An Incident Response (IR) Team

Mohith Naga Adithya Vasamsetti

MXV00070@UCMO.EDU

University of Central Missouri,

Lee's Summit

Abstract:

In the current digital environment, organizations encounter increased dangers of information security breaches, highlighting the importance of efficient incident response (IR) systems. Although technical factors are important, there is an increasing understanding of the importance of including wider socio-organizational views in information retrieval procedures. This paper is focused on filling this void by studying organizational challenges impacting incident management teams and suggesting ways to improve their performance. This paper aims to offer insights for creating better strategies to address disruptions by examining the role of IR teams in the larger organizational context and highlighting the importance of informal learning processes. Organizations can enhance their IR teams' ability to decrease security risks and safeguard critical assets by understanding how formal protocols and informal practices interact.

I - INTRODUCTION

In today's digital environment, the risk of information security attacks is high for organizations of all sizes and initiatives. To effectively combat these threats, many organizations have a dedicated IR function. The IR process includes several critical steps: preparation, detection, containment, containment, and incident recovery. At the forefront of this defence is the Incident Response Team (IRT), whose mission is to minimize the impact of security breaches and ensure successful recovery. IRT's are like modern-day "firefighters" and use specific skills and strategies. quickly respond to intrusions and security incidents.

While much of the existing disaster response literature emphasizes technical considerations and best practices, there is growing recognition of the need to consider broader socio-organizational perspectives. However, there is still relatively little research in this area, particularly in relation to the interface between IRTs and the wider organizational environment, particularly in the decision-making process. Effective incident response goes beyond technical expertise. it requires a comprehensive understanding of organizational dynamics and learning mechanisms. Formal methodologies, provide a structural framework for handling cases, but must be complemented by informal learning practices embedded in organizational culture. This synthesis of formal and informal learning is essential to maximize actual response effectiveness.

This paper aims to address this gap in the literature by examining organizational issues affecting incident

management teams and proposing solutions to improve their effectiveness. Using a combination of theoretical frameworks and empirical evidence, we explore the role of IRTs in a wider organizational context and emphasize the importance of informal learning processes in optimizing disruption response capacity. By considering the dynamics of organizational learning, we aim to provide insights that help develop more effective strategies for responding to disruption. By recognizing the interplay between formal protocols and informal practices, organizations can better equip their IRTs to reduce security risks and protect critical assets in an increasingly complex threat environment.

II - BACKGROUND REPORT

Incident Response (IR) teams are crucial in maintaining the security posture of organizations by promptly addressing security incidents and minimizing their impact. Their expertise and swift action are essential in mitigating risks and safeguarding sensitive information and systems from potential threats. An IR Team alludes to the methods laid down by an organization to all its representatives, coordinating their course of activity in all circumstances related to information judgment, at whatever point in the line of obligation.

The overwhelming portion of data breaches inside the organizations are consequence of human on-screen characters and keeping in intellect that cybersecurity arrangements are ordinary among the organizations. Developing these arrangements or rules are at that point made aware to all workers, depending on the sort of information they handle. Awareness is ordinarily taken after by a consistent examination of compliance.

2.1 Roles in IR team:

- Executive Sponsor
- Incident Response Coordinator
- Technical Lead
- Forensic Analyst
- IT Administrator
- Communication Lead
- Legal Counsel
- Human Resources Representative
- External Partners
- Supporting Roles

2.2 Stages in IR Team plan: -

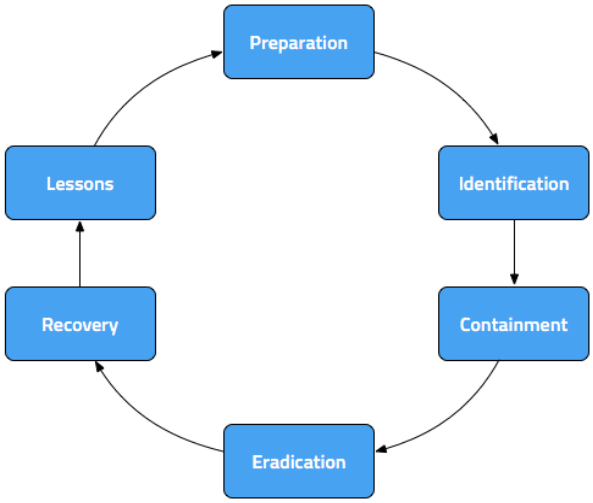

Fig.1 Six phases of plan

2.3 Drawbacks in IR Team: -

- **Limited Resources:**
  Incident response teams often don't have enough people, tools, or money to handle every issue effectively.
- **Skills Gap:**
  Sometimes, the team might not have the right expertise to deal with certain types of problems, making it hard to respond properly.

