Carnegie Mellon University
Software Engineering Institute

Building a New Assessment: How to Assess Ransomware Attack Readiness and Recovery

Brett Tucker
August 2023

Introduction

In 2021, approximately 37 percent of global organizations in IDC's 2021 Ransomware Study reported being the victim of a ransomware attack. Tech Target, which reported on the study, also noted that in 2021 and 2022, new ransomware trends emerged as attackers realized that certain techniques, such as supply chain attacks and double extortion, yielded better results. To get an appreciation for the scope of these attacks, AAG reported that there were 623.3 million attacks in 2021. Ironically, AAG also reported a 23% drop of attacks in 2022, which may be an indication of improved defenses. Regardless, ransomware has targeted critical infrastructure. A ransomware attack on a water distribution system in Israel, for example, shook executives at American utilities, and one on a petrochemical plant in Saudi Arabia revealed the vulnerability of its oil production.

Protection of our nation's critical infrastructure and those agencies and organizations that support it is of the utmost priority. The CERT Division at the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) aims to provide organizations with recommendations that would both reduce the likelihood of a ransomware attack and mitigate its effects if one was to occur.

Methodology and Catalyst

In the wake of the Colonial Pipeline ransomware attack CERT tapped its expertise in cyber risk management and assessment to give organizations an understanding of their security posture and their ability to prevent, detect, and respond to a ransomware attack. The goal of any assessment may include the collection of quantifiable evidence that relates appropriate deployment of control measures to protect their systems and demonstrate resilience in the face of an attack. The collection of such evidence may allow organizations to gain appreciation of their susceptibility to potential ransomware attacks. Unfortunately, assessments of this nature are driven largely by the context of the organization.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Demographic considerations for size, resources, mission, and strategy may influence how an organization assesses its risk exposure to ransomware. Therefore, CERT would like to prescribe specific considerations and requirements for proper ransomware assessment development.

In building out such an assessment methodology, CERT recommends that organizations exploit several widely accepted standards and resources to create a robust foundation for generally accepted practices. For example, organizations may seek direction from CISA Cross-Sector Cyber Performance Goals (CPGs) and the controls outlined in the NIST 800 series to build recommended control suggestions on gaps in security posture. To help organizations prioritize control selection, some organizations may also rely upon the MITRE ATT&CK Framework for a perspective on attack vectors commonly used by ransomware attackers.

Determining which organizational assets are in scope is an important part of any assessment. The CERT Resilience Management Model (CERT-RMM) may help organizations select focus areas, or domains, an organization should consider, beginning at the highest level, with the primary goals and objectives of an organization. OCTAVE FORTE provides a methodology for value stream mapping where overarching objectives can be decomposed into critical services. If an organization operates in the power sector, for example, an overarching objective might be to provide a service to a customer while earning revenue. Breaking that down, the identified critical service might be the delivery of electricity. From that, the organization's critical assets can be further categorized into the following:

- **people**—those who operate and monitor a service
- **information**—data associated with that service
- **technology**—tools and equipment that automate and support the service
- **facilities**—location or site that contains other assets
- **external dependencies**—third-party relationships and supply chain

These assets may also be categorized as high-value assets (HVAs), as defined by U.S. Government FIPS 199 because all derive their importance from their ability to meet the organization's mission.

The final step in developing a ransomware assessment is to acknowledge that, depending on available resources, many private organizations can supplement their ransomware resilience with assistance from consulting firms or cyber insurance providers. They can provide not only pre-event services, such as consultation for response strategies, but also services during and after a ransomware attack.

Ultimately, the ransomware assessment should focus on assets that derive their value from their importance in meeting the organization's service mission and assesses ransomware exposure in terms of susceptibility and ability to recover from an attack.

Assessment Nuts and Bolts

The duration of assessments depends upon the scope of the assessment and availability of resources. Regardless, CERT recommends that this type of assessment should initially survey the organization for "big picture" gaps to inform deeper dive research. Ultimately, the duration of the assessment should not be so long that the organization loses visibility and momentum for completion nor diminish the return on investment for gaining insight to ransomware risk exposure.

Preparation includes the initial notification of stakeholders, scheduling meetings, scope planning, and kickoff. A day or two may be scheduled for on-site, facilitated discussions. These technical exchange meetings provide important interface between assessors and organizational subject matter experts to gain greater clarification on technical issues. This onsite meeting may be followed by 10-15 days of report writing and post assessment. Unless necessary, the assessed organization may lose context and momentum to address critical issues if the post assessment period lingers.

After some research and testing, CERT recommends the use of at least eight subject matter areas, also known as domains, that may help organizations identify critical questions to ask when beginning an assessment:

- **business continuity disaster recovery (BCDR)**—includes backup systems or strategies, incident response, and backup testing. This domain focuses on ensuring that organizations ask if they have the right testing scenarios for ransomware.
- **configuration management**—includes allow/block lists, baselines, restricting permissions, limits to installations, and registry permissions
- **endpoint protection**—addresses cyber hygiene including anti-virus, intrusion prevention system (IPS), and web content
- **identity access management**—includes multi-factor authentication (MFA), least privilege enforcement, password management, and user/privileged account management
- **incident management**—focuses on event reporting and escalation including the type of reporting (i.e., when an incident occurs, how will it be reported across the organization)
- **network protection**—includes access limitations (such as remote desktop protocol), email management, and network segmentation

- **risk management**—includes insurance and user training
- **vulnerability management**—includes software updates, vulnerability scanning, and audit.

An organization's capabilities in these domains can be rated as fully implemented, partially implemented, or not implemented, which then correlates to the degree of susceptibility of the organization to ransomware attacks.

Lessons Learned

As alluded to earlier, CERT has developed and conducted a variety of methodologies with a large federal civilian agency, large municipalities, and private organizations. These experiences taught CERT some valuable lessons:

- **scope**—Trying to narrow the scope to one high-value-asset (HVA) system, such as a payroll, can be challenging. Because ransomware typically infects an entire environment—including people, technology, facilities, and external dependencies—a single-asset focus was incomplete. Organizations may begin with an HVA system as an anchor and then expand to all assets touched by that system or its subsystems.
- **operational tempo**—The organization's operational tempo must be acknowledged because it can greatly influence progress. As an example, an assessment team may realize a need to adapt to the organization's availability of critical resources such as subject matter experts. This might involve breaking up a technical exchange meeting over several days to accommodate different schedules of the stakeholders involved.

- **domain establishment**—From the outset, it is important to establish the assessment domains to be included in scope to help the organization identify who should participate in the technical exchange meeting. A discussion surrounding BCDR, for example, would involve different employees than a meeting on risk management, which would typically involve an enterprise risk manager.

- **data quality**—The assessment team must work together to identify the pedigree and quality of information sought. Frequent communications with the assessed organization provided clarifications and context.

- **source documentation**—In our experience, comprehensive policies must stand behind each organizational procedure, or too often it will not get completed. The assessment

should seek to advise on improving source documentation to avoid reliance on culture as a guide to day-to-day activities.

- **terms and conditions**—Each assessment will likely involve an exchange of a substantial amount of information. This means that agreements must spell out specifics, such as whether information can be shared and the terms and conditions for sharing it. There may also be consideration if the information be shared in a safe environment.

- **pedigree of information**—during assessment development, organizations should consider whether information may be collected through attestation or validation. Attestation involves subject matter experts declaring the existence of a practice, while validation would demand evidentiary proof of practice. Attestation may enable a quicker assessment with less strain on the workforce, while rigorous validation may take longer for collection. However, validation may provide greater efficacy and understanding of policy implementation.

In general, these lessons learned can be applied to the development of any assessment, not just one about ransomware. Similar relevant assessments for development could include zero trust architecture, mobile devices, and cloud implementation.

Going Beyond Ransomware

Ransomware represents one of the premiere threats to critical infrastructure. Recent events, such as the attack on the Colonial Pipeline, brought the threat of ransomware and its impact on critical infrastructure to the forefront of concerns for our nation's security.

While most CERT assessments focus on generalized cyber ecosystem review, the suggestion of developing a ransomware assessment is different in that it focuses on a specific form of attack rather than a type of asset. Ransomware attacks are common enough that in building the assessment, organizations may be able to draw upon fundamental gaps that may be exploited by other attack vectors.

Like all things in risk management, assessment development has an iterative lifecycle. Organizations must constantly work to improve their methodology in the wake of new assessment opportunities.

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0901

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu