October 2021 Vol. 21-10

Advanced & Fully Automated Cybersecurity Risk Management

Swimage Monthly Newsletter

NIST Ransomware Profile

In September, the National Institute of Standards and Technology (NIST) issued a report titled *Cybersecurity Framework Profile for Ransomware Risk Management**. This report contains a Ransomware Profile which provides guidance on helping organizations prevent, respond to, and recover from ransomware events.

The purpose of the Ransomware Profile "is to help organizations identify and prioritize opportunities for improving their security and resilience against ransomware attacks."

The profile suggests the following "basic preventative steps that an organization can take now to protect against the ransomware threat":

- Use antivirus software at all times.

- Keep computers fully patched.
- Segment networks.
- Continuously monitor directory services (and other primary user stores) for indicators of compromise or active attack.
- Block access to potentially malicious web resources.
- Allow only authorized apps.
- Use standard user accounts versus accounts with administrative privileges whenever possible.
- Restrict personally owned devices on work networks.
- Avoid using personal apps from work computers.
- Educate employees about social engineering.
- Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has the appropriate access only.

To help recover from a future ransomware event, the following steps are recommended:

- Make an incident recovery plan. Develop and implement an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify business-critical services to enable recovery prioritization, and business continuity plans for those critical services.
- Backup data, secure backups, and test restoration. Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
- Keep your contacts. Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

The bulk of the report consists of a Ransomware Profile table which provides detailed guidance and informative references to the NIST Cybersecurity Framework Version 1.1. The main categories are the five Cybersecurity Framework Functions:

- Identify
- Protect
- Detect
- Respond
- Recover

For purposes of this article, we are focusing on the Recover function. The sub-categories for the Recover function include:

- Recovery Planning - Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

- Improvements - Recovery planning and processes are improved by incorporating lessons learned into future activities.

- Communications - Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

The report also contains multiple helpful references and resources, including NIST SP 800-184, *Guide for Cybersecurity Event Recovery*.

Ransomware risk management is essential for every organization. *Cybersecurity Framework Profile for Ransomware Risk Management* provides extremely helpful guidance to prevent, respond to, and recover from ransomware events.

*https://doi.org/10.6028/NIST.IR.8374-draft

Swimage + TRANXITION
Ransomware Recovery

Swimage + Tranxition Ransomware Recovery

Swimage + Tranxition Ransomware Recovery fits into the NIST Ransomware Profile as a vital component of the Recover function.

Installation of our Ransomware Recovery solution is a fundamental part of the recovery planning process. Our software performs incremental backups and stores them in a secured location. Upon the occurrence of a ransomware event, the systems are automatically rebuilt from the ground up, from a known good source. This includes the operating system and applications. Then user data, profiles, and settings are restored from the secure backup location. This is all completed in about an hour and multiple systems may be rebuilt at the same time.

Please visit Swimage.com/RansomwareRecovery for more information, including a short video.

We are offering existing customers a special discount for Swimage + Tranxition Ransomware Recovery. Please contact us to discuss how we can assist with your organization's ransomware recovery planning.