Nexus Global Research Journal of Multidisciplinary
Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Research Article

Development of Web-Based Learning Resource Cybersecurity Incident Response Playbook for the City Schools Division of Urdaneta

Hajie A. Rosario [1*], Dr. Diosdado C. Caronongan [2]

[1] *Graduate School, University of Luzon, Master in Information Technology Program, Department of Education, Schools Division Office of Urdaneta City.*
[2] *University of Luzon, College of Computer Studies.*

ABSTRACT:
The primary goal of this study is to develop and evaluate a Cybersecurity Incident Response (IR) Playbook for web-based learning resources maintained by the City Schools Division of Urdaneta, rather than to conduct a simple assessment of existing cybersecurity practices. Specifically, the study sought to identify the challenges encountered in current cybersecurity incident response (IR) practices, develop a standardized IR Playbook tailored for Google Sites and WordPress platforms, and evaluate its usability and user acceptance among intended users. A Design and Development Research (DDR) approach, supported by descriptive research methods, was employed. Data were gathered from seventeen (17) respondents consisting of Learning Resource Personnel, Division ICT Personnel, Administrative Staff, and ICT Coordinators through researcher-made questionnaires, semi-structured interviews, and document analysis. Findings revealed that respondents encountered serious challenges in incident detection and reporting, incident response and containment, and recovery, documentation, and post-incident evaluation due to the absence of standardized procedures, inconsistent reporting mechanisms, unclear roles, and inadequate documentation. Guided by these findings and anchored on the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27035, and relevant Philippine cybersecurity laws and DepEd ICT policies, a comprehensive Cybersecurity Incident Response Playbook was developed. The playbook includes standardized procedures, reporting workflows, recovery guidelines, documentation templates, platform-specific response procedures for Google Sites and WordPress, and post-incident evaluation forms. Evaluation results showed that the developed playbook achieved a Highly Acceptable usability rating (WM = 3.47) and a Strongly Agree user acceptance rating (WM = 3.47), indicating that it is practical, comprehensive, and suitable for adoption within the SDO. The study concludes that implementing the developed playbook can strengthen cybersecurity governance, standardize incident handling, and improve the protection and resilience of web-based learning resources.

Keywords: Cybersecurity Incident Response Playbook, Web-Based Learning Resources, Google Sites, WordPress

Citation: Rosario, H. A., & Caronongan, D. C. (2026). Development of web-based learning resource cybersecurity incident response playbook for the City Schools Division of Urdaneta. Nexus Global Research Journal of Multidisciplinary, 2(8), 417–433.

INTRODUCTION:

The increasing adoption of digital technologies in basic education has transformed the way educational institutions develop, manage, and disseminate learning resources. In the Philippines, the Department of Education (DepEd) has strengthened the integration of Information and Communication Technology (ICT) through initiatives such as the Basic Education Learning Continuity Plan and the Digital Rise Program, encouraging schools and Schools Division Offices (SDOs) to utilize web-based platforms to support teaching, learning, and administrative operations (DepEd, 2020; DepEd, 2021). In the Schools Division Office of Urdaneta City, Google Sites and WordPress have become essential platforms for hosting learning resources, instructional materials, and school-related information.

Despite their benefits, these web-based platforms are increasingly exposed to cybersecurity threats, including unauthorized login attempts, website defacement, broken website links, malware

***Corresponding Author:** Hajie A. Rosario, Email: hajie.rosario@deped.gov.ph
Received: 08 July 2026 | **Accepted:** 01 Aug 2026 | **Published:** 15 Aug 2026
Copyright © 2026 The Author(s): This work is licensed under a Creative Commons Attribution- Non-Commercial-No Derivatives 4.0 (CC BY-NC-ND 4.0) International License

infections, phishing attacks, and content manipulation. Based on the operational experiences of the Schools Division Office of Urdaneta City, incidents such as unauthorized login attempts and broken website links have been encountered and addressed through existing ICT operational procedures. However, incident handling primarily relied on manual coordination, email exchanges, messaging applications, and the technical experience of ICT personnel. The absence of a dedicated and standardized Cybersecurity Incident Response (IR) Playbook resulted in inconsistent incident reporting, response, documentation, recovery, and post-incident evaluation across offices and schools.

International cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and ISO/IEC 27035, emphasize that organizations should implement standardized incident response procedures to minimize operational disruption, strengthen organizational resilience, and continuously improve cybersecurity capabilities (NIST, 2024; ISO, 2018). Likewise, previous studies have shown that educational institutions commonly experience challenges related to limited cybersecurity awareness, inconsistent reporting procedures, inadequate documentation, and unclear response responsibilities, highlighting the need for structured incident response guidance (Kumar et al., 2024).

In response to these challenges, this study focused on the development and evaluation of a Cybersecurity Incident Response (IR) Playbook specifically designed for Google Sites and WordPress-based learning resources maintained by the Schools Division Office of Urdaneta City. The study sought to identify the challenges encountered in the implementation of cybersecurity incident response practices in terms of (1) incident detection and reporting mechanisms, (2) incident response and containment procedures, and (3) recovery, documentation, and post-incident evaluation. The identified challenges served as the basis for developing a standardized Cybersecurity Incident Response Playbook tailored to the operational needs of the division. Furthermore, the developed playbook was evaluated by its intended users in terms of usability and user acceptance to determine its suitability as a standardized operational guide.

The findings of this study are expected to contribute to the enhancement of cybersecurity governance within the Schools Division Office of Urdaneta City by providing a practical, standardized, and user-validated Cybersecurity Incident Response Playbook. The developed playbook may benefit Learning Resource Personnel, Division ICT Personnel, Administrative Staff, ICT Coordinators, Web Portal Administrators, and other educational institutions seeking to strengthen the security posture of their web-based learning resources through consistent and effective cybersecurity incident response practices.

Statement of the Problem

This study aimed to develop and evaluate a Cybersecurity Incident Response (IR) Playbook for the web-based learning resources of the Schools Division Office of Urdaneta City.

