RANSOMWARE ATTACK RESPONSE AND ENTERPRISE RECOVERY: A COMPREHENSIVE FRAMEWORK FOR CONTAINMENT, FORENSIC PRESERVATION, AND POST-INCIDENT HARDENING

Dr. Aniket Patel[1], Parikh Vishva[2], Dr. Rohit Patel[3]
[1] Associate Professor
Institute of Computer Technology
Ganpat University
Mehsana, India
arp02@ganpatuniversity.ac.in
[2] Student
Institute of Computer Technology
Ganpat University
Mehsana, India
vishvaparikh22@gnu.ac.in
[3] Professor
Institute of Computer Technology
Ganpat University
Mehsana, India
rohit.patel@ganpatuniversity.ac.in

ABSTRACT

The ransomware attacks have evolved into multi-phased attacks by incorporating both file encryption and data exfiltration in their operations. In this paper, we present a unified enterprise response framework that is geared towards quick isolation of the network, restriction of credentials, and thorough collection of forensic evidence as well as informed decision making on how to handle the attackers through negotiations. The framework describes the stages of the attack life cycle that should be followed to guarantee a successful response: Detect – Isolate – Preserve – Investigate – Contain – Recover – Harden. Negotiations with ransomware attackers can only be considered in high-priority cases where there is no backup of data and verification of a decryptor by law enforcement. This framework, which is based on NIST Special Publication SP 800-61, will provide organizations with guidance on how to deal with ransomware.

Keywords: *Ransomware, Incident Response, Forensics, Backup Recovery, Cyber Extortion, Decision Matrix, System Hardening.*

I. INTRODUCTION

The current statistics highlight the rising severity of ransomware attacks. For example, the number of ransomware-related complaints registered by the FBI IC3 for 2023 amounts to some 2,800 cases—constituting a roughly 18% year-on-year growth, as well as $74.3 million in financial losses reported[1]. Such figures illustrate ransomware's evolution from being a technical problem in IT infrastructure to becoming a full-fledged business disaster. In particular, today ransomware campaigns frequently use combined file encryption and large-scale data exfiltration as the strategy called double extortion. According to the industry survey conducted in 2024, roughly 59% of all businesses have been hit by ransomware, with nearly 70% of the attacks involving encryption and an average downtime of 24 days[2][3]. Thus, one can see that ransomware has shifted its focus from mere disruptions to actual cyber extortion.

Given this situation, it becomes obvious that a business needs an approach to ransomware that will take both technical and legal factors into account. That is what this study proposes to deliver with its developed response model based on threat intelligence and conventional incident response practices. More specifically, this model accounts for the risk-based approach, incorporating the evaluation of data importance and availability of backups as decision criteria. In addition, this model suggests negotiating strategies along with the typical IR phases. Decision matrices and negotiation trees are provided to help the organization decide between paying the ransom and resorting to backups.

II. BACKGROUND AND LITERATURE REVIEW

Incident Response Lifecycles: Incident response is defined as a structured life-cycle (e.g. NIST SP 800-61 Rev.3) that consists of preparation, detection/analysis, containment, eradication, recovery, and lessons learned[4]. These phases are recommended by similar frameworks (SANS, ISO/IEC 27035). But the special pressures of ransomware reveal weaknesses in these models. According to Lai et al., the ransomware playbooks that are currently available address technical attack situations, but they tend to neglect business goals, recovery priorities, and strategies in negotiation[9]. Practically, even a technically informed IR plan can bring systems back online without the executives being ready to deal with extortion threats or regulatory blowback.

Attack Trends: Variants of ransomware are more advanced. The 2022 report by ENISA records a period of data-based extortion: a selection of threat groups is now stealing over 10 terabytes of data each month to leverage it. Indeed, it has been analyzed that the effectiveness of double-extortion attacks is so strong that certain gangs have declared that they will only target data leaks but not file encryption. This change presents challenges and opportunities to defenders: by monitoring data transfers that are unusual (e.g. the use of tools such as Rclone, WinSCP(commonly observed in data exfiltration incidents)[5]), one can get early notice of an active attack. On the other hand, it implies that merely recovering a backup might no longer be sufficient in case of stolen information which needs to be recovered.

