From: Continuity Software, Inc., Doron Pinhas

Proposal: 1550 (RIN 7100--AE-61) (Ver 1)- Enhanced Cyber Risk Management Standards

Subject: Enhanced Cyber Risk Management Standards

Comments:

Date:Jan 16, 2017

Proposal:Enhanced Cyber Risk Management Standards [R-1550]
Document ID: R-1550
Revision: 1
First name: Doron
Middle initial:
Last name: Pinhas
Affiliation (if any):
Affiliation Type: Commercial (Com)
Address line 1: 5 Penn Plaza
Address line 2: 23rd Floor
City: New York
State: New York
Zip: 10001
Country: UNITED STATES
Postal (if outside the U.S.):
Your comment:

This public comment refers mainly to questions 29 & 36 of the joint advance notice of proposed rulemaking for Enhanced Cyber Risk Management Standards.

Continuity Software has been helping dozens of financial service companies - including five (5) of the largest financial institutions in the United States - to avoid unplanned critical IT outages and data loss incidents by applying a proactive process based on automated infrastructure resilience validation. At Continuity Software, we view resilience as a combination of an entity's ability to detect, respond, and recover from a disruption. The following comments represent a summary of our expertise and knowledge, accumulated over years of experience in the system configuration recovery and data protection and recovery disciplines. Our feedback below is limited to these two areas.

36. What methodologies should the agencies consider for the purpose of measuring inherent and residual cyber risk quantitatively and qualitatively? What risk factors should agencies consider incorporating into the measurement of inherent risk? How should the risk factors be consistently measured and weighted?

Enhanced standards are needed in order to increase operational resilience and reduce the potential impact on the financial system in the event of a disruption. One of the objectives of the proposed rulemaking is for sector-critical systems to meet a 2-hour RTO. This obviously requires very quick systems and data recovery. Indeed, to ensure recoverability, appropriate methodologies must be adopted and exercised. Measuring inherent risk is a critical step in the process of increasing operational resilience and ensuring recoverability of financial systems. Another key factor is the ability to apply the measurement (and process) in a proactive and a continuous manner. An annual/bi-annual periodic measurement or testing, which is how most entities measure readiness today, does not provide sufficient indication, because the IT environment is extremely dynamic. In our experience, the frequency of risk measurement and assessment must correspond with the rate of change within the entity's IT systems. Otherwise, the risk level is virtually unknown. Thus, if changes are made on a weekly basis, testing and measurement must also be performed at least every week.

Measuring risk is possible and we know of selected financial institutions that have implemented effective processes to that end. These processes include both evaluating the readiness of their critical systems, and the ability to successfully recover in the event of a failure or cyber-attack. Working with leading financial institutions on ensuring service availability and business continuity, our experience shows that being able to measure risk quantitatively is important in order to increase cyber resilience. The risk management process should be actionable, so that when a deviation is measured, the required remediation actions are easily identified, enabling systems to be quickly brought back into the desired state. In order to measure risk correctly and accurately, granularity must be maintained in three dimensions:

- Risks should be measured on a per-application and application-component basis
- Risks for data recoverability and for systems recoverability should be measured independently
- Risk must be measured over time

As described in the proposed rulemaking, cyber resilience includes several different categories that should be quantified. The ability to provide both cyber resilience and accurate measurement lies in the ability to fully understand the entity's SLAs, standards, and processes, and the ability to compare them with the actual infrastructure elements and environment. As mentioned above, segmented measurement by business entities (applications) and criticality tiers is crucial, and on top of that, the agencies should apply aggregative scoring. Measuring risk and cyber resilience over time is needed in order to identify trends and track improvement. The following metrics are commonly used by state-of-the-art enterprises:

1. Data recoverability and safety

These metrics check and quantify whether the application data is protected, as required by the standards for the criticality of the system. This allows entities to determine if all data is backed up as needed, in order to ensure cyber resilience, and more specifically, recoverability. These metrics should answer questions such as: Is sufficient copy frequency being maintained (in particular, to meet the required RPOs)? Is the data retention period sufficient? Are copies adequately isolated from tampering and alteration by unauthorized individuals? Are copies kept in an appropriate geo-distribution?

2. Availability of recovery infrastructure

This metric should address the following question: Does a recovery infrastructure exist? If so, how much capacity and performance does it allow after recovery, compared with normal operations? (Capacity and performance could be measured either in transaction volume and speed; or in network, compute and data storage).

3. Currency of the recovery infrastructure

How current is the configuration of the recovery infrastructure? It is important to make sure that the configuration can be recovered to the same point in time as that of the data. Otherwise, a successful system restore might not be possible.

29. The agencies request comment on the appropriateness and feasibility of establishing a two-hour RTO for all sector-critical systems. What would be the incremental costs to covered entities of moving toward a two-hour RTO objective for these systems?

The two-hour RTO is an ambitious objective, but our experience indicates that it is possible when the right architecture is implemented and coupled with the appropriate testing and recovery processes.

The incremental cost could be significantly higher in certain dimensions, and marginally higher in others. Compute infrastructure costs would likely not be affected significantly &ndash; as most systems impacted by the proposed rulemaking are already designed with appropriate levels of redundancy (High Availability and Disaster Recovery). Data protection costs may be more significantly impacted due to the need to implement new technologies for data copy management that can guarantee the required SLAs. A higher impact would probably be incurred on operational costs due to the need to significantly increase testing and auditing frequency. Finally, there should be significant one-time costs in order to define and manage new processes and methodologies which can also include the need to train employees and partners. Another incremental cost will go to re-architect specific IT components and revise existing IT design-patterns.

Regards,
Doron Pinhas
Chief Technology Officer
Continuity Software, Inc.
Tel: 646.216.8628
DoronP@ContinuitySoftware.com
www.continuitysoftware.com