Ransomware Playbook
By Raqib Chowdhury

Step	Action	Rational
1. Identify	Complete an inventory of all IT assets.	Document all hardware, software, systems, and data, and identify which assets are critical for business functions. This is essential for prioritizing protection and recovery efforts for business critical assets.
1. Identify	Conduct a formal ransomware risk assessment.	Identify specific threats and their potential impact on critical assets. As well as establish an acceptable level of risk.
1. Identify	Define clear roles and responsibilities for the Incident Response Team	Ensure everyone knows who is in charge of decision-making, containment, and communication *before* an attack occurs.
2. Protect	Implement and enforce the principle of Least Privilege.	Ensure users and system accounts only have the minimum permissions necessary for their jobs to prevent privilege escalation by threat actors.
2. Protect	Enforce a strong password and multi-factor authentication policy.	Dedicated MFA protects against credential theft, and a lockout policy slows down brute-force attacks by threat actors. Decreasing the potential spread of attacks
2. Protect	Implement and test a robust, isolated backup strategy.	Critical data must be backed up, and secured, to ensure smooth recovery or enforcement of a business continuity plan. A hot site that is offsite is preferable.
2. Protect	Maintain a comprehensive vulnerability and patch management program.	Continually hunting for vulnerabilities allows organizations to stay ahead of zero day exploits and many

		other exploits that may lead to ransomware attacks.
2. Protect	Implement network segmentation and isolation policies.	Divide the network into zones to prevent ransomware from spreading across the entire organization. This also isolates malware, which slows down potential spread.
2. Protect	Develop and conduct mandatory employee training and awareness programs.	Train employees on recognizing phishing, social engineering, and safe use practices such as not connecting to the company server from a public network to prevent initial infection.
2. Protect	Implement application whitelisting and configure security software.	Use anti-malware and antivirus (AV) software like Windows Defender, and strictly abide by a whitelist of approved applications to prevent unauthorized programs (like new ransomware variants) from executing.
3. Detect	Implement continuous security monitoring	Continuously monitor network traffic, system logs, and user behavior for unusual activity, which can indicate the presence of a threat actor or a running ransomware process.
3. Detect	Audit systems and networks regularly.	Review logs and system configurations to find anomalies or unusual activity that may not be flagged by automated tools.
3. Detect	Develop and test detection processes.	Ensure security teams are alerted when pre-defined indicators of compromise are found, such as mass file encryption, unusual network communication, or suspicious account lockouts.
4. Respond	Execute the Incident Response Plan and establish communications.	Follow the pre-defined IRP, confirm the incident, and initiate communication protocols with IT, Legal, PR and external stakeholders (Law Enforcement, customers, regulatory bodies) as

		needed.
4. Respond	Contain the incident.	Immediately isolate affected systems and network segments to stop the ransomware from spreading and limit the damage.
4. Respond	Analyze the attack.	Determine the initial access vector, the extent of the damage, and which systems were affected.
4. Respond	Eradicate the threat.	Remove the ransomware code, malware, and all threat actor backdoors or persistence mechanisms from the network. This includes wiping and rebuilding systems if necessary to ensure a clean slate.
5. Recover	Restore systems and data from secure backups.	Use the isolated and verified backups to restore business-critical systems and data to a pre-incident state.
5. Recover	Implement system improvements and validate functionality.	Correct the vulnerabilities that allowed the ransomware attack to succeed before reconnecting the systems to the network. Fully test and validate that all systems are operational and secure.
5. Recover	Communicate recovery activities.	Keep internal and external stakeholders informed of the recovery status, ensuring transparent public relations where required.
5. Recover	Conduct a post-incident review and update plans	Hold a lessons-learned meeting to document what happened, what went well, what failed, and use this information to update and improve the Identify, Protect, Detect, and Respond functions.