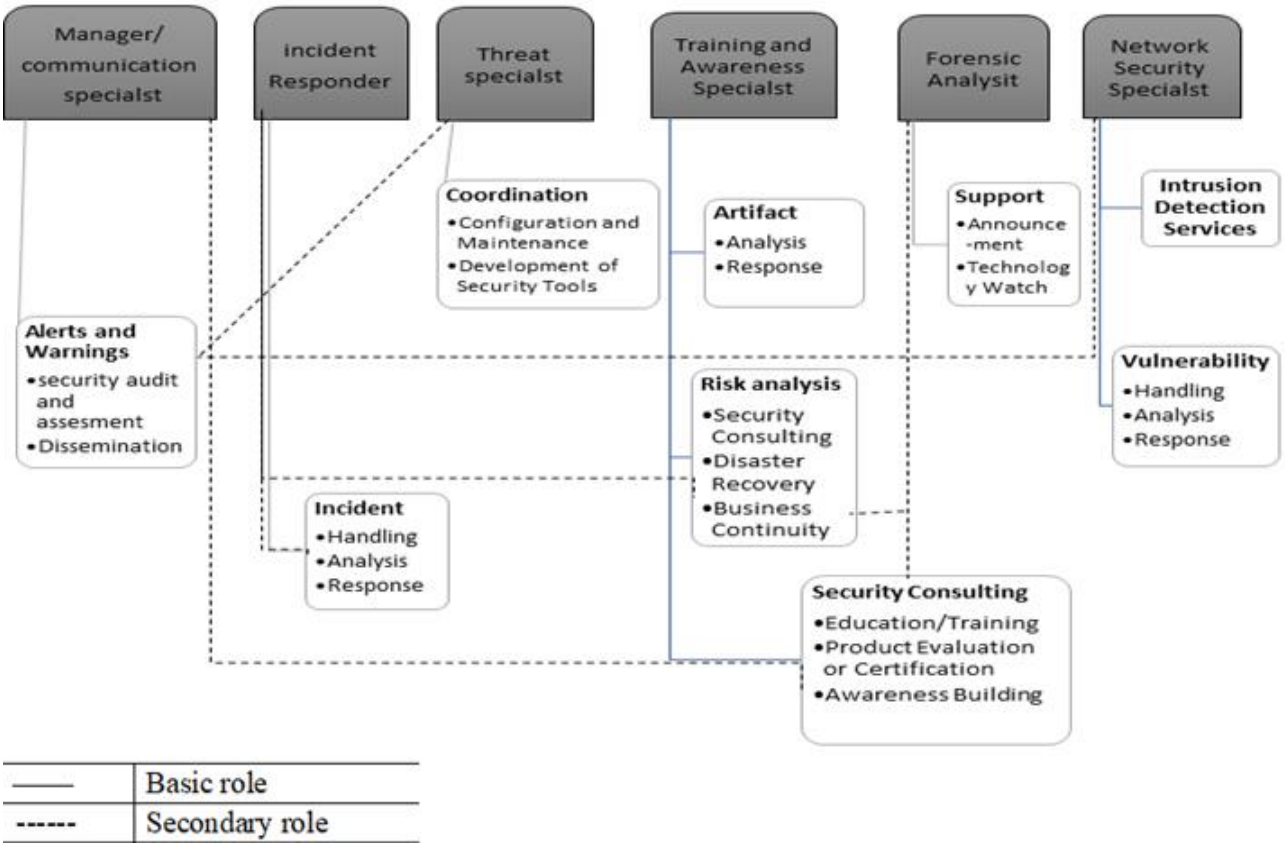

Figure 1proposed model of CSIRT roles distribution

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.

Table 1 risk analysis role

	Incident responder	**Training specialist**	**Forensic analyst**
Basic role	**Incident (handling, analysis, and response)**	**Artifact and Risk analysis**	**Support**
Shared role	***Risk analysis***		

Table 2 alerts and warnings role

	Network specialist	**Threat specialist**	**Manager communication specialist**
Basic role	**Vuln (handling, analysis, and response) + intrusion detection**	**Coordination**	**Alerts and warnings**
Shared role	***Alerts and warnings***		

Table 3 security consultant role

	Manger or communication specialist	Training specialist	Forensic analyst
Basic role	**Alerts and warnings**	**Artifact and Risk analysis**	**Support**
Shared role	***Security consultant***		

4.2 Role's Distribution Result Discussion:

Sharing threat intelligence can be instrumental for monitoring changes in the threat landscape and predicting major cyber threats that might have a disruptive. [7]

According to above three tables it is clear that there are many roles and responsibilities shared between job's positions, which comes basically divided into three basic roles (Risk Analysis, Alerts and Warnings and Security Consultant), each role of these three, consists of a number of jobs and tasks that CSIRT must be applied, achieving these tasks properly will affects whole role positively and then enhance the complete process of responding to incidents.

As well as these three roles consist of more than these mentioned tasks written in figure no (1), but these are the most important.

4.2.1 Risk Analysis role shared between Incident Responder, Training and Awareness Specialist and Forensic Specialist behind their basic roles also, this role includes different tasks and also required different well understanding functions as described below:

- **Disaster recovery**
- **Security consultant**
- **Business continuity**
- **Risk assessment**
- **Risk countermeasure**
- **…**

4.2.2 Training and Awareness role also shared between Network, Threat and Manager communication **specialist, and** this role includes too many tasks as the following:

- **Developing training programs.**
- **Awareness campaigns.**
- **Customize training material.**
- **Security policy compliance.**
- **Phishing awareness and testing.**
- **Etc.**

4.2.3 Security Consultant role also shared between manager and communications, training and forensic specialists, and it has too many functions as follow:

- **Incidents assessment**
- **Forensic analysis**
- **Incident containment and eradication**
- **Root cause analysis**
- **Incident documentation**
- **Continuous monitoring**
- **Etc.**

4.3 Logistics Role:

After incident occurred, responder assess and classify the nature of severity, begins to notify others (stakeholders and incident team) following structured steps and determine people's receivers, and messages content to be sent, and differentiate between the following:

4.3.1 First: Who must be informed:

According to incident's nature, responder will determine to whom alerts or reports must be sent, because there are many classes of users, some of them have a direct responsibility of computer system, and others haven't (See figure 1), and recipients basically can be divided into two main classes as follow:

- **Internal recipients**:

The incident responder informs internal stakeholders, team members, managers, and executives about the incident's nature and impact, because those are considered as an internal community who responsible of dealing with accidents and affected by its impact.

This notification may involve creating an incident report or sending out an initial alert to gather the relevant team members.

- **External recipients**:

If the incident has legal or regulatory implications, involves customers or partners, or could affect the organization's reputation, the incident responder might need to communicate externally. This communication should be coordinated carefully to avoid misinformation or panic.

4.3.2 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.

4.3.3. **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. RELATED WORK:

In [7] authors make distinguish between two types which are, first, Computer Security Incident Response Teams (CSIRT) at public and private organizations, and second, Security Intelligence and Coordination Centre (SICC) for society, and discuss what information needs to be shared and how this can be done using the dominant threat intelligence sharing standards, also we showed that it is possible to leverage from threat intelligence sharing infrastructures to gain early insight into the large scale effects of cyber threats and incidents.

6. CONCLUSION

In this paper roles of CSIRT's are distributed into three main categories (risk analysis, alert and warning, and security consultant) which considered the main roles that must be effectively achieved by incidents response actors if incidents occurred. These three main roles consist of variety and many roles which required skills and expert. Also, one actor can apply number of missions at the same time to avoid or fix attacks side by side with others in the team.

7. 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.