Published on *The National Law Review* https://www.natlawreview.com

NIST Issues Cybersecurity Framework for Ransomware Risk Management

Article By:

Scott Ferber

Todd S. McClelland

Michael G. Morgan

David P. Saunders

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued a Ransomware Profile* identifying steps organizations can take to prevent, respond to and recover from ransomware events**. According to the profile, its "purpose…is to help organizations identify and prioritize opportunities for improving their security and resilience against ransomware attacks." NIST encourages organizations to use the document as a guide for profiling the state of their own readiness and to identify gaps to achieve their goal.

IN DEPTH

Modeled on NIST's Cybersecurity Framework Version 1.1, the profile provides practical guidance to organizations to protect against the ransomware threat, including the following "basic preventative steps":

- Use antivirus software at all times;
- Keep computers fully patched, including scheduled checks and installation of patches "as soon as feasible";
- Segment networks;
- Continuously monitor directory services (and other primary user stores) for indicators of compromise or active attack;
- Use products or services to block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity;

- Allow only authorized applications—including establishing processes for reviewing, adding or removing authorized applications—on an allowlist;
- Use standard user accounts versus accounts with administrative privileges whenever possible;
- Restrict personally owned devices on work networks;
- Avoid using personal apps—like email, chat and social media—from work computers;
- Educate employees about social engineering; and
- Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has the appropriate access only.

The profile outlines steps that organizations "can take now" to help recover from a future ransomware event, including:

- Develop and implement an incident recovery plan that has defined roles and strategies for decision-making and identifies business-critical services to enable recovery prioritization;
- Carefully plan, implement and test a data backup and restoration strategy, with secure and isolated backups of important data; and
- Maintain an up-to-date list of internal and external contacts for ransomware attacks.

The profile applies the five foundational pillars of cybersecurity (*i.e.*, identify, protect, detect, respond and recover) to ransomware. Based on this framework, organizations should, among other things:

- Inventory assets, systems and processes, including where controls may be shared with third parties;
- Ensure everyone in the organization understands their roles and responsibilities for preventing and responding to ransomware events, with documentation memorializing the structure;
- Establish and communicate policies needed to prevent or mitigate ransomware events, which are in line with legal and regulatory requirements;
- Factor ransomware risks into organizational risk management governance;
- Ensure the ability to receive cyber threat intelligence from information-sharing sources;
- Understand the business impact and expenses of potential ransomware events;
- Implement an incident response plan that appropriately prioritizes ransomware events, has defined roles, contains both technical and business responses and is regularly tested (to ensure the plan and processes match changing organizational needs and structures, as well

as new ransomware types and tactics);

- Coordinate ransomware contingency planning with suppliers and third-party providers;
- Conduct ongoing training regarding ransomware threats; and
- Monitor personnel activity to detect insider threats, insecure staff practices and compromised credentials.

NIST's guidance comes on the heels of a variety of measures from the Biden administration to combat ransomware, including:

- Deputy National Security Advisor Anne Neuberger's June 2, 2021, Open Letter to Corporate Executives and Business Leaders, emphasizing that the private sector has a "critical responsibility" to protect against cyber threats, "urg[ing]" businesses "to take ransomware crime seriously and ensure [their] corporate cyber defenses match the threat," and recommending a variety of cyber "best practices" to be implemented by companies (*i.e.*, multifactor authentication, endpoint detection and response, encryption, and a skilled, empowered security);
- The creation of a Ransomware & Digital Extortion Task Force led by the US Departments of Justice and Homeland Security on June 3, 2021;
- President Joe Biden's August 25, 2021, meeting with corporate leaders from technology, finance, energy and water, insurance and education sectors to discuss the "whole-of-nation" effort needed to address cyber threats, especially in critical infrastructure;
- The US Department of the Treasury's September 21, 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments; and
- Guidance from the Federal Bureau of Investigation's (FBI) Internet Crime Compliant Center's (IC3) (Ransomware: What It Is & What To Do About It), Cybersecurity and Infrastructure Security Agency (CISA) (Stop Ransomware), and CISA and FBI (Ransomware Awareness for Holidays and Weekends).

In addition, a bipartisan group of US Senators has introduced the Cyber Incident Notification Act, which, if enacted, would require federal agencies, government contractors and critical infrastructure owners and operators to report cyber intrusions to CISA within 24 hours of their discovery. A number of states—including New York, North Carolina, Pennsylvania and Texas—are considering legislation that would ban or restrict state and local government agencies from paying ransom in the event of a cyberattack.

NIST's recent guidance and the parallel executive and legislative branch action underscore that ransomware is both a top-of-mind concern across the government and that there may be heightened expectations for what constitutes reasonable cybersecurity measures.

**Ransomware is a type of malware that encrypts an organization's data, with cyber actors demanding payment as a condition of restoring access to that data. In some instances, the cyber*

actors also may steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors or the public.

***NIST's National Cybersecurity Center of Excellence (NCCoE) has produced additional reference materials intended to support ransomware threat mitigation. These include:* NIST Special Publication (SP) 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, which addresses how an organization can handle an attack when it occurs and what capabilities it needs to have in place to detect and respond to destructive events;* NIST SP 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, which addresses how an organization can work before an attack to identify its assets and potential vulnerabilities and remedy the discovered vulnerabilities to protect these assets;* NIST SP 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events*, which addresses approaches for recovery should a data integrity attack be successful; and* Protecting Data from Ransomware and Other Data Loss Events*, which is a guide for managed service providers to conduct, maintain and test backup files that are critical to recovering from ransomware attacks.*

National Law Review, Volumess XI, Number 266