Specifically, it sought to answer the following questions:

1. What challenges/issues are concerns in the implementation of cybersecurity IR Practices along:
    a) incident detection and reporting mechanisms;
    b) incident response and containment procedures; and
    c) recovery, documentation, and post-incident evaluation?
2. What cybersecurity IR playbook can be developed to enhance the system security posture based on the identified challenges?
3. What is the level of usability and user acceptance of the proposed playbook among the target users?

Significance of the Study

This study is significant because it provides a standardized and user-validated Cybersecurity Incident Response Playbook that can strengthen cybersecurity management for web-based learning resources within the Schools Division Office of Urdaneta City. The findings and developed

playbook may serve as a practical reference for Learning Resource Personnel, Division ICT Personnel, Administrative Staff, ICT Coordinators, and Web Portal Administrators by establishing consistent procedures for incident detection, reporting, response, containment, recovery, documentation, and post-incident evaluation.

The study may also benefit school administrators by supporting cybersecurity governance and improving organizational preparedness against cyber threats. IT professionals and cybersecurity practitioners may utilize the playbook as a reference for developing incident response procedures tailored to educational institutions and similar public-sector organizations. Likewise, DepEd policymakers and ICT managers may use the findings to enhance cybersecurity policies, operational guidelines, and capacity-building initiatives for schools and division offices.

Finally, the study contributes to the existing body of knowledge on cybersecurity incident response in the Philippine education sector and may serve as a valuable reference for future researchers conducting studies on cybersecurity governance, incident response management, digital learning environments, and educational information security.

MATERIALS AND METHODS:

Research Design

This study employed a descriptive research design combined with elements of design science research to assess the current implementation of Cybersecurity Incident Response (IR) Playbook in learning resources developed using Google Sites and WordPress.

Descriptive research design was utilized to systematically gather information about the existing cybersecurity practices within the City Schools Division of Urdaneta. According to research methodology principles, descriptive research is appropriate when the goal is to determine the current conditions, practices, or perceptions of respondents regarding a particular phenomenon. In this study, descriptive research was used to evaluate the extent of implementation of cybersecurity practices in terms of incident detection, reporting, response, containment, and recovery procedures.

In addition, the study incorporated elements of design science research, which focuses on developing practical solutions to real-world problems through the design and evaluation of systems or frameworks. Through this approach, the researcher analyzed the findings from the survey data and used them as a basis for designing a Cybersecurity Incident Response Playbook System tailored to the needs of the City Schools Division of Urdaneta.

By combining descriptive analysis and system design, the research not only assessed the current cybersecurity preparedness of the division but also proposed a structured solution to address identified challenges.

System Development and Methodology

The development of the proposed Cybersecurity Incident Response Playbook System followed an Agile-inspired system development methodology. Agile methodology emphasizes iterative development, flexibility, and continuous improvement through stakeholder feedback.

The Agile approach was selected because cybersecurity management requires continuous adaptation to emerging threats and evolving technologies. The methodology includes several stages that guide the design and development of the proposed incident response system.

1. **Planning Phase**

   In this phase, the researcher identified the need for a structured Cybersecurity Incident Response Playbook for the learning resources of the City Schools Division of Urdaneta. Initial consultations were conducted with ICT personnel and educators to determine existing practices and identify potential cybersecurity challenges in managing Google Sites and WordPress platforms.

   Relevant policies, cybersecurity frameworks, and previous research studies were also reviewed to establish the theoretical foundation for the system.

2. Requirement Analysis Phase

The researcher analyzed the collected information to determine the system requirements needed to support the implementation of the Cybersecurity IR Playbook system. This phase involved identifying essential features such as incident detection procedures, reporting mechanisms, response protocols, containment actions, recovery strategies, and documentation processes.

The requirements were also aligned with recognized cybersecurity frameworks such as the NIST Incident Response Model and ISO 27001 information security management principles.

3. System Design Phase

During the design phase, the researcher developed the conceptual structure of the proposed system. This included designing the system architecture, incident response workflow, incident response playbook matrix, and security governance structure.

These design components define how cybersecurity incidents will be detected, reported, managed, and documented within the division's learning resource platforms.

4. Evaluation and Validation Phase

The developed system design was evaluated based on the responses gathered from the respondents and the identified cybersecurity challenges. The evaluation focused on determining whether the IR Playbook system addresses the current gaps in incident response practices within the City Schools Division of Urdaneta.

Feedback from ICT personnel and education stakeholders may also be considered to further refine the proposed system.

Research Respondents

The respondents of this study consisted of selected personnel from the City Schools Division of Urdaneta and its public schools who are directly involved in the management and development of digital learning resources.

The respondents included:

- School ICT Coordinators
- Teachers responsible for developing learning resources
- Division LR Personnel
- Division ICT Personnel

These individuals were selected because they are directly involved in managing, maintaining, or supervising digital learning platforms such as Google Sites and WordPress.

Table 1. Distribution of Respondents According to Position

Position	Frequency	Percentage
Learning Resource Personnel	3	17.65%
Division ICT Personnel	2	11.76%
Administrative Staff	2	11.76%
ICT Coordinators	10	58.83%
Total	**17**	**100%**

Table 1 presents the distribution of respondents according to their positions within the Schools Division Office. Most respondents are ICT Coordinators (58.83%), followed by Learning Resource Personnel (17.65%). Division ICT Personnel and Administrative Staff both represent 11.76% of the total respondents.

The dominance of ICT Coordinators is appropriate for this study since they are directly involved in managing school-based ICT systems, including Google Sites and WordPress platforms. Their insights are highly relevant in assessing cybersecurity incident response practices. Meanwhile, Learning Resource Personnel provide valuable perspectives on content management and digital resource handling. Division ICT Personnel contribute technical and policy-level insights, while Administrative Staff provide operational and support perspectives.

This distribution ensures that the study captures a multi-perspective view of cybersecurity incident response implementation, which strengthens the validity of findings related to the statement of the problems. And it also indicates that the participants possess relevant professional roles and technical responsibilities related to the development, management, and maintenance of digital learning resources. Their participation in the study ensures that the data gathered reflects practical experiences and operational realities regarding cybersecurity practices in the City Schools Division of Urdaneta.

