Cybersecurity Recovery Planning as Part of Disaster Recovery Planning

Introduction

Disaster recovery and cybersecurity recovery planning are not one in the same. Disaster recovery's primary goal is to provide business continuity after a major disruption from man-made or natural causes. The goal of cybersecurity recovery, on the other hand, is to protect and recover data assets and software systems after a data breach.

Given the dramatic rise in cyber crime, it is reasonable to assume that any given enterprise will eventually be successfully attacked. Focusing on prevention only and not on documenting and testing a recovery plan from such an attack is therefore not the best strategy. The best approach is to plan for all possible cyber events, their containment and the recovery planning, to fully restore operations.

Creating an Effective Cybersecurity Recovery Plan

Additional goals for your cybersecurity recovery efforts may include: restoring systems using alternate methods like the public cloud; performing standard operating procedures in alternate ways; and recovering information systems in physically-separate locations. When formulating a cybersecurity recovery plan, the following steps should be pursued.

Identify which Data Sets and Software Systems are the Most Critical

The first step involves identifying which data sets and software systems are the most critical for the enterprise. After doing so, document the employees who have access to those tools and data and at which access level. Authorization controls should be reviewed on an on-going basis to ensure only a minimum number of employees are authorized and have the appropriate level of access. Identify the mitigation steps to be taken in each case and the probable time delay to restore data and systems. If third parties are involved, their point of contact should be identified and maintained up-to-date.

Implement a Layered Protection Approach

Adopt a layered protection approach when developing the enterprise cybersecurity recovery plan. This means adopting a multi-pronged strategy that includes:

- Preventive elements such as advanced firewall capabilities with content inspection and antivirus software to block vulnerabilities, exploits and viruses;
- Implementing a strict software change control process including timely patch management;
- Strict access control and audits on activities to prevent compromised data or services, through Intrusion Detection Systems (IDS) or equivalent;
- Firewalling, local anti-virus, and malware protection on business service compute and storage elements;
- Implement an on-going third party/supply chain threat analysis to ensure the enterprise is not inadvertently sourcing malware, ransomware, viruses, etc.
- Configure the environment so that successful backups can be made that support the ability to recover.

It should be noted that AWS S3, Azure Blob, Google Object Storage and other cloud-hosted object storage is often immutable, or unable to be changed over time, or can be marked as such. Therefore, cloud backups can be seen as a “golden copy” repository due to their cloud security protocols and the integration of cloud immutable storage. They can be made immune to ransomware attacks, *as long as the source data is clean.*

Full backups should be made into cloud storage, as incremental delta archives (overwriting old data) may end up with mixed encrypted and unencrypted payloads. An alternative approach is to implement a versioning-based approach, which can be of benefit. The recommendation is not to replicate the back-up tactics normally used on premise as cloud storage provides alternate protections and requires new strategies.

In addition, when restoring to clean deployments it is far easier to provision in the cloud than on premise.

Plan for the Recovery Phase

Perform a business impact analysis to evaluate potential effects and to establish priorities, including financial, legal, regulatory, etc. of cyber events on the enterprise. With these priorities in mind:

- Define the incident management roles and responsibilities for implicated staff;
- Develop a comprehensive communications plan, identifying distribution, cadence and degree of detail. Determine in advance if and when the event will be publicly communicated;
- Identify alternate services and/or physically-diverse facilities for data and software systems, including cloud and other third-party services;
- Identify and fix gaps in crisis planning before an incident occurs through simulations or exercises, like table-top exercises;

Document any other ramifications of a breach including how staff, customers and other stakeholders will be affected and any legal, financial or regulatory implications.

Update Plans Frequently and Improve

The enterprise should update its cybersecurity recovery plan regularly based on the current threat landscape, best practices and lessons learned from simulation exercises or similar breaches.

Periodically test and evaluate the cybersecurity recovery plan and update where needed. After a breach, address any issues not addressed in the plan and address any vulnerabilities and issues with the plan for more comprehensive results.

Track the Success of Recovery Metrics

Use real metrics to evaluate the success of the cybersecurity recovery plan, including, as examples:

- Actual patch policy compliance, specifically average time delay to patch;
- Actual mean-time to incident discovery and incident recovery;
- Actual mean-time between security incidents;
- Number of known vulnerability instances and mean-time to mitigate and recover;
- Number of applications and percentage of which are critical applications;

Documentation

Procedures, roles and responsibilities, metrics tracking, and adjustments should be fully documented for improved response times and recovery. This includes:

- Develop diagrams of infrastructure and equipment;
- Maintain a comprehensive assets and systems inventory, including copies of any third-party agreements. Keep the inventory up-to-date;
- Document all application dependencies, inter-dependencies and prioritization. Prioritize restoring applications in order of most critical;
- Document any regulatory compliance requirements, including the need to inform regulatory bodies;
- Document recovery team members including their contact information and maintain this information up-to-date.

Next Steps

Disaster recovery and cybersecurity recovery planning are both essential tools to protect the enterprise in today's increasingly hostile cyber environment. A well-documented and exercised cybersecurity recovery plan will result in the enterprise recovering more effectively from a successful cyber attack.

September 1, 2021