

RANSOMWARE VULNERABILITY & RECOVERABILITY ASSESSMENT

Every ransomware attack has one target: data. Early ransomware attacks focused on denying organizations access to their data by locking down systems internally. As security improved, attackers upped the ante by exfiltrating data with threats of public exposure. Without access to data, most organizations can't continue day-to-day operations. Attackers take full advantage of this pain point to gain faster submission and larger ransomware payments from their targets. With ransomware attacks on the rise, how secure is your organization against today's sophisticated attacks, and do you have the capabilities to recover if you are breached?

COMPREHENSIVE, INTEGRATED PROTECTION

Vulnerable networks are fertile ground for malicious data exfiltration, and current data recovery practices often fall short in the face of a ransomware attack. Your enterprise security program should include security measures to prevent a ransomware attack, and recovery processes that quickly return your business to full operation if an attack does occur.

The Sirius Ransomware Vulnerability & Recoverability Assessment is a purpose-driven engagement that provides a comprehensive review of your enterprise environment's data protection (including IBM Z®), your security programs and controls, as well as your networks, applications (on-prem and cloud, including Microsoft 365® and Office 365®) and data. Areas of ransomware risk are identified and remediation methods are recommended. Sirius applies review and recommendations based on the frameworks of the Common Vulnerability Scoring System (CVSS), the Capability Maturity Model Integration (CMMI), and NIST SP 1800-25/26. For mainframe environments, our dedicated IBM Z security experts offer corresponding solutions focused on the platform's unique architectural, security and software requirements.

FOCUS IS ON THESE AREAS

- Identification of potential areas of exposure
- Evaluation of existing recovery capabilities
- Development of a remediation plan that mitigates liability and exposure
- Validation of best practices for recoverability using multi-layered security and hardening of your data protection solution

BENEFITS

- Gain an objective analysis and receive a grade of your current ransomware susceptibility and ability to recover based on industry-endorsed frameworks.
- Receive reports for stakeholders that outline the potential cost and impact of a ransomware attack on your organization.
- Understand your current recovery capabilities in the event of an attack and learn methods and best practices for recovery, including the role of cloud-sourced backups.
- Get prioritized guidance on gaps, risk and liabilities that can be addressed to reduce risk and improve recovery capabilities at an enterprise level.
- Learn some of the key security controls that insurers may use to calculate your cybersecurity insurance premiums. Some insurers subsidize the cost of this assessment for their customers.

THE RANSOMWARE LANDSCAPE

- Ransomware remains the most prominent malware threat, with attacks estimated to occur every 11 seconds and malicious emails up 600% during the 2020 pandemic.
- Forecasts call for ransomware costs to reach \$20B by the end of 2021. Individual ransom payments averaged \$200,000 in 2020.
- 50% of surveyed security professionals do not believe their organization is properly prepared to stave off or recover from a ransomware attack.
- No industry or organization is outside of the target zone for attackers. Small to midsize businesses, healthcare, financial, education, utilities and infrastructure, and city and local governments have all been breached.

WHY SIRIUS

Sirius draws on decades of experience from across the IT spectrum to help you focus on what's valuable, move protection closer to the point of risk, and adapt your security practices to meet current threats.

We help to advance your security program and optimize your overall IT risk management strategy so you can protect your data, your intellectual property, and your brand.

TIMELINE AND PRICING

Sirius scopes and executes this assessment based on the number of systems and domain objects included. We also provide custom pricing for larger engagements.

Size	Systems	Domain Objects	Backup Attributes	Duration	Price
Small	1,000 or less	Up to 100,000	1 data protection product and/or 2 sites	2 - 4 weeks	\$50,000
Medium	2,500 or less	Up to 250,000	2 data protection products and/or 5 sites	4 - 6 weeks	\$90,000
Large	5,000 or less	Up to 500,000	3 data protection products and/or 8 sites	6 - 8 weeks	\$130,000
Custom	Over 5,000	Over 500,000	Over 3 data protection products and/or 8 sites	8 weeks or more	Varies

At an additional cost, Sirius' dedicated IBM Z security consultants will perform a comprehensive vulnerability and recoverability assessment for each production security database (IBM® RACF®, CA® ACF2®, CA Top Secret®) in combination with each production environment running on IBM Z.

Cost per Security Database and Production Environment	Duration	Price
First security database + production environment	2 - 4 weeks	\$50,000
Each additional security database + production environment	2 - 4 weeks	\$30,000

WHAT TO EXPECT

Each engagement is unique to the client, but the following process provides the general idea of how the assessment has been conducted in numerous client engagements:

1. Set up an introductory call with all involved parties to review the plan and expected outcomes.
2. Schedule discovery meetings as needed with identified participants and stakeholders.
3. Gather all materials and determine any gaps in needed information.
4. Produce a list of key findings.
5. Present the results and takeaways of the assessment to executive sponsors.

DELIVERABLES

Sirius will create and present your customized deliverables at the conclusion of your engagement:

- Risk/maturity grade based on security frameworks
- Heat map of high-priority exposures and recommended steps for remediation
- Identification of data protection deficiencies that could inhibit recovery

For more information, please contact your Sirius client executive, visit siriuscom.com, or call 800-460-1237.