Data Gathering Techniques

The study employed a combination of qualitative and quantitative data-gathering techniques to identify the challenges encountered in the implementation of cybersecurity incident response (IR) practices and to evaluate the usability and user acceptance of the developed Cybersecurity Incident Response (IR) Playbook. The use of multiple data-gathering methods enabled the researcher to obtain comprehensive, reliable, and valid information necessary for the development and evaluation of the proposed cybersecurity solution.

Interview

The primary qualitative data-gathering technique utilized in the study was the semi-structured interview. Interviews were conducted with selected Learning Resource Personnel, Division ICT Personnel, Administrative Staff, and ICT Coordinators of the City Schools Division of Urdaneta. The interview aimed to gather detailed information regarding the current cybersecurity incident response practices implemented within the division and to identify challenges encountered in managing cybersecurity incidents affecting web-based learning resources.

The interview questions were aligned with the first Statement of the Problem, specifically focusing on the following areas:

1. Incident Detection and Reporting Mechanisms;
2. Incident Response and Containment Procedures; and
3. Recovery, Documentation, and Post-Incident Evaluation.

Through the interviews, the respondents were encouraged to share their experiences, observations, and recommendations regarding cybersecurity incident management. The qualitative responses obtained from the interviews served as the basis for identifying existing gaps, weaknesses, and operational challenges that informed the design and development of the Cybersecurity Incident Response Playbook.

Additionally, follow-up interviews were conducted during the evaluation phase to gather respondents' perceptions regarding the usability, practicality, and applicability of the developed playbook. The interview findings were analyzed using thematic analysis to identify common themes and insights that supported the quantitative evaluation results.

Survey Questionnaire

A researcher-made survey questionnaire was utilized as the primary quantitative data-gathering instrument. The questionnaire was designed to collect data regarding the challenges encountered in cybersecurity incident response practices and to evaluate the developed

Cybersecurity Incident Response Playbook.

RESULTS AND DISCUSSIONS:

This section presents the findings, analysis, and interpretation of data gathered in relation to the development and evaluation of Cybersecurity Incident Response (IR) Playbook for Web-Based Learning Resources in the City Schools Division of Urdaneta. The presentation of results is organized according to the Statement of the Problem. Specifically, it discusses the challenges encountered in the implementation of cybersecurity incident response practices, the developed Cybersecurity IR Playbook, and the usability and user acceptance evaluation conducted among the intended users of the developed playbook.

Challenges Encountered in the Implementation of Cybersecurity Incident Response practices

Cybersecurity incident response is widely recognized as a systematic process involving the identification, reporting, response, containment, recovery, documentation, and continuous improvement of cybersecurity incidents. As discussed in Chapter II, the National Institute of Standards and Technology (NIST, 2024) and ISO/IEC 27035 emphasize that effective incident response requires standardized procedures, clearly defined roles, and consistent documentation to minimize operational disruption and improve organizational resilience. Likewise, previous studies by Kumar et al. (2024), Ojala (2024), and Andaya (2025) highlighted that educational institutions and government organizations commonly experience challenges due to manual reporting procedures, inconsistent documentation, and the absence of standardized incident response guidelines. These concepts provided the theoretical basis for examining the cybersecurity incident response challenges encountered by the City Schools Division of Urdaneta across the three operational areas investigated in this study.

To determine the identified challenges in implementing Cybersecurity Incident Response practices, respondents were asked to rate several indicators using a four-point Likert scale.

Scale	Range	Interpretation
4	3.26 – 4.00	Very Serious Challenge
3	2.51 – 3.25	Serious Challenge
2	1.76 – 2.50	Moderate Challenge
1	1.00 – 1.75	Not a Challenge

Incident Detection and Reporting Mechanisms

Incident detection and reporting constitute the first phase of the cybersecurity incident response lifecycle. As discussed in the conceptual literature in Chapter II, NIST (2024) emphasized that timely identification and reporting of cybersecurity incidents significantly reduce response time and organizational impact. Similarly, the research literature synthesized and showed that educational institutions frequently encounter delayed reporting, inconsistent documentation, and dependence on informal communication channels, resulting in inefficient incident management (Ojala, 2024; Kumar et al., 2024; Sepillo, 2024). Guided by these concepts, this section assesses the challenges encountered by the respondents regarding the detection and reporting of cybersecurity incidents affecting the web-based learning resources of the City Schools Division of Urdaneta.

Table 2. Challenges Encountered in Incident Detection and Reporting Mechanisms

Indicator	4	3	2	1	Weighted Mean	Interpretation
Lack of clear procedures for detecting cybersecurity incidents	8	6	2	1	3.26	Very Serious Challenge
Limited awareness in identifying cybersecurity threats	7	6	3	1	3.12	Serious Challenge
Absence of standardized incident reporting process	9	5	2	1	3.29	Very Serious Challenge
Difficulty in documenting incidents consistently	6	7	3	1	3.06	Serious Challenge
Delayed reporting of cybersecurity incidents	6	7	3	1	3.06	Serious Challenge
Overall Mean					**3.15**	**Serious Challenge**

Table 2 shows the challenges encountered in incident detection and reporting mechanisms. The highest-rated challenge was the absence of a standardized incident reporting process, which obtained a weighted mean of 3.29 and was interpreted as a Very Serious Challenge. This finding indicates that respondents experience difficulty in consistently reporting cybersecurity incidents due to the lack of formal procedures.

The lack of clear procedures for detecting cybersecurity incidents obtained a weighted mean of 3.26, also interpreted as a Very Serious Challenge. This suggests that personnel are often uncertain about how to identify and classify cybersecurity incidents affecting web-based learning resources.

The overall mean of 3.15 indicates that incident detection and reporting mechanisms remain a serious concern within the Schools Division Office. The findings emphasize the need for standardized reporting workflows and incident detection guidelines to improve cybersecurity preparedness.