- **Slow Detection and Response:**
  It can take a while to notice when something's wrong, which means damage can get worse before it's fixed.
- **Communication Problems:**
  Teams need to talk to each other and sometimes outside groups like the police or other companies. If communication isn't good, it slows everything down.
- **Following Rules:**
  There are often rules and laws about how incidents need to be handled, and it's easy to mess up if you don't know them well.
- **Keeping Records:**
  It's important to write down what happened during an incident and what was done to fix it, but sometimes this gets forgotten or done poorly.
- **Stopping the Problem:**
  After finding an issue, it's not always easy to stop it from spreading.
- **Learning from Mistakes:**
  After an incident is over, it's crucial to figure out what went wrong and how to avoid it in the future, but this step can be overlooked.

2.4 Precautions that can improve IR team strength: -

- **Regular Training and Skill Development:**
  Keep the team up to date with the latest threats, technologies, and response techniques through regular training sessions and skill development programs.
- **Mock Drills and Simulations:**
  Conduct regular tabletop exercises and simulations to test the team's response capabilities and identify areas for improvement.
- **Clear Roles and Responsibilities:**
  Define clear roles and responsibilities for each team member during incident response to ensure efficient coordination and execution of tasks.
- **Continuous Monitoring and Detection:**
  Implement robust monitoring solutions and regularly review logs and alerts to detect security incidents at the earliest possible stage.
- **Effective Communication Channels:**
  Establish clear communication channels and protocols for sharing information within the team and with external stakeholders during incident response.
- **Documentation and Knowledge Sharing:**
  Maintain comprehensive documentation of incident response procedures, lessons learned, and best practices to facilitate knowledge sharing and continuous improvement.
- **Cross-Functional Collaboration:**
  Foster collaboration between the incident response team and other departments, such as IT, legal, and management, to ensure a holistic approach to incident management.
- **Regular Review and Updates:**
  Periodically review and update incident response plans,

procedures, and technologies to adapt to evolving threats and organizational changes.

- **Vendor and Partner Coordination:**

  Establish relationships with external vendors and partners for specialized support and coordination during incident response, such as forensic analysis.

- **Post-Incident Analysis and Learning:**

  Conduct thorough post-incident analysis to identify root causes, lessons learned, and areas for improvement, and incorporate these insights into future incident response efforts.

2.5 Can these precautions improve the IR Team strength?

Implementing a thorough set of precautions significantly strengthens an incident response team. These measures include ongoing training, practice drills, clear roles, and continuous monitoring. Effective communication, documentation, and collaboration with other departments are also crucial.

Regular updates to response plans and learning from past incidents further enhance the team's capabilities. By following these precautions, the team becomes better prepared to detect and respond to security threats, ensuring the organization's safety and resilience.

III - CONCLUSION

Ultimately, a comprehensive approach that extends beyond just technical skills is needed for successful incident response in the modern digital landscape. This paper emphasized the significance of considering wider socio-organizational viewpoints to improve the efficiency of Incident Response Teams (IRTs). This research addresses a significant gap in the current body of literature by studying organizational problems impacting IRTs and suggesting potential solutions. The results emphasize the importance of comprehending organizational dynamics and promoting informal learning practices among IRTs. While formal methodologies offer a structural framework for managing incidents, they need to be supported by informal learning that is ingrained in the culture of the organization. This combination is crucial for optimizing the real response efficiency of IRTs.

Important suggestions involve defining roles and responsibilities clearly in the team, providing regular training and development of skills, ensuring effective communication channels, and encouraging cross-functional collaboration. Furthermore, it is crucial to consistently monitor, document, and analyse incidents after they occur in order to learn from them and enhance future response tactics. By putting these measures in place, companies can greatly improve the effectiveness and durability of their incident response teams. These actions not only enhance the team's capacity to quickly identify and address security incidents but also foster a culture of ongoing growth and education in the organization.

Essentially, incident response is a dynamic and collaborative process that necessitates a thorough comprehension of technical and organizational elements. By acknowledging the relationship between official procedures and unofficial habits, organizations can empower their IR teams to effectively safeguard critical assets

amidst the intricacies of today's threat landscape. It is crucial for organizations to focus on investing in technical resources and organizational development initiatives to enhance incident response capabilities going forward. By adopting this comprehensive strategy and promoting a work environment that emphasizes teamwork and ongoing education, companies can actively reduce security vulnerabilities and strengthen their ability to withstand new challenges in a constantly changing online environment.

REFERENCES

1. Atif Ahmad, Justin Hadgkiss, A.B. Ruighaver,Incident response teams – Challenges in supporting the organisational security function,Computers & Security,Volume 31, Issue 5,2012,Pages 643-652,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2012.04.001.
2. Shedden, Piya; Ahmad, Atif; and Ruighaver, Anthonie B., "Informal Learning in Security Incident Response Teams" (2011). ACIS 2011 Proceedings. 37.
3. https://aisel.aisnet.org/acis2011/37
4. Miora, Michael & Kabay, M. & Cowens, Bernie. (2015). Computer Security Incident Response Teams. 10.1002/9781118820650.ch56.
5. Brown, J. M., Greenspan, S., & Biddle, R. (2016). Incident response teams in IT operations centers: the T-TOCs model of team functionality. Cognition, Technology & Work, 18(4), 695–716. doi:10.1007/s10111-016-0374-2
6. Karabulut, Yunus & Boylu, Gulistan & Kucuksille, Ecir Ugur & Yalçınkaya, Mehmet. (2015). Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey. Balkan Journal of Electrical and Computer Engineering. 3. 10.17694/bajece.93521.
7. van der Kleij, Rick & Kleinhuis, Geert & Young, Heather. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. Frontiers in Psychology. 8. 10.3389/fpsyg.2017.02179.
8. Lockhart, Charlotte & Woods, Kevin. (2016). Exploring the development of critical incident response teams. International Journal of School & Educational Psychology. 5. 1-12. 10.1080/21683603.2016.1234987.
9. Ruefle, Robin & Dorofee, Audrey & Mundie, David & Householder, Allen & Murray, Michael & Perl, Samuel. (2014). Computer Security Incident Response Team Development and Evolution. Security & Privacy, IEEE. 12. 16-26. 10.1109/MSP.2014.89.
10. Steinke, Julie & Alaybek, Balca & Fletcher, Laura & Wang, Vicki & Tomassetti, Alan & Repchick, Kristin & Zaccaro, Stephen & Dalal, Reeshad & Tetrick, Lois. (2015). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. IEEE Security & Privacy. 13. 20-29. 10.1109/MSP.2015.71.
11. Ahmad, Atif & Ruighaver, Anthonie & Teo, W.T.. (2005). An Information-Centric Approach to Data Security in Organizations. 1 - 5. 10.1109/TENCON.2005.301322.
12. Siponen, Mikko. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. Information and Organization. 15. 339-375. 10.1016/j.infoandorg.2004.11.001.
13. Werlinger, Rodrigo & Muldner, Kasia & Hawkey, Kirstie & Beznosov, Konstantin. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response.

Inf. Manag. Comput. Security. 18. 26-42. 10.1108/09685221011035241.

14. M. Ioannou, E. Stavrou and M. Bada, "Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 2019, pp. 1-4, doi: 10.1109/CyberSecPODS.2019.8885240. keywords: {Computer security;Organizations;Training;Information management;Teamwork;cybersecurity;culture;CSIRT;incident management;communication;cooperation},
15. Reed, T., Abbott, R. G., Anderson, B., Nauer, K., & Forsythe, C. (2014). Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58(1), 427-431. https://doi.org/10.1177/1541931214581089
16. M. Jezreel, M. Mirna and U. Edgar, "Services establishment in the computer security incident response teams: A review of state of art," 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, 2015, pp. 1-6, doi: 10.1109/CISTI.2015.7170502. keywords: {Computer security;Internet;Business;Systematics;ARPANET;Uniform resource locators;Systematic Review;CSIRT;Services},