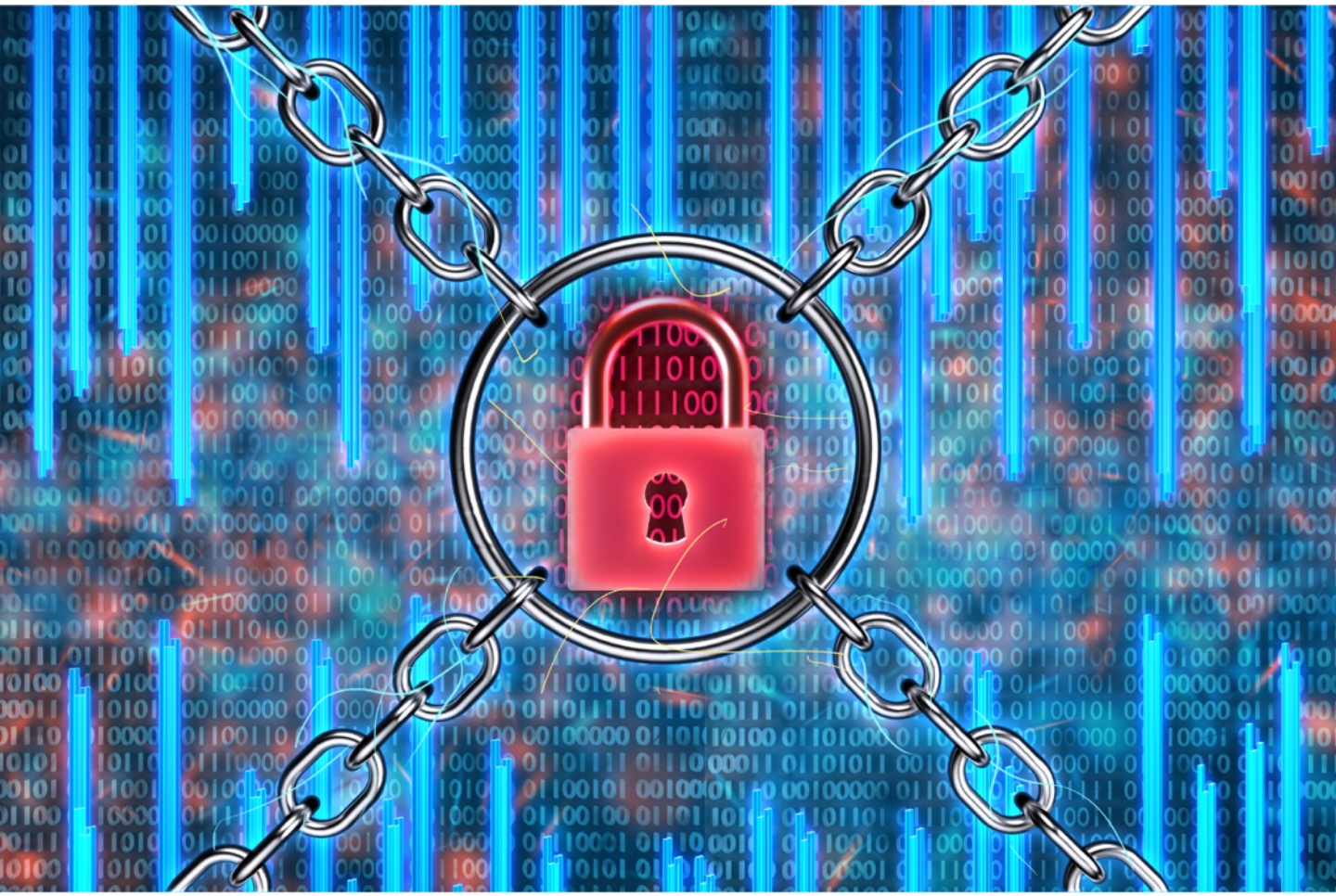
Ransomware Playbook

Best Practices and Starter Guide



Pillar Technology

P A R T N E R S

V 05132022

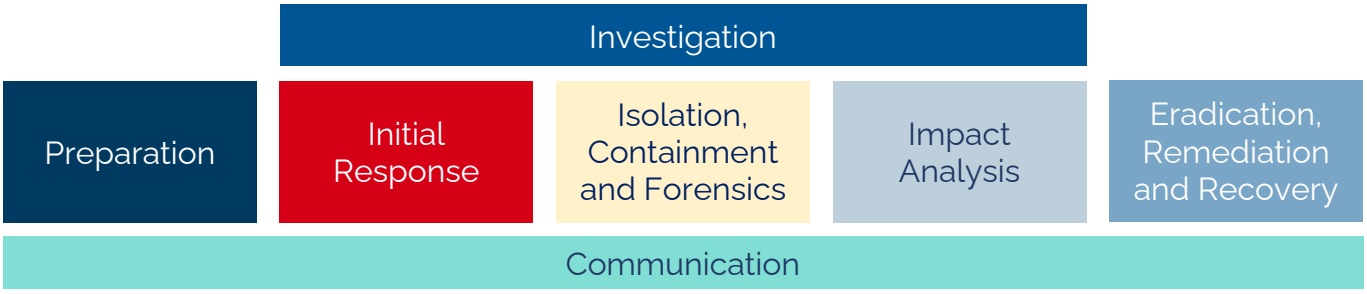
Ransomware continues to threaten organizations worldwide. In 2021, the average ransom demand was $2.2m, with the average payment rounding out at roughly $540k. Threat actors continue to improve and enhance attack methodologies, and ransomware-as-a-service makes this attack method more accessible to cyber criminals.

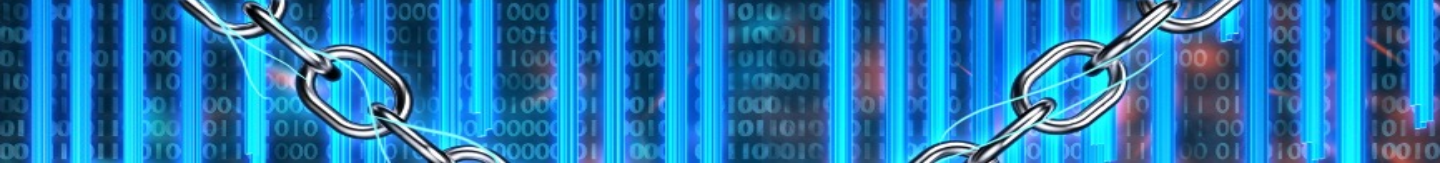
The purpose of this document is to provide a framework and best practices for ransomware planning, rapid response, remediation and recovery.

This document is intended to provide guidelines each organization can customize to fit their specific environment and business. Context must be considered to ensure relevance of any ransomware response plan.

The framework presented is designed to provide focus and deliberation on each step of the process. Each process typically involves different employees and organizations that must be coordinated. Clear ownership of the entire process is essential to ensure that all processes support each other and allow for rapid, coordinated response. Program management is critical.

Ransomware Framework





Investigation

Preparation	Initial Response	Isolation, Containment and Forensics	Impact Analysis	Eradication, Remediation and Recovery

Communication

- Discuss necessity for more rapid response to ransomware.
- This plan, while linked to traditional incident response plan, should be distinct to ensure rapid response necessary for ransomware incidents.
- Form a Ransomware Rapid Insertion Team (RRIT) which is on call and has the authority to take 'ALL ACTIONS NECESSARY' to stop a ransomware attack.
- Create and deploy all procedures and technologies necessary to detect and protect the organization from a ransomware attack:
    - Secure mail gateways
    - Web and URL filtering
    - Multifactor Authentication (MFA)
    - Security Information & Event Management (SIEM)
    - Network segmentation
    - Endpoint detection, EDR tools
    - Data loss prevention
    - Security awareness training
    - Air-gapped backup
- Implement and train team on Investigation & Forensic toolsets
- This phase includes testing of this plan (table-top testing) and incorporation of lessons learned as part of a continuous improvement process.
- COORDINATE WITH COMMUNICATIONS TEAM

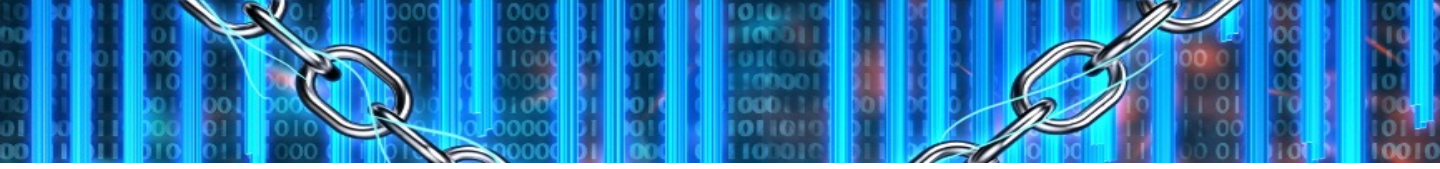
Initial Response

How an organization reacts to ransomware attack can make the difference between a major impact and a minor disruption. The keys to a successful Initial Response include:

