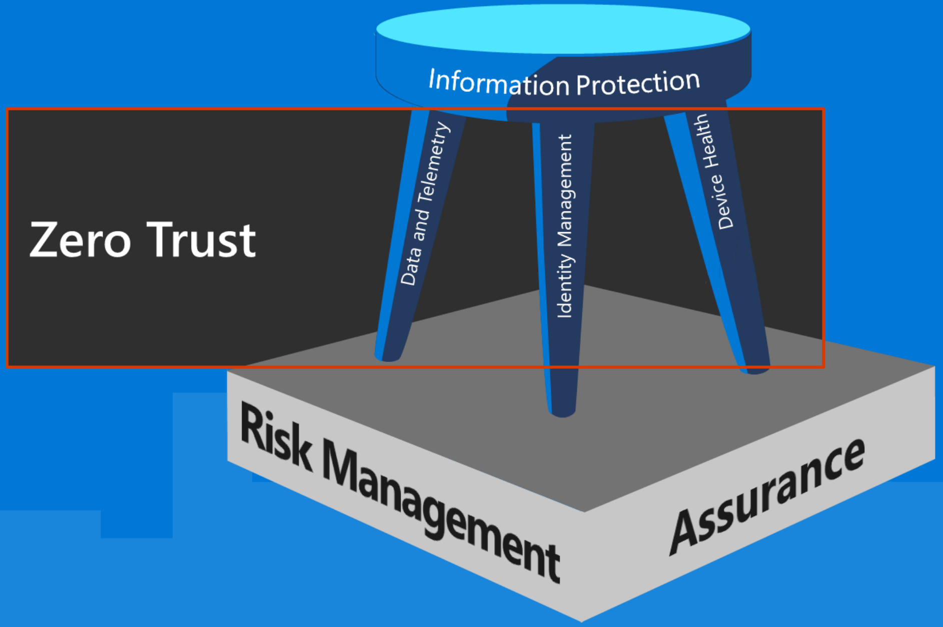
Microsoft

Microsoft’s NIST Ransomware Position

Carmichael Patton
Senior Security Architect



Key Recommendations

Microsoft Recommendations for NIST are to address common points of confusion around the attacks and where organizations should do first, next, and after that (1-2-3 style guidance)

1. Clarify Terminology and Scope – Drive clarity to address common misperceptions about these attacks.
   - *Extortion beyond ransomware* – While ransomware is the main monetization angle ("pay me to get your systems/data back"), the attackers are also aggressively stealing data and threatening to disclose on dark web or the internet (and likely keeping for later use).
   - *Enterprise-wide scope and impact* – We still see significant perception that current attacks are basic cryptolocker attacks (circa 2013), many professionals still don't realize the sophisticated toolkit/affiliate business model, use of human attack operators to steal admin credentials, and buying/selling of access to organizations from otherwise low risk commodity malware operators (e.g., botnets).
2. Publish Simple Prioritized Guidance – Develop and promote simple straightforward guidance (1-2-3 Steps) that links to deeper resources/documents on how to do it (e.g., clear simple visuals on a website/PDF/slide deck, not a formal paper with 3-5 pages of government headers).
   - Why: While NIST has done an awesome job of addressing many aspects of these attacks, organizations still struggle with where to start (especially smaller organizations with limited staff and experience).
   - How: Clearly state top priorities, and why they are important. Microsoft recommends starting with steps in the "Recommended Mitigation Prioritization" based on our learnings.
3. Create detailed Instructions for top recommendations.
   - NIST should prioritize making following these steps as easy and clear as possible (via NCCoE projects and other efforts).
   - This should include both Technical Procedures through the NCCoE process (or an accelerated version of this process) and Project guidance to accelerate planning and improve project success.

Prioritized Mitigations

Step 1: Prepare for the Worst: recover without paying

- What: Plan for the worst-case scenario and expect that it will happen (at all levels of the organization)
- Why: This will both help your organization to limit the
  - Damage from an attack to your organization
  - Financial returns of the attacker
- How: Organizations should ensure they
  1. Include ransomware to your Enterprise Risk Management (ERM) risk register
  2. Define and Backup Critical Business Assets
  3. Protect backups against deliberate erasure and encryption
  4. Test ‘Recover from Zero’ Scenario
  5. Reduce on-premises exposure by moving data to cloud services with automatic backup & self-service rollback.

Prioritized Mitigations

Step 2: Limit Scope of Damage: Protect Privileged Roles (starting with IT Admins)

- What: Ensure you have strong controls (prevent, detect, respond) for privileged accounts like IT Admins and other roles with control of business-critical systems.
- Why: This slows and/or blocks attackers from gaining complete access to your resources to steal and encrypt them. Taking away the attackers’ ability to use IT Admin accounts as a shortcut to resources will drastically lower the chances, they are successful at attacking you and demanding payment / profiting.
- How: Organizations should have elevated security for privileged accounts (tightly protect, closely monitor, and rapidly respond to incidents related to these roles)

Step 3: Make it harder to get in: incrementally remove risks

- What: Prevent a ransomware attacker from entering your environment + rapidly respond to incidents (to remove attacker access before they can steal and encrypt data).
- Why: This causes attackers to fail earlier and more often, undermining the profit of their attacks. While prevention is the preferred outcome, it is a continuous journey and may not be possible to achieve 100% prevention and rapid response across a real-world organization (with complex multi-platform, multi-cloud estate and distributed IT responsibilities).
- How: Organizations should lean in to the Zero Trust Architecture and identify and execute quick wins to implement or strengthen security controls to prevent entry and rapidly detect/evict attackers while implementing a sustained program that helps them stay secure.