Exercise a System Recovery Plan

Catastrophic Loss

In 2015, a carefully-orchestrated nation state-level attack targeted power distribution systems in Ukraine causing more than 230,000 people to lose electrical power. While control centers were not fully operational for two months, the situation could have been much worse: the companies' manual backup functionality allowed operators to restore power in only a matter of hours [1].

The city of Atlanta was not so lucky. In March 2018, the city fell victim to a cyberattack employing SamSam ransomware, which encrypted files and locked the city's computer systems—blocking much needed access to services and portals—and forced the city back into the era of handwritten reports and carbon copies. Years of valuable files and data were lost [2]. Roughly six million people call metropolitan Atlanta home and rely on its services. The city requested $9.5 million to aid in recovery from the ransomware, and the aftershocks would be felt for some time: three months later, in June of 2018, an estimated third of the city's affected software programs remained hobbled, some of them completely offline [2], [3], [4].

There is some good news: a 2017 report from Datto, Inc. found that 96% of small-to-mid-sized businesses were able to fully recover from a ransomware infection with use of a reliable backup and disaster recovery solution [5]. Regardless of the cause of data or system loss, organizations must be prepared in order to quickly recover to full operations.

Information systems are vital elements of most modern day organizations; it is imperative that those services and functions remain intact or recoverable in the face of disaster. By implementing a System Recovery Plan (SRP), organizations can prepare for disruptions stemming from natural disasters, technological failures, user errors, and malicious actions, and minimize the impact to their operations. System Recovery Plans are a valuable method of ensuring quick and effective restoration of system functionality, including data and configuration. About 70% of professionals have or will experience data loss due to accidental deletion, disk or system failure, viruses, fire, or some other disaster. And 60% of companies that lose a significant amount of their data will shut down within six months of the disaster [6].

The System Recovery Plan

A System Recovery Plan is a proactive, coordinated strategy that enables the recovery of information systems, operations, and data after a disruption. An SRP provides key information needed for system recovery which includes roles and responsibilities, inventory information, assessment methods, detailed recovery procedures and system testing.

An SRP is an integral part of an overall information system contingency plan (ISCP), mandated for all federal organizations by the Federal Information Security Modernization Act (FISMA) of 2002 and amended by the Federal Information Security Modernization Act of 2014. In addition to more tangible benefits, implementing an SRP helps assure compliance under FISMA [7]. Detailed requirements and recommendations for an ISCP can be found in NIST publication SP 800-184 and SP 800-34 Rev. 1 [8], [9].

Lifecycle

This section describes the process for creating and maintaining a useful SRP. The process is general to all information systems and should be modified and tailored to each organization implementing the plan.

Develop the Contingency Plan Policy Statement

This statement describes how the SRP aligns with the objectives of the organization. Key policy elements include roles and responsibilities; scope, as it applies to common platform types and enterprise functions; resource requirements; training requirements; exercise and testing schedules; plan maintenance schedule; and minimum frequency of backups and storage of backup media.

Conduct a Business Impact Analysis

The Business Impact Analysis (BIA) relates the organization's critical processes to the consequences resulting from disruption of those processes. Three core steps are involved in performing the BIA:

1. Determine business processes and recovery criticality
2. Identify resource requirements
3. Identify system resource recovery priorities

Identify preventive controls

Mitigating or eliminating the effects of physical outages through preventative measures can greatly reduce impacts to the system. Some common measures that may be applied are appropriately sized uninterruptible power supplies, generators to provide long term backup power, cooling systems with capacity to prevent failure of components, fire suppression systems, fire and smoke detectors, and water sensors. Redundancy should be integrated at all levels of the system to prevent system outages. Devices such as authentication servers, routers, and switches often have high availability functionality which can be enabled to provide automated failover.

In recent years, ransomware has proliferated to epidemic proportions, and countless variants affect most major classes of computing platforms, including servers, workstations, mobile devices, and industrial control systems, among others. Some restore systems upon payment of demands, while others will not. Many are capable of infecting or corrupting common backup technologies, irrespective of their physical locations, making offline backups of critical data, software, and services absolutely essential. Since offline backups are much more difficult to perform, they should generally be reserved as a "last line of defense" against the most catastrophic of losses.

In general, when it comes to ransomware, an ounce of prevention is worth a pound of cure. Recovery often requires wiping a system and starting over. The development of an SRP should inform the prioritization of common defenses, including hunting activities[1] and the enforcement of signed software policies[2] or application whitelists. If a system is critical to the organization, preventing unknown software from running on it is typically the best way to stop ransomware.

Create contingency strategies

Contingency strategies cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance. Systems should be backed up regularly and policies should detail the minimum frequency and scope of backups in addition to the location of stored data. Backup and recovery strategies address how to restore operations quickly and effectively during both planned and unplanned downtimes.