Forensic Preservation: Good forensic practice is the key to good recovery. Traditionally, teams have been encouraged to capture volatile evidence (capturing RAM, running processes) before non-volatile data (disk images, logs)[11]. This guarantees their preservation of critical artifacts (encryption keys in memory, malicious binaries)[11]. A hash and logging of all acquisitions ensures chain-of-custody. The industry guidelines emphasize gathering all the necessary logs: Windows Event Logs and Sysmon data,

Linux system logs, network flow logs, VPN/firewall logs, and so on. The correlation of the sources will enable the investigators to track the sequence of the attack. Our framework follows these practices, with evidence collection being a part of incident response.

Backup Resilience: Pre-incident backup strategy is a well known aspect of importance. Authorities frequently refer to the so-called 3-2-1 rule (three copies, two types of media, one offsite). ENISA particularly suggests immutable, offline backups due to ransomware, in line with its objectives of RTO/RPO. Recent advice (NIST and industry) continues to emphasize the need to secure backup systems - such as separate credentials and network segmentation of backup servers. We use these ideas in our recovery strategy of the framework such as a decision matrix which takes into consideration backup integrity (safe, partial, poisoned, etc.).

Negotiation and Decision Models: The issue of paying ransom is confronted. The U.S. regulators clearly express their dislike towards ransom payments, which is strongly discouraged, and the UK authorities say that the payments are not condoned[6]. The dilemma can be quantified by research: e.g. about 56 percent of paying companies received data back[7], but at the price of a lot more secondary demands in the future. Game theory models indicate that the victims must keenly evaluate the cost of downtime against the fine to pay to cybercrime. It is recommended that legal and law enforcement is involved at an early stage; an organization must confirm any decryptor keys prior to payment and ensure proper documentation of consent. We make this formalized in our work as a decision flow (Section 10), so that only in case of backups failure, when loss of business data would be disastrous, negotiation would take place.

III. PROPOSED FRAMEWORK

The above insights are incorporated in our proposed framework to create a response model at the enterprise level. It is based on a graduated strategy (see Figure 1) that prolongs regular IR life-cycles, including ransomware-specific operations. Detect, Isolate, Preserve, Investigate, Contain, Recover and Harden are important phases, but each of them is supplemented by strategic decision points. As an illustration, at the time of the Detect/Isolate, the framework also utilizes a Decision Matrix (founded on the importance of the data and backup) to define the further actions (Table I, Section 9). In the same vein, in Recover, we check a backup integrity check and then decide whether to restore or negotiate. This model assists in filling the gap between technical IR and executive decision-making by embedding business-context decisions at every stage.

Figure 1. Ransomware Incident Response Lifecycle.

A gradual process (Detect → Isolate → Preserve → Contain → Investigate → Recover → Harden) that incorporates decision making points and coordination between teams.

The framework focuses on integration between IT, legal and management. As an illustration, when there is a risk of loss of High-Value data without backup, the decision model will signal at once the necessity of the involvement of C-level and possibly negotiation. In case of backups, technical recovery will take precedence. Every stage encompasses tactical as well as policy reviews. In general, the design is intended

to make sure that no important step (e.g. data recovery of backups, contact with law enforcement, review of post-mortem) is forgotten amid the pressure of an incident.

IV. INCIDENT RESPONSE METHODOLOGY

In an active ransomware incident, the highest priority is halting further damage. The initial measure, in practice, consists in isolating impacted systems on the network. Cables on a network are usually unplugged or firewall blocks imposed on infected hosts within minutes of discovery to block lateral propagation. As an example, SMB/NFS file shares can be disabled at once and the VLAN of the server can be quarantined. All the suspected compromised accounts (service or administrator credentials) are disabled or reset. Most importantly, such containment measures are only taken after preliminary evidence is captured to prevent artifacts destruction.

Subsequently, responders are concerned with preservation of evidence. They verify telltale signs on every compromised server: abrupt extension changes of files, availability of ransom notes, or an abnormally high disk I/O or creation of archives. All the artifacts (the ransom note, encrypted file samples, unique file extensions) are stored. Write-blocked media is used to create a full disk image and the RAM is dumped to record in-memory keys or processes. Network perimeter access logs, VPN access logs and Active Directory access logs are all exported to be analyzed. Such copies are hashed (e.g. SHA-256) and recorded as soon as possible to ensure integrity.

Investigation: the preserved data is correlated by the analysts. They can see the precise files that have been encrypted and when the encryption started. Execution traces show the way the malware was executed (e.g. through scheduled tasks or the registry keys). Investigators also look into evidence of data exfiltration: they can locate tools such as Rclone or WinSCP in temp folders, or huge transfers in firewall logs. The objective is to trace the attack chain between the initial intrusion and data breach. This sparks subsequent Containment 2.0: when the knowledge is adequate, it will end all the malicious processes and the rest of the backdoors (new admin accounts) will be cleaned up.

All these measures are consistent with the best practices (NIST SP 800-61 guidance, SANS IR playbooks), but specific to the ransomware. The table II below summarizes the phased activities on a file server, in various ransomware situations. As an illustration, in Detect, the encryption-only attack indicator can be the alteration of file extension or the appearance of encrypted files, but the extortion-only attack can be represented by the huge uploads of archives. The Contain we stop services and firewall off the server. The table allows the responders to address all important tasks in a systematic manner.

Table II. File Server IR Actions by Phase and Ransomware Scenario.

IR Phase	**Encryption-Only Attack**	**Extortion-Only Attack**	**Encryption + Extortion**
Detect	File extensions change (e.g. ".locked"); ransom note appears; high write I/O.	Large-scale reading of sensitive data; creation of ZIP/RAR files.	Combination: both file encryption and large data transfers detected.

Isolate	Disconnect server from network; disable file-sharing protocols; block by firewall/switch; disable suspicious accounts.	Same steps as Encryption-Only.	Same steps as Encryption-Only.
Preserve Evidence	Take full disk image and memory snapshot; archive ransom note and encrypted files; collect relevant logs.	Preserve any staging folders and archives; collect logs of accesses; save evidence of file copying tools.	Preserve all relevant artifacts (logs, notes, both encrypted and exfiltrated data).
Investigate	Identify all encrypted folders; determine encryption timeline; check execution logs.	Trace accessed data and upload events; identify exfiltration tools (e.g. Rclone); correlate with network logs.	Perform both of the above: correlate encryption events with any exfiltration timeline.
Contain	Terminate ransomware processes; stop file services; disable file server operations.	Same as Encryption-Only.	Same as Encryption-Only.
Recover	Rebuild server from scratch; restore data from backups; verify integrity of restored files.	(No encryption to revert) Verify no further data leakage; restore systems.	Restore from backups; validate no malware remains before reconnecting.
Post-IR Hardening	Restrict file permissions; enable file integrity monitoring and auditing; implement least privilege.	Same as Encryption-Only; also monitor for leaked data exposure.	Same as Encryption-Only; prepare to initiate data takedowns if leaks occur.

This table is derived from industry playbooks and case studies. It ensures, for instance, that the *Preserve Evidence* steps always occur before any remediation.

V. FORENSIC PRESERVATION STRATEGY

File servers are primary ransomware targets and sources of forensic evidence. Investigations must follow a structured approach. The framework includes forensic evidence handling. One of the priorities is to capture volatile memory as soon as possible, as active decryption keys, or malicious processes can disappear during the shutdown. RAM is dumped using trusted tools and disks are quickly copied bit-by-bit. Every obtained data (memory image, disk image, encrypted files, logs) is hashed and digitally signed to guarantee its integrity throughout the years. This facilitates post recovery validation or litigation.

We gather logs of all the pertinent sources: Windows Event Viewer (and in particular, the Security and System logs), Endpoint Detection logs, Linux /var/logs, and network device logs (firewall, VPN, proxy, IDS). With detailed logs, it is possible to reconstruct the attack chain. Extortion can be verified by capturing how and when the data left the network (through a VPN or cloud upload, etc.). Practically, evidence is processed by a special forensic squad with the high chain-of-custody (signatures on all transfers, secure storage of the evidence). This process is optimised to ensure that delays are kept at the minimal level possible because any delay in this process will irreversibly lose important clues. Actually, lost memory captures or lost overwritten memory logs may indicate lost decryption key or key indicator of attack progress.

On the whole, preservation in our system is not an ancillary activity but a key part of every IR step (Detect, Preserve, Investigate). It guarantees that once it has been contained the organization is provided with a full, uncontaminated record of the breach to be analyzed, recovered and compliant with the law.

VI. BACKUP AND RECOVERY STRATEGY

Backup status is the driver of recovery strategy. The backup situation can be classified into: Safe (Intact), Partially Compromised, Deleted/Missing, Encrypted/Poisoned, or Immutable. The decision logic in every case is given in table III.

When backups are safe, it is easy to just isolate infected systems, wipe them, and put all data in the latest clean snapshot. We do the same validation of every backup even here (checking timestamps and hashes) to ensure that it was actually created prior to the attack.

When backups are Partially Compromised (some recent backups have been encrypted or lost), we find the last known clean backup and restore vital assets initially. Recently created data might be lost or might need to be restored using different means.

Deleted or Missing backups essentially leave the organization in no-backup situation (Section 11). In this case, we engage in recovery of the secondary sources (offline backup, email attachments, user devices) and scanning of publicly available decryptors. Only when the data value is high and these efforts fail, negotiation comes into the picture.

In case of backups that we find are Encrypted/Poisoned by the attacker, we do not restore them as-is. We instead consider it as a missing backup case, as using them may reintroduce malware. Any restore would only be attempted after a safe decryptor is obtained or other data recovered.

Lastly, Immutable backups (read-only snapshots) are maintained as end-of-the-road recovery points. Attackers are not able to modify these. We lock such snapshots and then restore them, being sure that the ransomware has not accessed them.

Table III. Backup Condition Decision Matrix.

Backup Status	**Recommended Action**
Safe (All Backups OK)	Rebuild systems and restore from the latest clean backup.
Partially Compromised	Restore from last verified clean backup; prioritize high-value data first.
Deleted/Missing	No reliable backups – follow no-backup recovery procedures (see Section 11).
Encrypted/Poisoned	Do not restore; focus on alternate recovery (decryptors, offsite copies).
Immutable Snapshot	Lock snapshot and restore systems safely from this untampered backup.

This plan is in line with NIST recommendations on contingency planning[12]. NIST SP 800-184 explicitly mentions the significance of off-site and immutable storage, in particular, due to the existence of the credible threat of ransomware, which encrypts the information and holds the decryption key as a ransom[8]. Our framework, by classifying the backup health upfront, eliminates the time-wasting second guesses and moves forward to the right recovery direction.

VII. DECISION MATRIX FOR RANSOMWARE SCENARIOS

We use the structured decision matrix to facilitate the first response (Table I). The inputs of the matrix are Data Value (High vs. Low), Backup Availability (Yes/No) and Attack Type (Encryption, Extortion or Both). The outputs are suggested actions: go to complete restoration (no payment), hire professionals to negotiate, or accept loss of data.

Table I. Ransomware Response Decision Matrix (Data Value × Backup × Attack Type).

Data Value	**Backup**	**Attack Type**	**Action**
High	Available	Encryption + Extortion	Do **not** pay. Restore from backups and inform stakeholders about data leak threat.
High	Available	Encryption Only	Restore from backups. No negotiation needed.
High	Available	Extortion Only	Restore data from backups; refuse payment.
High	Unavailable	Encryption + Extortion	Attempt decryptors or alternate recovery; if data is unrecoverable, negotiate under legal oversight.
High	Unavailable	Encryption Only	Try public decryptors; if unsuccessful, consider paying after risk evaluation.
High	Unavailable	Extortion Only	Engage law enforcement and data breach remediation; avoid payment.
Low	Available	*Any*	Restore from backups; refuse to pay (data is not worth ransom).
Low	Unavailable	*Any*	Recover what is possible (emails, local copies); generally decline to pay and accept data loss.

The use of this matrix will predetermine the risk-based decision: high-value assets that are not backed up will initiate negotiation procedures, but low-value assets will not. This decision juncture comes into play once the first evaluation has been done (prior to the commencement of any form of negotiation). It thereby limits options when stressed. An example is that a non-backup, high-value situation would warrant paying (with caution), but any situation with good backups would result in technical recovery and no payment. The explicit connection of the business impact (data value) to the response in the matrix inhibits ad-hoc or emotional decision making and guarantees consideration of regulatory/legal influences (e.g. sanctions risk) in a priori fashion.

VIII. NEGOTIATION STRATEGY AND CYBER EXTORTION HANDLING

Negotiation with attackers is highly risky and must follow strict rules. In general, most authorities advise strongly against paying ransom[6]. However, when extremely valuable data is at stake and all backups have failed, negotiation may be considered *only as a last resort*. Our model (Figure 2) formalizes this choice.

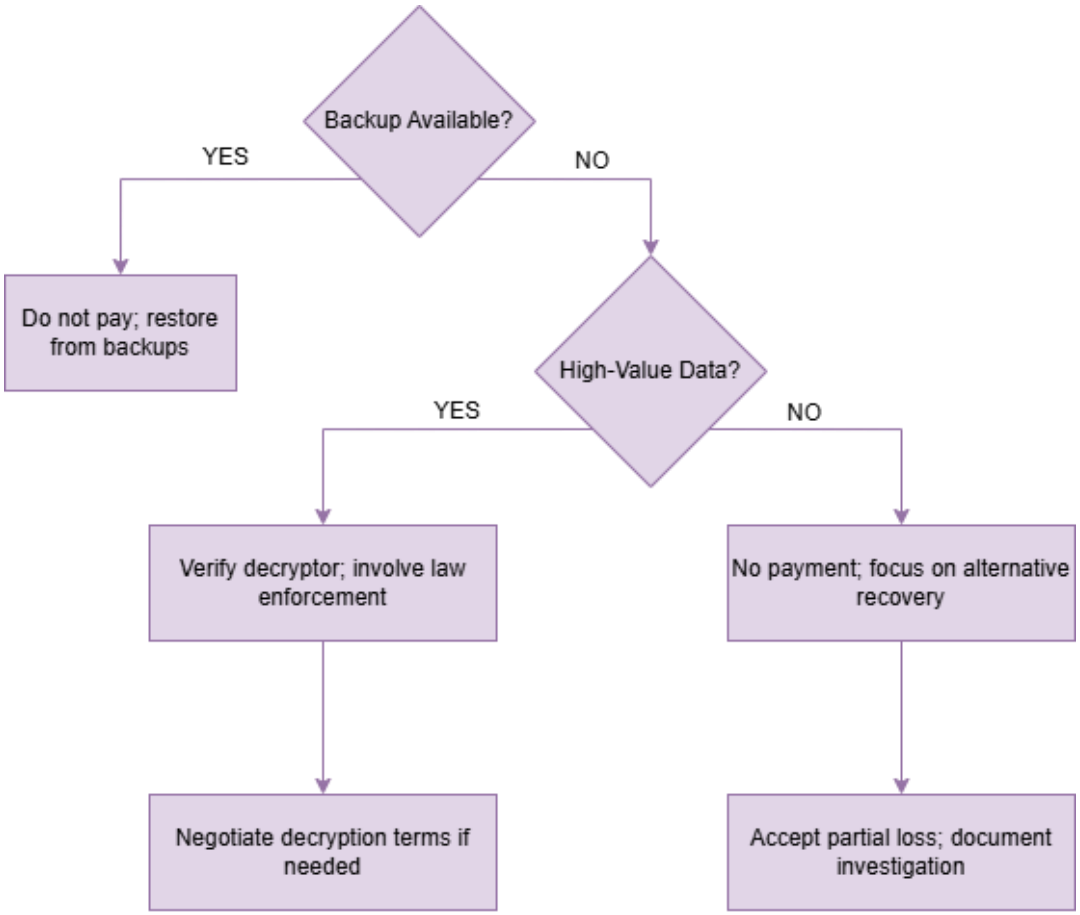

Figure 2. Ransomware Negotiation Strategy Decision Tree

A. **Backup Available:** Immediately reject payment. Recover operations using backups. The negotiation at this point is not required and is discouraged by law.
B. **No Backup, High-Value:** Begin controlled negotiation. First, the attacker is required to decrypt a sample file free of charge (to demonstrate the ability). Engage legal services and police early on. The ransom should be paid only in the case there are no other options to restore the data. All along, keep in mind that no guarantee of data return is given in paying. Negotiation in this case is simply a decision to take risks in peril.
C. **No Backup, Low-Value:** Do not negotiate. Rather, embrace partial loss of data and concentrate on containment and remediation.

The following steps are best practices: checking decryptors, minimizing the exposure of data, and obtaining the assistance of law enforcement. Interestingly, UK instructions clearly indicate that authorities do not condone payment[6], and that regulators caution companies that payment is not an alternative to

adequate security. Thus, we consider payment as just an operational risk, which can be considered only in situations when the business operation is not possible.

IX. CASE-BASED RESPONSE MODELING

We illustrate the framework using two opposite cases:

A. **Backups Present:** A financial services company has unchangeable backups and is attacked by a twofold extortion attack on its client database (high-value data). No ransom is demanded at all at the decision matrix. The staff restores all the systems that are affected by backups, verifies data integrity and gets operations up and running in hours. Meanwhile, an incident response coordinator takes care of the breach disclosure and monitors darknet sites. The company thereby does not have to pay a ransom and limits the damages through technical means.

B. **No Backups:** A manufacturing company that does not have recent backups is struck with the same attack. The decision matrix, now, results in controlled negotiation. The responders make efforts to recover data using alternatives (offline copies, partner systems) and find a decryptor tool. When the progress is not satisfactory after 48 hours, the executives give a go ahead to call the negotiator of the attacker. They initially require evidence-of-keys (e.g. decryption of some files). Law enforcement is kept informed of communications. Eventually, a decryptor can be acquired via negotiation or the company has to reconstruct by using partial data that was not destroyed.

The cases underscore the flexibility of the framework. In Case A, when there are backups, it is a technical recovery strategy. In Case B, the backups are not available, and the plan involves risk assessment and payment possibilities. These changes of approach are captured in Table I and in the negotiating tree (Figure 2).

X. POST-INCIDENT HARDENING FRAMEWORK

After the incident closure the organization deploys a multi-layered hardening plan:

A. **Short-term (0-30 days):** Fill the most pressing gaps. Patch every system (particularly those which are exploited). Implement multi-factor authentication on sensitive accounts and access points. Change or delete high-privilege credentials. Isolate servers (file, identity, backup) with a firewall. Facilitate stronger logging and endpoint detection of valuable assets. Such measures prevent the re-use of obvious attack vectors.

B. **Short-to-Mid Term (3-6 months):** Revise backup architecture: Implement a 3-2-1-1-0 policy (3 copies, 2 media, 1 offsite, 1 immutable, 0 errors) and quarterly restore exercises. In use Zero Trust network model (tight access controls, micro-segmentation). Deploy a Security Information and Event Management (SIEM) system to centralize logs and detect anomalies. Start active threat hunting drills to identify any left-over intrusion evidence. Provide new ransomware training to train personnel.

C. **Long Term (>6 months):** Implement advanced defenses. Identify ransomware activity in real-time with machine learning or behavior-based tools. Install deception tools (honeypots, spoof credentials) in order to get attackers revealing themselves accidentally. Ensure cloud and SaaS data are protected via native immutability and versioning features. Conduct frequent red-team

drills to check preparedness. Lastly, incorporate ransomware into the overall business continuity strategy and analyze supply-chain security to identify potential indirect exposures.

These stacked defenses are in line with professional suggestions. As an illustration, NIST and industry organizations point to the importance of immutable backups and regular patching as a key factor in resilience[8]. The point is that it is not a one-step process but a continuing program of improvement, which will be informed by lessons learned during the incident.

XI. ADVANCED DEFENSE MECHANISMS

In addition to conventional safeguards, we propose new safeguards. Machine learning and artificial intelligence (AI) can identify ransomware by identifying the usual patterns of file-access and reporting anomalies (e.g. dozens of files encrypted in seconds). Unapproved processes can also be blocked by behavioral whitelisting, which prevents alterations on business data. Deception platforms seed canary files and credentials; as an attacker tries to utilize them, the environment immediately notifies defenders. Anti-ransomware modules on Endpoint Detection and Response (EDR) tools also can kill suspicious encryption operations in progress. Lastly, sharing threat intelligence (through ISACs or CERT feeds) can assist companies in predicting novel ransomware variants and indicators. Although such sophisticated defenses are costly to invest in, they can greatly cut dwell time and damage in case an attacker breaks through first line perimeter defenses[2].

XII. DISCUSSION

This framework fills the gaps in existing guidance, filling technical IR with strategic decision-making. Our model is based on explicit negotiation protocols, business-impact analysis, unlike many other playbooks that stop at containment. It uses the most recent threat intelligence (of exfiltration indicators, trends in double-extortion) at each stage. As an example, instead of relying on system restoration[4], which NIST focuses on, we introduce a decision point to compare backups and ransom payment prior to recovery. Our approach provides specific decision tables and flow charts with respect to ransomware, in contrast to the general resilience advice provided by ENISA.

The complexity of the framework, however, is a trade-off: it presupposes cross-functional teams (IT, legal, compliance) to coordinate. The negotiation process could be quite challenging to organizations that have no resources. In addition, not all the details (including specific thresholds of the data qualifying as high value) can be coded in advance; there is still some judgment involved. With that said, the framework minimizes ad-hoc errors and makes it accountable by offering a structured template. To automate the process further, automated orchestration (e.g. IR platforms triggering decision branches) could be a future work.

XIII. CONCLUSION

Finally, this paper illustrates a holistic response and recovery model of ransomware attacks, which incorporates both short-term containment and long-term decision-making. The framework helps organizations to understand when to use backups, when to negotiate, and when to rebuild by classifying incidents based on data value, backups availability, and type of attack. The phased IR model helps to align every technical step (isolation, forensics, restoration) to the business and legal priorities. This framework

should be implemented to help to reduce the recovery time and lower the ransom payments so that the financial and reputational damage can be reduced. Finally, pre-attack preparedness and a layered security posture are essential to successful ransomware defense; this framework offers a roadmap to do so.

REFERENCES

[1] Federal Bureau of Investigation (FBI), "Internet Crime Report 2023," 2024.

[2] Verizon, "2024 Data Breach Investigations Report," 2024.

[3] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Nov. 2023.

[4] National Institute of Standards and Technology (NIST), "Computer Security Incident Handling Guide," SP 800-61 Rev. 3, Apr. 2025.

[5] European Union Agency for Cybersecurity (ENISA), "Threat Landscape for Ransomware Attacks," 2022.

[6] UK Government, "Financial Sanctions Guidance for Ransomware," 2026.

[7] Y. Sun et al., "Ransomware Negotiation: Dynamics and Privacy-Preserving Mechanism Design," IEEE Trans. Dependable Secure Computing, 2025.

[8] National Institute of Standards and Technology (NIST), "Guide for Cybersecurity Event Recovery," SP 800-184, 2016.

[9] H. Lai et al., "Proactive Ransomware Incident Response Model," IEEE Security Workshops, 2025.

[10] National Institute of Standards and Technology (NIST), "Contingency Planning Guide for Federal Information Systems," SP 800-34 Rev. 1, 2010.

[11] M. Casey, "Digital Evidence and Computer Crime," 3rd ed. Academic Press, 2011.

[12] National Institute of Standards and Technology (NIST), "Ransomware Risk Management: A Cybersecurity Framework Profile," NIST IR 8374, 2025.