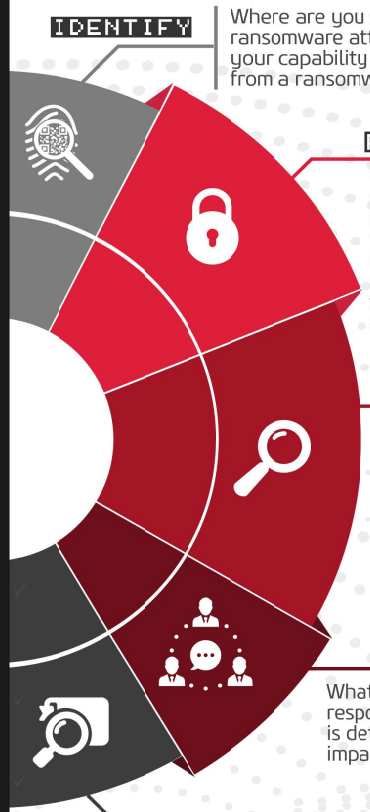
Ransomware Playbook

Ransomware exploits human and technical weaknesses to gain access to an organization's technical nfrastructure in own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack.



Ransomware Best Practices

IDENTIFY

Determine Susceptibility to and Impact resulting from a Ransomware Attack

- Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
  - i. What are your most significant threats and vulnerabilities?
  - ii. What are your highest cybersecurity risks?
- Discuss the role of cybersecurity in contracts with third-party support vendors and crucial suppliers.
- What mission essential functions depend on information technology and what are the cascading effects of their disruption?
- What other sources of cybersecurity threat intelligence does your organization receive? For example, information from Federal Bureau of Investigation (FBI), InfraGard, opensource reporting, security service providers, others?
- How well do your service level agreements or BAA address incident response?
- Does your cyber insurance have a plan for ransomware?
- Have you tested your backups? What is your RTO and RPO for recovery from a ransomware attack?
- Are your employees trained to identify potential ransomware and phishing attacks?
- Potential losses from a Ransomware Attack?
- Are your systems patched?
- What are your critical systems?

PROTECT

Take steps to reduce the risk of an Attack

- How is cybersecurity integrated into both organizational and project risk assessments and management?
- Does your organization employ a formal sanctions process?
- Does your organization have a cybersecurity incident response plan?
- Does it include a process for responding to indicators of ransomware?
- Does this plan include a risk management strategy that addresses the following considerations?
  - i. The risks of not patching reported vulnerabilities.
  - ii. Extended downtime?
  - iii. Impaired functionality?
  - iv. The loss of data?
- Does your organization utilize multi-factor authentication to mitigate the potential effects of phishing?
- Keep systems patched and updated
- Is there a terminations checklist and reviews of access for third party accounts?
- Are there flowcharts showing the high-level relationships and crisis lines of communication?
- Is there a plan of protective actions for non-impacted systems?
- Implement Phishing training (KnowBe4) or similar?
- Have you implemented tools which can block ransomware attacks?
- Do you test your employees on their ability to detect ransomware and Phishing attacks?

DETECT

Implement Technologies and Practices to Identify Ransomware Attacks or Vulnerabilities

- How do employees report suspected phishing attempts?
- What actions does your department take when suspicious emails are reported?
- Does your department conduct phishing self-assessments?
- What is your baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
- What resources and capabilities are available to analyze the intrusions?
- Spam Filtering
  - i. Imprivata Fair Warning
  - ii. Mimecast
  - iii. Forcepoint
  - iv. O365 Filtering
- IDS Implementation
- HIDS – Host Based Intrusion Detection System
  - i. OSSEC - https://www.ossec.net
  - ii. Wazuh - Wazuh · The Open Source Security Platform
- NIDS – Network Based Intrusion Detection System
  - i. Snort - https://www.snort.org
  - ii. Suricata - https://suricata.io
- DNS Filtering Malicious Domain Blocking
  - i. CISCO Umbrella https://www.cisecurity.org/msisac/services/mdbr/

RESPOND

Ransomware Response Plan

- What is your planned cyber incident management structure?
  - i. Who (by department and position) leads incident management and why?
  - ii. How are they notified?
- Do you have someone within your organization who monitors the Dark Web?
- What is your chain of evidence processes and forensics process?
- Does your organization carry Cyber Liability insurance? What is covered?
- When do you activate your IRP team and Insurance company?
- Is there a way to maintain service availability of key assets?
- Do you pay the ransom?
  - i. Who decides?
  - ii. What's the process?
  - iii. What are the advantages/disadvantages to paying?
  - iv. What are the political ramifications?
  - v. What outside partners/entities do you need to contact?
- Are you connected to a third-party IT provider to help support your decision?
- Have you proactively identified and established the service provider relationships needed for incident/breach response issues (e.g. credit courseling forensic/computer security services)?

RECOVER

Assess, Restore, Notify, Learn, Claim

- Assess – Determine the impact of the attack
- Determine the systems that have been infected
- Quarantine the affected systems
- Restore – Get back to a production state before a Ransomware attach
- What formal policies and procedures does your organization use to decide when and how to restore backed-up data, including measures for ensuring the integrity of backed-up data before restoration?
- Does your organization have back-ups of vital records in a location that is separated from your primary working copies of your files?
- How much downtime would exist between your primary files and the restoration of files via your back-up?
- How confident are you in the restoration process?
- Notify – Communicate internally and externally as needed on the attack
- Notify key stakeholders during all stages of the restoration process
- Assign a team member to address the public on the event and the restoration process.
- Learn – What can be learned to reduce an attack in the future?
- Increased monitoring
- Determine if the restoration process was efficient
- Claim – File a claim with your Cyber Insurance carrier