Data is not the only thing that an organization must back up. Some organizations depend on critical physical processes that could be effected by the corruption of non-traditional computing platforms like programmable logic controllers (PLCs). For these organizations, having physical replacements for certain components and "gold copies" of their configurations on hand may be the best option. For no-fail items, like generators, medical devices, and weapon systems, having spare components is always essential.

Plan Testing, Training, and Exercises

A Testing, Training, and Exercises (TT&E) program defines methods for determining, scheduling, and setting objectives for TT&E activities. Testing allows for detection of any faults in the recovery plan. Training instills confidence in personnel's ability to perform their roles and responsibilities during recovery. Exercises simulate an unplanned outage, enabling personnel to practice their recovery skills and to uncover any gaps in the SRP.

Complete guidance on creating a TT&E program can be found in NIST SP 800-84 [10].

---

[1] For more information on threat hunting, refer to "Continuously Hunt for Network Intrusions", part of the *NSA Cybersecurity Top 10 Mitigations.*

[2] For more information on signed software policies, refer to "Enforce Signed Software Execution Policies," part of the *NSA Cybersecurity Top 10 Mitigations.*

Plan maintenance

The SRP must be maintained in order to reflect the current status of requirements, procedures, and policies as well as any changes in the environment. To maintain the SRP, it should be reviewed for accuracy at a defined frequency or whenever significant changes are made.

Cloud considerations

Network security administrators have additional considerations when exercising system recovery for networks hosted in the cloud. When utilizing cloud services, negotiate a service agreement containing contractual language that clearly delineates the recovery responsibilities between the cloud service provider and the cloud consumer. If an agreement is not made, the consumer should assume recovery responsibilities in the event of a disaster. Even if the provider assumes recovery responsibilities, the consumer should have a backup recovery plan in the event that the provider's recovery process fails. In either case, the SRP still needs TT&E to ensure proper recovery in the cloud environment.

Network security administrators can also outsource the entire system recovery process for certain types of failures to cloud service providers using Disaster Recovery-as-a-Service (DRaaS). While DRaaS saves time and resources that would otherwise be spent on certain parts of in-house system recovery planning, network security administrators must still prepare their network to be able to recover critical functions in the event that the DRaaS fails.

Deciding to automate

While countless benefits come from automating many business processes, an organization pursuing automation should carefully consider how it will operate in the case of a loss of computing services. When automating processes, ensure recovery plans are documented. Manual processes may be essential as a temporary alternative option.

Bounce back confidently

Networks are never fully protected from threats and failures. Network security administrators must exercise a system recovery plan to use as the next mitigation when network resources are lost. SRPs incorporate people, policies, and procedures needed to provide critical information and coordination for networks to return to normal operations after a catastrophic event. By using both in-house and cloud recovery options, enterprises can achieve cost and resource savings by reducing the impact to business operations and avoiding the extra manpower that would otherwise be required to rebuild lost network hosts and services. The system recovery plan, along with its essential testing, training, and exercises, will instill resilience into enterprise networks and enable them to maintain critical operations while bouncing-back from adverse events with an efficient recovery.

Works Cited

[1] K. Zetter. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, 2016 March 3. [Online] Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[2] L. Kearney. "Atlanta Officials Reveal Worsening Effects of Cyber Attack." Reuters, 2018 June 6. [Online] Available: https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-iduskcn1j231m

[3] L. Hay Newman. "Atlanta Spent $2.6m to Recover From a $52,000 Ransomware Scare." Wired, 2018 April 23. [Online] Available: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[4] M. Niesse. "Census: Metro Atlanta's population approaches 5.8 million." Atlanta Journal Constitution, 2017 April 10. [Online] Available: https://www.ajc.com/news/local-govt--politics/census-metro-atlanta-population-approaches-million/1pxspbryl6l26zn4jq

[5] "Global State of the Channel Ransomware Report 2017." Datto, 2017. [Online] Available: https://www.datto.com/resources/ch-ransomware-survey-17/

[6] "With the Bigger Dangers of Data Loss and Some statistics, the Value of Backups is Becoming Prominent." International Data Group & Boston Computing Network's Data Loss Statistics, 2018 April 29. [Online] Available: https://www.cso.com.au/mediareleases/31466/with-the-bigger-dangers-of-data-loss-and-some/

[7] Federal Information Security Modernization Act (FISMA). [Online] Available: https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA

[8] M. Bartock, et al. "Guide for Cybersecurity Event Recovery." NIST, SP 800-184, 2016 December. [Online] Available: https://csrc.nist.gov/publications/detail/sp/800-184/final

[9] M. Swanson, et al. "Contingency Planning Guide for Federal Information Systems." NIST, SP 800-34 Rev. 1, 2010 May. [Online] Available: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

[10] T. Grance, et al. "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities." NIST, SP 800-84, 2006 September. [Online] Available: https://csrc.nist.gov/publications/detail/sp/800-84/final

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov