Ransomware: Assessing Defense and Resilience Strategies

Brett Tucker

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

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.

DM22-0903

Agenda

- Background
- Establishing Goals and Objectives
- Selecting Methodologies
- Domains for Consideration
- Assessment Logistics
- Scoring
- Piloting

Carnegie Mellon University (CMU)

Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
  - #1 in computer engineering, AI, cybersecurity, and software engineering
  - #2 in overall computer science
  - #3 in data analytics/science

CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

The CERT Division: Birthplace of Cybersecurity

Trusted
Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued
Collaborating with military, industry, and academia globally to innovate solutions

Relevant
Achieving technology and talent results for our mission partners

History: Burning Platform for Development

As of 2021, assessment deemed necessary to address Ransomware threat(s) so prevalent in recent years

- Ransomware damages may exceed $30B worldwide in 2023
- Half of the reported breaches began with stolen credentials in 2022
- Majority of attacks were through phishing emails
  - Source: White-Paper-Acronis-Cyber-Protect-Cloud-Cyberthreats-Report-Mid-year-2022-EN-US-220811.pdf

What can be done?

- Leverage known frameworks to protect against ransomware actors
- Develop novel means to assess organizational readiness
- Prioritize most adversary-disrupting controls

Goals and Objectives of a Ransomware Assessment

Measure and drive action from stakeholders in two ways

- Reduce susceptibility to attacks
- Raise the resilience of an organization for recoverability

Assessment must support technical exchange to achieve:

- Risk identification
  - Measure impact to assist in prioritization
- Recommend responses for mitigation
  - Must be scaled to the capability of the organization

Try to use efficient and iterative development cycle and leveraged existing capabilities

Pilots highly desired for lessons learned to evolve maturity

Cyber Essentials, MITRE ATT&CK, CSA STAR, etc.

Sources:

[MITRE ATT&CK®]

[Home | CSA (cloudsecurityalliance.org)]

[Cyber Essentials | CISA]

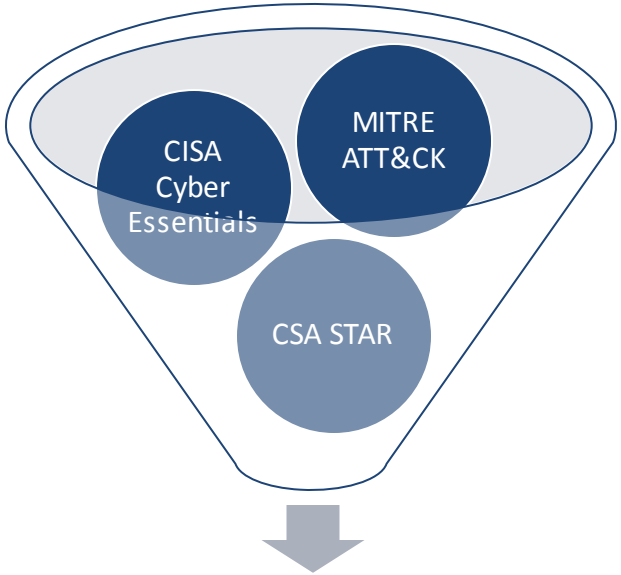
Taking the Best from Several Places

Best practices must prevail

- Diverse resources with varied focus helps
- Assessment may remain the same, but the solutions may not

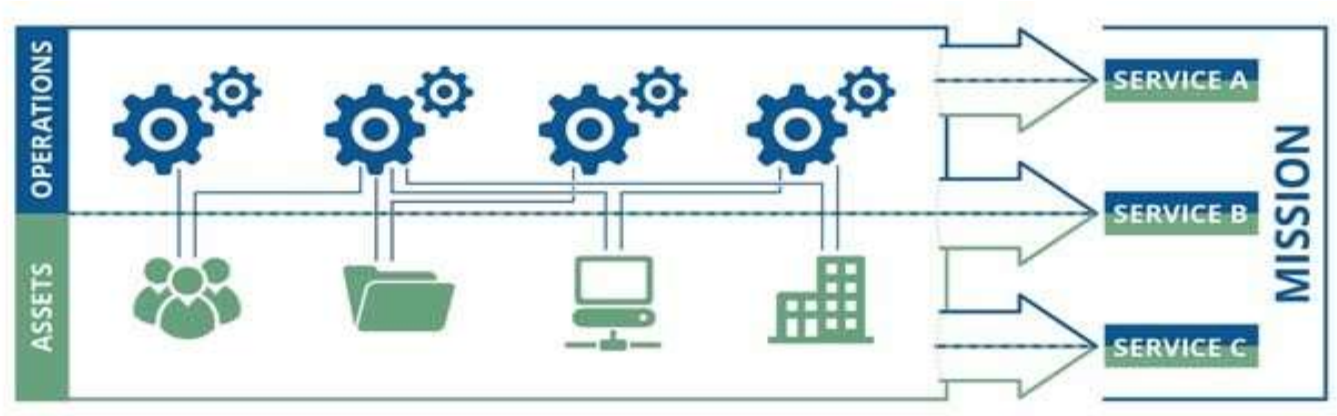
Other sources of help exist

- Trusted advisors
- Cyber insurance
- Other assessments



Tailored to Scope and Needs of the Customer Set

Link Cybersecurity to Business Objectives



People: those who operate and monitor the service
Information: data associated with the service
Technology: tools and equipment that automate and support the service
Facilities: where the service is performed
External Dependencies: value gained from relationships/supply chain

! Assets derive their value from their importance in meeting the service mission.

Domains to Consider

8 Domains with sub-categorical areas of assessment:

- **Business Continuity/Disaster Recovery**: back-up systems, incident response, and back-up testing
- **Configuration Management**: allow/block lists, baselines, restricting permissions, limits to installations, and registry permissions
- **Endpoint Protections**: anti-virus, IPS, and web content control
- **Identity Access Management**: MFA, least privilege enforcement, password management, and user/privileged account management

Domains Considered - 2

- 8 Domains with sub-categorical areas of assessment:

  - **Incident Management**: event reporting and escalation

  - **Network Protection**: access limitations (e.g., RDP), email management, and network segmentation

  - **Risk Management**: insurance and user training

  - **Vulnerability Management**: software updates, vulnerability scanning, audit,

Think Through Team Composition and Process

Primary roles could include an assessment lead, subject matter experts, and administrative support

Preparation could take ~10 days – this would include initial notice, initial meetings, scope planning, and kick-off

Duration with customer, around 1 day or 2 days if disrupted and not prepared, large organization

- This time will account for the actual on-site facilitated discussions

Report writing duration, post assessment, 10 - 15 days

- This includes analysis, drafting, coordination, and technical editing

Total duration = 23 - 28 days per entity

The Risks Related to the Assumptions Made Here are Mitigated by Providing a Range of Possible Durations for the Reviews

Attack Vectors and Scoring

Attack vectors for ransomware may include:

- Exploit public-facing application
- Stolen credentials
- Phishing
- Ransomware encryption of data impacting operations

Each domain contains capabilities that can be rated as “Fully Implemented”, “Partially Implemented”, and “Not Implemented”.

Capabilities could be correlated to Basic, Intermediate, and Advanced practices.

- Must consider the scope, scale, industrial sector, and size of customer set

Degree of alignment with best practices could translate to a level of susceptibility – “Highly Susceptible”, “Susceptible”, and “Resistant”

Lessons Learned from Pilots

- Establishing scope boundaries can be challenging
- Terms and conditions may need to be negotiated
  - Standard set of terms and conditions developed
- Customer operational tempo greatly influences progress
- Pedigree and quality of demonstrable evidence is variable
  - Analysts must scrutinize until baseline of standards can be made
- Source documentation can be vague or non-existent
  - Technical Exchange Meeting (TEM) may require additional time

Key Takeaways in Summary

Prioritize

- Set priorities and remember that if everything is the priority, then nothing is priority.
- Not all threats, vulnerabilities, and assets are equal—analyze and measure where possible.
- Select the most cost-effective controls to conserve resources.
- Strategies vary based upon confidentiality, integrity, and availability.

Specialize

- Know your enemy and your environment.
- Target high frequency vectors like spear phishing and ransomware.
- Tailor your security program to your organizational strategy.
- Demand an implementation roadmap.

Engage with Us

Download [software and tools]

Participate in [education] offerings

Attend an [event]

Search the [digital library]

Read the [SEI Year in Review]

Explore our [research and capabilities]

[Collaborate] with the SEI on a new project

Contact Us

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479
info@sei.cmu.edu
www.sei.cmu.edu

Brett Tucker, PMP, CSSBB, CISSP, CAP
Technical Manager, Cyber Risk Management
412.268.6682
batucker@cert.org