REQUEST FOR COMMENT RESPONSE

RANSOMWARE RISK MANAGEMENT: A CYBERSECURITY FRAMEWORK 2.0 COMMUNITY PROFILE

September 10, 2025

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") request for comment on *Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile* ("draft profile") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike welcomes the opportunity to respond to NIST's draft profile. Adversaries are increasingly cloud-focused and are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally and maintain persistent access for malicious activities like ransomware - making this consultation timely and relevant.[1] Ransomware continues to be an acute threat to U.S. entities across multiple critical sectors, including telecommunications, technology, finance, government, and notably healthcare. The shift towards more aggressive extortion tactics, including threats to publicly leak sensitive data, underlines the severity and urgency of this threat.

[1] 2025 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/explore/2025-global-threat-report?tab.consessionscheduledday=1730400114135003mEeJ&utm_medium=dir

Adversaries are increasingly fast, agile, and brazen. The entry barrier for a ransomware operator has considerably lowered with the development of Ransomware-as-a-Service offerings, where Ransomware technology can be purchased or leased on a commission basis from more sophisticated groups to lesser capable groups, with powerful tools that automate the complex steps of targeting a victim.

As adversaries continue to evolve and find new ways to target victims, organizations must increase their emphasis on cybersecurity practices that leverage the most effective technologies.

A. Table 1. Ransomware Community Profile Feedback

PR.AA-03 correctly notes that most ransomware attacks are conducted through network connections, and social engineering-based compromise of passwords is a major source of compromise. The document recommends authentication of identities using phishing-resistant multi-factor authentication (MFA).

Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

CrowdStrike recommends the "Ransomware Application" column include a recommendation for Zero Trust architecture implementation in PR.AA-03. Additionally, we recommend this category be designated a Priority 1.

PR.PS-04 notes that the availability of audit/log records can assist forensics in support of recovery and response processes. Organizations should collect and retain security-relevant log information to support not only responsive use-cases, but also proactive security measures and threat hunting. The advent and increasing adoption of Next-Generation Security Information and Event Management (Next-Gen SIEM) tools allows defenders to leverage such data to these ends.

CrowdStrike recommends proactive security measures and threat hunting be listed in the ransomware applications column as use cases of logging practices. Additionally,

due to logging practice's important role in a cybersecurity strategy, PR.PS-04 should be a Priority 1.

PR.IR-01 correctly notes that many ransomware attacks are executed remotely and recommends the use of zero-trust network principles. NIST also states because remote attacks are so prevalent, this outcome is designated Priority 1. CrowdStrike agrees with this recommendation and designation as a Priority 1, and recommends it remain in the final draft of the profile.

DE.CM-03 describes that monitoring personnel activity can sometimes detect insider threats or insecure staff practices, and thwart potential ransomware events. The category also explains that monitoring can also be used to find unusual patterns of usage, like someone logging on from another country.

The ransomware application column should recommend organizations deploy Endpoint Detection and Response ("EDR") in this category. EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks.

In addition to recommending EDR deployment, CrowdStrike recommends this category be designated Priority 1.

III. CONCLUSION

We appreciate NIST's efforts to provide resources to organizations which in turn will improve cybersecurity practices. As NIST moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving

adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

VII. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com