- Quick notification to the RRIT
- Immediate isolation of impacted systems
- Diagnosis of ransomware variant
- Development of point of entry hypothesis
- Protection of evidence

- General Counsel for the organization should be engaged immediately to ensure appropriate legal response and to protect all communications.
- Notify Insurance Carrier of the event and determine if Law Enforcement involvement is appropriate.
- Determine need to engage third party forensic support.
- Conduct initial interviews with user(s) who reported issue, and document initial understanding.
- Determine if business continuity plan activation is necessary.
- COORDINATE WITH COMMUNICATIONS TEAM

Evidence protection should be the first thought before any analysis occurs.



Isolation, Containment and Forensics

It is vital to isolate any devices which may have been impacted by ransomware. This containment could involve:

- Limiting access to other network segments
- Disconnecting equipment from the network or the Internet
- Blocking communications with other devices
- Potentially stopping business services until the impact is understood

Once the impacted machines have been isolated and the attack is contained, forensics teams can begin to analyze the attack and determine what happened and how it occurred.

- Create a system image and memory capture of affected devices.
- Conduct detailed analysis of logs and detection systems to identify evidence of infection or abnormal activity.
- Follow path of attack
    - Initial entry
    - System level tactics and techniques
    - Lateral movement
    - Encryption methodology and technology
    - External communications (command and control)
    - Likelihood of exfiltration
- COORDINATE WITH COMMUNICATIONS TEAM

Evidence protection should be front of mind.

Impact Analysis

When the attack is better understood, it is important to assess damage which has occurred. This will involve:

- Defining files which have been impacted
- Understanding if any data may have been exfiltrated

It is also important to understand what customer data and regulatory requirements may exist to ensure notification compliance requirements are met.

The final piece of impact analysis is to estimate the financial impacts which have been incurred, including:

- Outage/productivity loss/ revenue loss
- Reputational and market share loss
- Professional services expense
- Technology costs
- Recovery related expenses
- Third-party impact expense
- If necessary, ransom costs.

- COORDINATE WITH COMMUNICATIONS TEAM

Eradication, Remediation and Recovery

- Once ransomware has been contained, eradication can begin.
- This can involve anything from the simple eradication of ransomware components to full bare-metal restoration of systems.
    - **Ensure 100% of the components of the ransomware are removed so the environment cannot be reinfected.**
- Determine if data be decrypted by a known decryptor (check with federal agencies).
- Determine what to do with exfiltrated files (e.g. communicate with customers, regulators, etc.). COORDINATE WITH COMMUNICATIONS TEAM
- Determine if ransom payment is required in order to recover. Consider professional ransom negotiator or law enforcement agency.

PAYMENT OF RANSOM NOT RECOMMENDED, IF AT ALL POSSIBLE

- Remediation and recovery in many cases involves the complete restoration of available data from backup.
    - **Thus, it is extremely important to maintain multiple copies of backups that can not be reached from the network (air-gapped).**
- Prioritize systems for restoration.
- Issue password resets for all affected systems including email accounts.
- Coordinate filing of insurance claims.
- Coordinate with legal and communications team to determine legal, regulatory and reputation repair.
- Resume normal business operations.
- Conduct lessons learned to understand failed or missing controls and mitigate future incidents.

Communications

An effective communications plan includes:

- Internal communications (which could be segmented into those involved, those with a need to know and all other employees)
- External communications
- Client communications (which could be segmented into current, past a prospective clients)
- Media and Press responses (news outlets, social media, website)
- Regulatory and government notifications (agencies, regulatory bodies, compliance organizations, FBI, USSS, IC3)
- Website and/or portal updates

Training on the plan is essential for all employees as well as communications team

Table-top testing goes a long way towards ensuring smooth communications and execution during an incident.

Pre-planned and pre-scripted communiques accelerate communications as well as ensure that all audiences and facets of any situation have been considered, outside of a time of potential crisis.

PLAN
BE PREPARED
RESPOND QUICKLY

FOR MORE ASSISTANCE

CONTACT PILLAR TECHNOLOGY PARTNERS

678-341-0808