END TO END
ENTERPRISE SOLUTIONS

RANSOMWARE RESPONSE CHECKLIST

www.eecomputing.com

END TO END
ENTERPRISE SOLUTIONS

RANSOMWARE RESPONSE CHECKLIST

Ransomware continues to be a major cybersecurity threat with a significant increase in incidents over recent years. In 2023, the number of ransomware victims surged by 55.5%, with a total of 5,070 attacks documented—a notable rise from the previous year. This escalation is reflected in both the increased number of ransomware groups and the sophistication of their attacks. LockBit, Clop, and BlackCat were among the most active ransomware-as-a-service (RaaS) groups in this period (Cyberint) (Trend Micro).

As an increasingly prevalent form of malware, ransomware often gains access to your systems through spear phishing emails and the malicious software targets your critical data and systems for extortion. Once it gains access to higher order network systems, it locks you out of your data and
the attacker issues a demand for payment to release your data. Security experts agree that paying the ransom is the worst thing you can do since many attackers lack the keys that will guarantee giving you access to your data.

Ransomware is frequently delivered through spear phishing emails. After they have locked the user out of the data or system, the cyber attacker demands a ransom payment. While there are many types of ransomware threats, some of the most active include:

1. Ryuk, targets logistics/technology companies, local/ state government agencies and municipalities with the ransomware arriving via spam.
2. The LockerGoga ransomware, which often targets industrial and manufacturing environments. It often arrives via compromised credentials, modifies the passwords of the infected systems' user accounts, and prevents infected systems from being rebooted.
3. GandCrab ransomware gains access to the domain controller to compromise an enterprise host.
4. RobbinHood, which has targeted local and state governments and municipalities, arrives via insecure remote desktops or trojans and encrypts each file with a unique key

Recent ransomware trends show a broad diversification of ransomware families and an increase in ransomware-as-a-service (RaaS), which allows cybercriminals to launch attacks more easily. This change is driven by technological advancements and the increasing sophistication of cybercriminal networks that continuously develop new ransomware variants and tactics

PREVENTIVE MEASURES CHECKLIST

○	Perform a risk assessment of your organization to identify any vulnerabilities and potential risk of cyber-attack vectors.
○	Perform a network vulnerability assessment to pinpoint gaps in systems and security protocols.
○	Implement an awareness and training program since end users such as employees are primary targets. Virus-laden email attachments are a key infiltration tactic for ransomware, so educating everyone to never click unsolicited links or open unsolicited attachments in emails is paramount. It's important to have internal or external security teams test the workforce periodically with simulated phishing emails.
○	Institute a policy and controls that are guided by least privilege access standards. This ensures that only authorized users have access to privileged accounts while also defining and restricting administrative access to only those that absolutely need it with very specific access parameters.
○	Set anti-virus and anti-malware programs to conduct regular scans automatically
○	Implement consistent patch management protocols and ideally a centralized patch management system to ensure updated patches on all operating systems, software, and firmware on devices.
○	Consider implementation of next gen firewalls (NGFW) or ensure that stately firewalls are configured to block access to known malicious IP addresses at the very least.
○	Put strong spam filters in place to help prevent phishing emails from making it to end users. Also implement technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM). This supports inbound email authentication to prevent email spoofing.
○	Implement policy restrictions on software that includes any needed technology controls to stop program execution in common ransomware locations. These can include temporary folders for internet browsers compression/decompression programs, including the AppData/LocalAppData folder
○	If you are not using Remote Desktop protocol (RDP), you should consider disabling it.
○	Set up application whitelisting protocols to ensure that only authorized systems can execute authorized programs that are validated by security policies.
○	Perform periodic penetration testing to ensure that all endpoints and security systems have no vulnerabilities as your network evolves over time.

Ransomware Incident Response

Measures While proactive prevention of ransomware attacks by guarding end points like the network and implementation of employee education are key, you also need to have a plan in place to recover from a ransomware attack:

- Develop and implement an Incident Response plan that provides a detailed roadmap of how cybersecurity incidents are handled.
- Put a comprehensive data and systems backup and recovery plan in place to ensure that critical systems, application and data are backed up offsite in the cloud for recovery in the event of a ransomware attack. This system to revert to backups during an incident should be regularly tested.

Guarding against ransomware requires ongoing vigilance and planning to meet evolving threats and increasingly sophisticated attackers. While this checklist is an important foundation in protecting your public or private organization, it's important to have the support of an experienced MSSP to partner with internal IT teams.

By providing the security expertise technologies, implementation and consultative support, you have a partner that can deliver the needed long-term planning and execution to keep your data and systems safe. At End-to-End Computing, we specialize in ransomware preparedness. Contact us at eecomputing.com, and we'll set up a complimentary risk assessment for your organization.