Incident Response and Containment Procedures

Incident response and containment involve the coordinated actions taken after a cybersecurity incident has been detected to prevent further damage and restore operational stability. As discussed in Chapter II, ISO/IEC 27035 and NIST (2024) emphasize the importance of clearly defined responsibilities, standardized response procedures, and effective coordination among personnel. Previous studies also revealed that organizations without documented incident response procedures often experience role ambiguity, inconsistent implementation, and delayed containment activities (Kick, 2022; Nyre-Yu, 2021; Ojala, 2024). These concepts guided the assessment of the challenges encountered by the respondents regarding incident response and containment procedures within the Schools Division Office.

Table 3. Challenges Encountered in Incident Response and Containment Procedures

Indicator	4	3	2	1	Weighted Mean	Interpretation
Lack of defined actions during cybersecurity incidents	8	6	2	1	3.26	Very Serious Challenge
Delayed response of responsible personnel	6	7	3	1	3.06	Serious Challenge
Difficulty in containing cybersecurity incidents	7	6	3	1	3.12	Serious Challenge

Unclear roles and responsibilities	8	6	2	1	3.26	Very Serious Challenge
Ineffective coordination among personnel	6	7	3	1	3.06	Serious Challenge
Overall Mean					**3.14**	**Serious Challenge**

Table 3 presents the challenges encountered in incident response and containment procedures. The lack of defined actions during cybersecurity incidents and unclear roles and responsibilities both received the highest weighted mean of 3.26, indicating Very Serious Challenges.

These findings reveal that personnel lack a formal reference when responding to cybersecurity incidents, resulting in uncertainty regarding responsibilities and response actions. Effective incident response requires clearly documented procedures and role assignments to ensure coordinated actions among stakeholders.

The overall mean of 3.14 suggests that the respondents perceive incident response and containment procedures as a serious challenge. This finding supports the need for a standardized Cybersecurity Incident Response Playbook that clearly defines responsibilities and response workflows.

Recovery, Documentation, and Post-Incident Evaluation

Recovery, documentation, and post-incident evaluation represent the final phase of the incident response lifecycle and are essential for restoring services, documenting incidents, and improving future cybersecurity preparedness. The conceptual literature in Chapter II emphasized that organizations should consistently document incidents, conduct post-incident reviews, and apply lessons learned to strengthen their cybersecurity posture (NIST, 2024; Stallings, 2021). Likewise, the reviewed studies found that many educational institutions continue to experience weaknesses in incident documentation and organizational learning due to the absence of standardized procedures (Andaya, 2025; Sepillo, 2024). Anchored on these concepts, this section examines the challenges encountered by the respondents in relation to recovery, documentation, and post-incident evaluation.

Table 4. Challenges Encountered in Recovery, Documentation, and Post-Incident Evaluation

Indicator	4	3	2	1	Weighted Mean	Interpretation
Difficulty in restoring affected systems	7	6	3	1	3.12	Serious Challenge
Lack of backup and recovery procedures	8	6	2	1	3.26	Very Serious Challenge
Inadequate documentation of incidents	8	6	2	1	3.26	Very Serious Challenge
Absence of post-incident reviews	9	5	2	1	3.29	Very Serious Challenge
Failure to apply lessons learned	7	6	3	1	3.12	Serious Challenge
Overall Mean					**3.20**	**Serious Challenge**

Table 4 presents the challenges encountered in recovery, documentation, and post-incident evaluation. The absence of post-incident reviews obtained the highest weighted mean of 3.29,

indicating that the organization lacks formal processes for evaluating incidents after resolution.

The lack of backup and recovery procedures and inadequate incident documentation both received weighted means of 3.26, indicating Very Serious Challenges. These findings suggest that cybersecurity incidents may not be properly recorded or reviewed, limiting organizational learning and continuous improvement.

The overall mean of 3.20 reveals that recovery and post-incident activities remain a serious challenge that requires attention through standardized documentation and evaluation procedures.

Summary of Challenges Encountered

Based on the quantitative and qualitative findings, the major challenges encountered in the implementation of cybersecurity incident response practices include:

- Lack of standardized IR procedures
- Absence of centralized incident reporting mechanisms
- Delayed reporting processes
- Limited cybersecurity knowledge and training
- Resource constraints
- Unclear roles and responsibilities
- Weak documentation practices

These findings served as the basis for the development of the Cybersecurity Incident Response Playbook.

Development of the Cybersecurity Incident Response Playbook

The development of the Cybersecurity Incident Response (IR) Playbook followed the Agile software development methodology, which emphasizes iterative planning. During the Requirements Gathering and Planning Phase, the researcher collected data through survey questionnaires, semi-structured interviews, and document analysis involving Learning Resource Personnel, Division ICT Personnel, Administrative Staff, and ICT Coordinators of the City Schools Division of Urdaneta. The findings identified significant challenges in the areas of incident detection and reporting mechanisms, incident response and containment procedures, and recovery, documentation, and post-incident evaluation. These identified challenges, together with the review of international cybersecurity standards such as the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27035, and applicable Philippine cybersecurity policies, served as the foundation for defining the functional requirements and scope of the playbook.

During the Design Phase, the researcher translated the identified requirements into a structured incident response framework specifically designed for Google Sites and WordPress-based learning resources. Standardized workflows, incident classification matrices, reporting and escalation procedures, communication protocols, response checklists, documentation templates, recovery guidelines, and post-incident evaluation forms were carefully designed to address the operational needs of the Schools Division Office. Roles and responsibilities of Learning Resource Personnel, Division ICT Personnel, Administrative Staff, ICT Coordinators, and Web Portal Administrators were likewise clearly defined to ensure accountability and coordinated incident handling.

The Development Phase focused on producing the initial version of the Cybersecurity Incident Response Playbook by integrating all identified procedures into a comprehensive operational guide. The playbook was organized into logical sections that outlined the complete incident response lifecycle, from incident identification to post-incident evaluation. Platform-specific response procedures for Google Sites and WordPress were incorporated to ensure that the playbook directly addressed the technologies utilized by the division.

In the Testing and Evaluation Phase, the developed playbook was presented to its intended users for evaluation using structured survey questionnaires and interviews. Guided by the Technology Acceptance Model (TAM), the evaluation focused on usability and user acceptance, particularly the respondents' perceptions of the playbook's clarity, practicality, ease of use, usefulness, and overall suitability for organizational implementation. The feedback obtained from the respondents was analyzed and used to refine the contents, improve procedural clarity, and ensure that the playbook aligned with the actual cybersecurity practices and operational requirements of the Schools Division Office.

Finally, during the Deployment and Refinement Phase, the finalized Cybersecurity Incident Response Playbook was completed after incorporating the recommendations obtained during the evaluation process. The completed tactical playbook consists of comprehensive components including the purpose and scope of the playbook; cybersecurity policies and standards; roles and responsibilities; incident severity classification; incident detection and reporting procedures; reporting workflows and escalation matrix; incident response and containment procedures; platform-specific response guides for Google Sites and WordPress; recovery and restoration procedures; incident documentation templates; communication and notification protocols; post-incident evaluation and lessons learned forms; incident response checklists; process flowcharts; appendices; and supporting references. These integrated components provide a standardized and practical operational guide that enables the City Schools Division of Urdaneta to consistently manage cybersecurity incidents affecting its web-based learning resources while strengthening its overall cybersecurity posture.

Table 5. Components of the Development of the Cybersecurity Incident Response Playbook

Component	Purpose
Incident Detection and Reporting Playbook	Standardize incident identification and reporting
Response and Containment Playbook	Guide personnel during incident response
Recovery and Restoration Playbook	Ensure service recovery and continuity
Documentation Templates	Standardized recording of incidents
Post-Incident Evaluation Procedures	Capture lessons learned
Google Sites Security Playbook	Platform-specific procedures
WordPress Security Playbook	Platform-specific procedures

Based on the identified challenges, a comprehensive Cybersecurity Incident Response Playbook was developed. The playbook provides structured procedures covering the entire incident response lifecycle and includes platform-specific guidance for Google Sites and WordPress. The developed playbook directly addresses the gaps identified in the quantitative and qualitative findings.

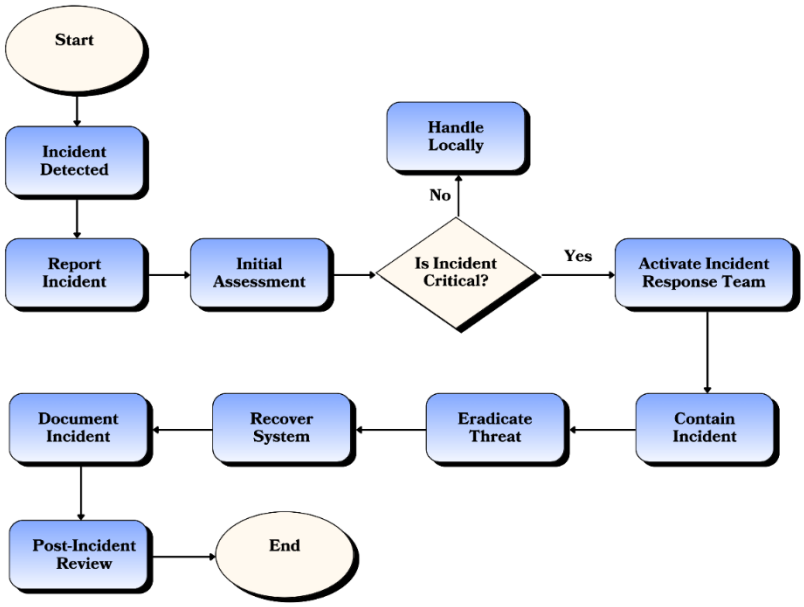

Figure 1. Cybersecurity Incident Response Workflow

The Cybersecurity Incident Response workflow illustrates the overall cybersecurity incident response process implemented in the City Schools Division of Urdaneta. The process begins with incident detection, which may originate from user observation or system alerts. Given that SDO environments often rely on manual detection, this stage is critical in ensuring early identification of threats.

Once detected, incidents are formally reported and assessed to determine their severity. The decision point distinguishes between minor and critical incidents, allowing efficient allocation of resources. Critical incidents trigger the activation of the Incident Response Team (IRT), ensuring coordinated and structured actions.

The containment, eradication, and recovery stages reflect the core of incident handling, where threats are isolated, removed, and systems restored. The inclusion of documentation and post-incident review addresses a major gap in manual systems by promoting accountability and continuous improvement. This structured flow ensures consistency, reduces response time, and aligns with cybersecurity best practices.

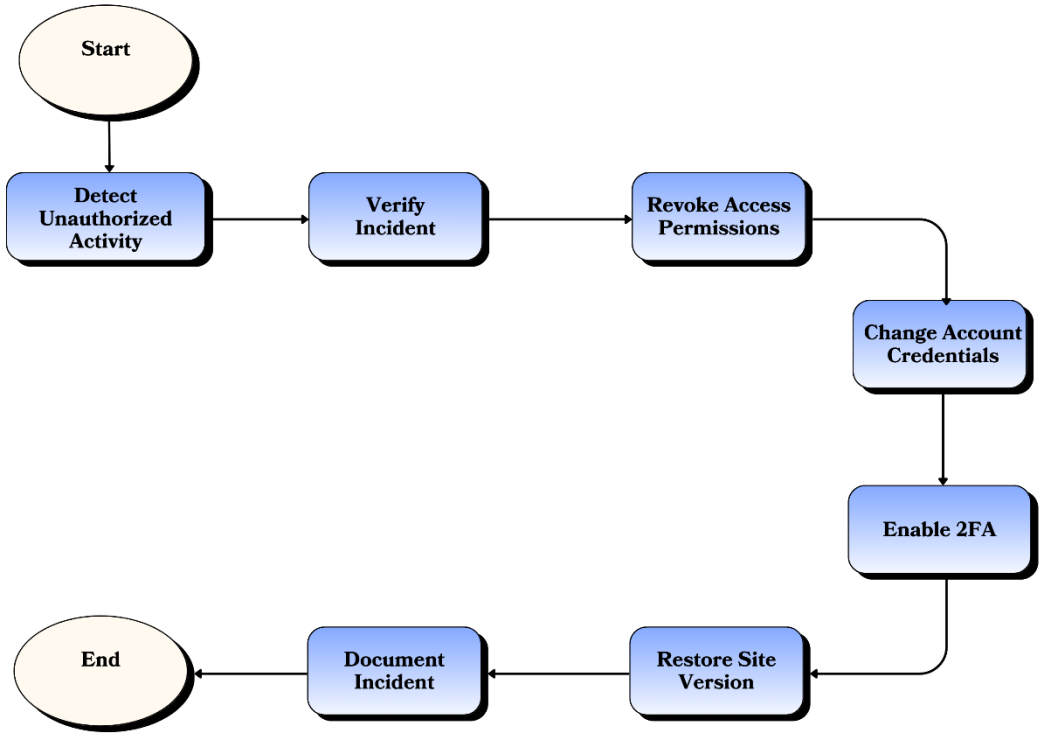

Figure 2 presents the incident response process specific to Google Sites. The flow emphasizes account-level security, as most incidents in Google Sites environments are related to unauthorized access or improper sharing permissions.

The process begins with detection and verification, ensuring that false alarms are minimized. Immediate actions such as revoking access and changing credentials are critical in preventing further unauthorized modifications. The activation of two-factor authentication (2FA) enhances account security and reduces the likelihood of recurrence.

The recovery stage focuses on restoring previous versions of the site using built-in version history, which is a key feature of Google Sites. This ensures minimal disruption to learning resources. The final documentation step ensures that all actions are recorded for future reference and improvement.

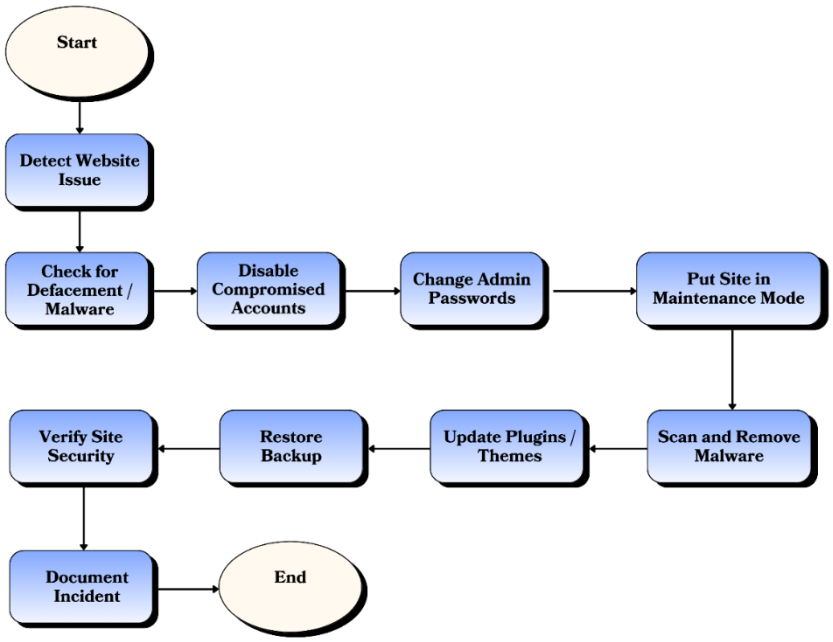

Figure 3. WordPress Incident Response Workflow

Figure 3 illustrates the incident response process for WordPress platforms, which are more vulnerable to attacks such as malware injection and website defacement. The flow begins with detection and verification of the issue, followed by immediate containment actions such as disabling compromised accounts and restricting access.

Maintenance mode is used to prevent further damage while remediation is ongoing. The eradication phase includes malware scanning and removal, ensuring that all malicious components are eliminated. Updating plugins and themes addresses vulnerabilities that may have been exploited.

Recovery involves restoring clean backups and verifying the integrity of the website. The structured approach ensures that all critical steps are followed, reducing the risk of reinfection. Documentation supports accountability and future improvements.

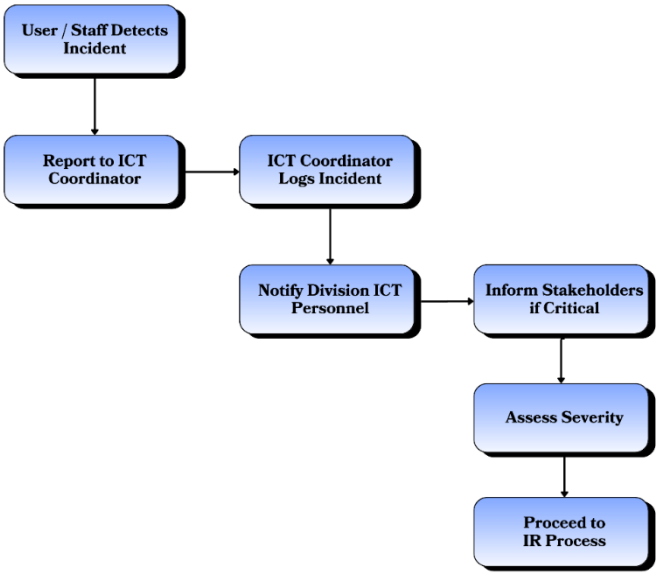

Figure 4. Incident Reporting and Communication Flow

Figure 4 shows the communication and reporting structure for cybersecurity incidents. This flow addresses one of the key challenges identified in the study, the lack of centralized reporting systems.

The process ensures that all incidents pass through a standardized reporting channel, beginning with the user and progressing to ICT personnel. Logging the incident creates a formal record, which is essential for tracking and analysis.

The escalation mechanism ensures that critical incidents are communicated to higher authorities, enabling timely decision-making. This structured communication flow improves coordination and reduces delays associated with manual reporting methods.

Usability and User Acceptance of the Developed IR Playbook

Following the development of the Cybersecurity Incident Response Playbook, its quality was evaluated in terms of usability and user acceptance by its intended users. As discussed in Chapter II, the Technology Acceptance Model (Davis, 1989) explains that users are more likely to adopt a tool when they perceive it as useful and easy to use. Likewise, ISO 9241-11 (2018) identifies usability as the degree to which users can effectively, efficiently, and satisfactorily achieve their intended goals. Previous studies further emphasized that user-centered evaluation is essential in determining whether cybersecurity operational guides are understandable, practical, and suitable for organizational implementation (Fallatah, 2024; Nyre-Yu, 2021). Anchored on these concepts, this section presents the respondents' evaluation of the developed Cybersecurity Incident Response Playbook.

Table 6. Usability Evaluation of the Developed Cybersecurity Incident Response Playbook

Criteria	4	3	2	1	Weighted Mean	Interpretation
Functionality	11	4	2	0	3.53	Highly Acceptable
Usability	10	5	2	0	3.47	Highly Acceptable
Reliability	9	6	2	0	3.41	Highly Acceptable
Security	10	5	2	0	3.47	Highly Acceptable
Overall Mean					**3.47**	**Highly Acceptable**

Verbal Interpretation Scale

Scale	Range	Interpretation
4	3.26 – 4.00	Highly Acceptable
3	2.51 – 3.25	Acceptable
2	1.76 – 2.50	Less Acceptable
1	1.00 – 1.75	Not Acceptable

Table 6 presents the usability evaluation of the developed Cybersecurity Incident Response Playbook. Functionality received the highest weighted mean of 3.53, indicating that respondents perceived the playbook as comprehensive and capable of addressing cybersecurity incident response requirements.

.

The overall weighted mean of 3.47 indicates that the developed playbook is Highly Acceptable in terms of functionality, usability, reliability, and security. The findings suggest that the developed playbook can serve as an effective cybersecurity management tool for web-based learning resources

Table 7. User Acceptance of the Developed Cybersecurity Incident Response Playbook

Indicator	4	3	2	1	Weighted Mean	Interpretation
The developed IR Playbook addresses the cybersecurity needs of the division.	10	5	2	0	3.47	Strongly Agree
The procedures provided are practical and easy to implement.	9	6	2	0	3.41	Strongly Agree
The playbook can improve the security of web-based learning resources.	11	4	2	0	3.53	Strongly Agree
The playbook should be adopted as a standard cybersecurity guide.	10	5	2	0	3.47	Strongly Agree
I am willing to use and recommend the playbook.	10	5	2	0	3.47	Strongly Agree
Overall Mean					**3.47**	**Strongly Agree**

Table 7 presents the level of user acceptance of the developed Cybersecurity Incident Response Playbook. The indicator "The playbook can improve the security of web-based learning resources" obtained the highest weighted mean of 3.53, interpreted as Strongly Agree. This finding indicates that respondents believe the developed playbook can significantly contribute to strengthening the cybersecurity posture of the City Schools Division of Urdaneta.

The indicators pertain to the playbook's ability to address cybersecurity needs, its adoption as a standard cybersecurity guide, and respondents' willingness to use and recommend the playbook each obtained a weighted mean of 3.47, also interpreted as Strongly Agree. These results suggest a high level of confidence in the effectiveness and applicability of the developed playbook.

Meanwhile, the indicator regarding the practicality and ease of implementation of the procedures obtained a weighted mean of 3.41, which remains within the Strongly Agree category. This demonstrates that the respondents perceive the playbook as user-friendly and suitable for implementation by personnel with varying levels of cybersecurity expertise.

The overall weighted mean of 3.47 indicates that the respondents strongly agree with the adoption and implementation of the developed Cybersecurity Incident Response Playbook. The findings confirm a high level of user acceptance and support the use of the playbook as a standardized cybersecurity incident response framework for web-based learning resources in the City Schools Division of Urdaneta.

Summary of Qualitative Findings

The interview results revealed that the developed Cybersecurity Incident Response Playbooks:

1. Provide clear and structured guidance for cybersecurity incident management.
2. Improve preparedness and response readiness.
3. Promote standardization and accountability among personnel.
4. Strengthen cybersecurity and risk management practices.
5. Received strong acceptance and support from intended users.

These findings corroborate the quantitative evaluation results, which showed that the developed playbooks were rated Highly Acceptable in terms of functionality, usability, reliability, security, and overall acceptability.

Overall Summary of Findings

The study revealed that the City Schools Division of Urdaneta experiences significant challenges in cybersecurity incident detection, reporting, response, recovery, and documentation. The quantitative and qualitative findings consistently identified the absence of standardized procedures, centralized reporting mechanisms, and structured post-incident evaluation processes as major concerns.

To address these challenges, a comprehensive Cybersecurity Incident Response Playbook was developed. The playbook provides standardized procedures for managing cybersecurity incidents involving Google Sites and WordPress and includes reporting templates, escalation procedures, recovery guidelines, and post-incident evaluation mechanisms.

The usability and user acceptance evaluation demonstrated that the developed playbooks are highly acceptable to intended users. The qualitative feedback further confirmed that the playbooks are practical, understandable, and relevant to the operational needs of the division. Collectively, these findings indicate that the developed Cybersecurity Incident Response Playbooks can serve as an effective framework for improving cybersecurity governance, strengthening incident response capabilities, and protecting web-based learning resources within the City Schools Division of Urdaneta.

CONCLUSION AND RECOMMENDATIONS

This section presents the conclusions drawn from the results of the study and provides recommendations based on the findings. The conclusions are derived from the statistical analysis and interpretation of the data gathered from the respondents regarding the development and evaluation of Cybersecurity Incident Response (IR) Playbooks for learning resources developed using Google Sites and WordPress in the City Schools Division of Urdaneta.

Conclusion

Based on the findings of the study, the following conclusions were drawn:

The study revealed that the City Schools Division of Urdaneta encounters several challenges of cybersecurity incident response (IR) practices across the areas of incident detection and reporting mechanisms, incident response and containment procedures, and recovery, documentation, and post-incident evaluation. The results indicated that the absence of standardized incident response procedures, unclear reporting mechanisms, inadequate documentation practices, limited cybersecurity awareness, and the lack of formal post-incident evaluation processes were among the major challenges experienced by personnel responsible for managing web-based learning resources. These findings demonstrate that the current cybersecurity IR practices are primarily manual, informal, and dependent on the individual knowledge and experience of personnel, resulting in inconsistencies in handling cybersecurity incidents.

In response to the identified challenges, a Cybersecurity Incident Response (IR) Playbook was successfully developed for web-based learning resources utilizing Google Sites and WordPress platforms. The developed playbook provides standardized procedures for incident detection, reporting, escalation, containment, recovery, documentation, and post-incident evaluation. It also includes reporting templates, incident documentation forms, workflow diagrams, and platform-specific response procedures designed to support Learning Resource Personnel, Division ICT Personnel, Administrative Staff, ICT Coordinators, and Web Portal Administrators in managing cybersecurity incidents effectively. The development of the playbook addressed the gaps identified during the assessment of existing cybersecurity practices and provided a structured approach to incident response management within the division.

The evaluation results further revealed that the developed Cybersecurity Incident Response Playbook attained a high level of usability and user acceptance among the respondents. The respondents strongly agreed that the playbook is practical, understandable, useful, and capable of improving the cybersecurity posture of web-based learning resources maintained by the City Schools Division of Urdaneta. The playbook was likewise perceived as an effective tool for standardizing cybersecurity incident response activities and enhancing organizational preparedness against cybersecurity threats. The positive evaluation results indicate that the developed playbook is suitable for implementation and can serve as a valuable cybersecurity management resource within the division.

Overall, the study concludes that the development and evaluation of a Cybersecurity Incident Response Playbook can significantly contribute to strengthening cybersecurity governance, improving incident response readiness, and promoting the protection of digital learning resources within the City Schools Division of Urdaneta. Through the adoption of standardized procedures and continuous cybersecurity improvement efforts, the division can better safeguard its web-based learning resources against evolving cybersecurity threats.

Recommendations

Based on the conclusions drawn from the study, the following recommendations are proposed:

The City Schools Division of Urdaneta formally adopted and implemented the developed Cybersecurity Incident Response Playbook as an official guide for managing cybersecurity incidents affecting web-based learning resources. Institutionalizing the playbook can help establish standardized incident response procedures and

promote consistency among personnel involved in cybersecurity management.

Regular cybersecurity awareness and incident response training programs should be conducted for Learning Resource Personnel, Division ICT Personnel, Administrative Staff, ICT Coordinators, and Web Portal Administrators. Continuous capacity-building activities can improve personnel competency in identifying, reporting, responding to, and recovering from cybersecurity incidents while ensuring effective utilization of the developed playbook.

The division may establish a centralized cybersecurity incident reporting and monitoring mechanism to complement the implementation of the playbook. Such a system can facilitate timely reporting, incident tracking, documentation, and coordination among concerned personnel, thereby improving the overall effectiveness of cybersecurity incident management.

Periodic review, validation, and updating of the Cybersecurity Incident Response Playbook should be undertaken to ensure its relevance and effectiveness in addressing emerging cybersecurity threats, technological developments, and organizational requirements. Cybersecurity is a continuously evolving field, and response procedures must likewise evolve to remain effective.

Web Portal Administrators and Learning Resource developers should integrate cybersecurity incident response planning into the design, deployment, and maintenance of web-based learning resources. Adopting security-by-design principles and incident preparedness measures can help minimize risks and improve organizational resilience.

Information Technology and cybersecurity practitioners within the Department of Education may utilize the developed playbook as a reference in formulating similar cybersecurity frameworks, guidelines, and operational procedures for other Schools Division Offices and educational institutions. The findings of this study may contribute to the strengthening of cybersecurity governance across the education sector.

Future researchers may conduct further studies focusing on the development of a web-based Cybersecurity Incident Management System that automates incident reporting, escalation, monitoring, and documentation processes. Additional studies may also evaluate the long-term effectiveness of the implemented playbook and explore its integration with broader cybersecurity governance frameworks and information security management systems.

The implementation of these recommendations is expected to enhance the cybersecurity preparedness, resilience, and security posture of web-based learning resources and support the continuous delivery of secure and reliable digital learning services within the City Schools Division of Urdaneta.

REFERENCES

1. Alharbi, F., & Tassaddiq, A. (2021). Cybersecurity awareness and practices in educational institutions: A systematic review. International Journal of Advanced Computer Science and Applications, 12(5), 613–621.
2. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
3. Department of Education. (2020). DepEd Order No. 12, s. 2020: Adoption of the Basic Education Learning Continuity Plan for School Year 2020–2021 in light of the COVID-19 Public Health Emergency. https://www.deped.gov.ph
4. Department of Education. (2021). DepEd Order No. 29, s. 2021: Adoption of the Basic Education Development Plan 2030 and Digital Rise Program. https://www.deped.gov.ph
5. Department of Information and Communications Technology. (2023). National Cybersecurity Plan 2023–2028. https://dict.gov.ph
6. El Hamdaoui, M. (2023). Cybersecurity threats in educational institutions: Current trends and mitigation strategies. Journal of Information Security and Applications, 73, 103448.
7. International Organization for Standardization. (2018). ISO 9241-11:2018 Ergonomics of human-system interaction—Part 11: Usability: Definitions and concepts. https://www.iso.org
8. International Organization for Standardization. (2018). ISO/IEC 27035-1:2016 Information technology—Security techniques—Information security incident

management—Part 1: Principles of incident management. https://www.iso.org

9. Kumar, R., Sharma, P., & Singh, A. (2024). Cybersecurity preparedness and incident response in educational institutions: A systematic review. Computers & Security, 137, 103614.
10. National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework
11. NIST. (2024). Computer Security Incident Handling Guide (Draft Revision 3, SP 800-61r3). National Institute of Standards and Technology. https://csrc.nist.gov
12. Ojala, J. (2024). Improving cybersecurity incident reporting and organizational response through standardized procedures. Journal of Information Security Research, 15(1), 44–61.
13. Republic Act No. 10173. (2012). Data Privacy Act of 2012. Official Gazette of the Republic of the Philippines.
14. Republic Act No. 10175. (2012). Cybercrime Prevention Act of 2012. Official Gazette of the Republic of the Philippines.
15. SANS Institute. (2023). Incident response playbooks. https://www.sans.org
16. Stallings, W. (2021). Effective cybersecurity: A guide to using best practices and standards (2nd ed.). Addison-Wesley.
17. Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th ed.). Cengage Learning.