Business Continuity and Disaster Recovery Plan Scenario by Gerald Blackmon

2/24/2022

Prompt:
An organization, MyFoneApp Inc., supplies mobile phone services including applications for storing photos, video conferencing, and email. MyFoneApp Inc. has two office locations, in New York, NY and Phoenix, AZ, as well as third-party data centers in Tempe, AZ, Ausn, TX, and Roanoke, VA. The photo storage app, MyPhotoApp, stores all of its data in AWS in S3 buckets. Personnel work primarily from laptops in the office locations although some employees work remotely full-me. Call center personnel work out of the Phoenix office and top management primarily operates out of the New York Office. The Director of Infrastructure Operations has paired with the organization's Facilities Managers to develop a business continuity program (BCP). They have engaged you, as a consultant, to gain an understanding of their environment, provide them guidance on the documentation they would need to create, and advise them on the best way to implement their BCP.

1. List at least three (3) documents that the organization would need to maintain as part of their
business continuity program:

2. Create an outline (4-5 lines) of what the contents of one (1) of these documents would be:

3. Recommend at least three (3) technical controls that would support MyFoneApp Inc.'s business continuity processes:security awareness training. Background checks NDA backups testing. Infrastructure as code work from home accessibility. Generators for power loss

4. Express, in a short paragraph, a few of the primary risks to business operations that MyFoneApp Inc. is likely to face

Documents

The documents needed to assist in an efficient Business Continuity Plan (BCP) include, but are not limited to:

1. List of Company Personnel and Responsibilities. This will include the management lists, how they can be contacted and their responsibilities in an emergency
2. List of Company Assets. This will provide a prioritized list of company hardware, functions, and data.
3. List of Company Data. This will provide a listing of data contents, how it is backed up regularly and how to access it.
4. Operational Procedures to Recover Service (sometimes called a playbook). This will detail each of the measures taken by each member of the Business Continuity Plan Recovery Team. This plan is designed to be rehearsed and implemented during crisis situations. For this reason, the steps listed within must be followed with the highest degree of efficiency to ensure a quick and seamless recovery.

OBJECTIVES

The fundamental components of a business continuity plan must include workspace recovery, cyber resilience, change management, and several other elements. Additionally, sharing a business continuity plan with the essential personnel and educating them on how to handle disasters is another vital component. The ISO 22301 offers a reliable source of guidelines and standards to develop a Business Continuity Disaster Recovery (BCDR) plan.

1. Recovery personnel

Assign a dedicated person to manage the process and assemble a team comprising a member of each critical business department within the organization. There should also be a chain of command and assigned responsibilities; who is doing what, where, when and how, as well as where the relevant participants can be reached.

2. Recovery procedure

The recovery procedure is that part of the BCP that outlines the strategies for business functionality. This strategy should identify and prioritize critical business assets such as equipment, the IT system (including network diagrams), contact lists, etc. In order to ensure your BCP is capable of protecting these assets, identify the potential risks and threats to those assets and compile a system that will assist you in recovering from a critical event or natural disaster.

3. Data backup

Implement a proper backup strategy as part of your BCP. There are two types of backups that you must consider when designing your backup strategy: on-site backup and off-site backup. On-site can use tape drives, external hard drives and are easier to access than off-site backup. Off-site backup and the need for it may mitigate risks based on disasters which center within certain geographic regions such as natural disasters or power outages. You should furthermore include the following company documents in your backup plan: financial documentation (such as bank statements, tax records etc.), a list of fixed assets and legal documents such as copies of agreements, policies, memoranda of understanding, insurance documents, etc.

Technical Recommendations

Regular testing of backup assets must be followed as part of the BCP in order to ensure that the plan can be effective. Quarterly or annual tests of isolated to full systems review may be alternated.

Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and

employees understand the role they play in helping to combat information security breaches.

Battery backups as well as emergency generators may be implemented in order to offer a short term failsafe in the event of power loss. Backup options provided here are offered as a way to offset the risks of data loss as well as lost accessibility to MyFoneApp. The following options are provided on a scale of most effective and costly vs least effective and costly measures.

1. The “Hot Server” option will allow data to be stored, accessed, and available in a redundant system which remains running and distributed by Load Balanced access. This would direct customers and employees evenly to either site. In the event that one server location is affected, the other site assumes the workload of both until remediation efforts can be concluded. This option offers the best protection and functionality at a higher cost. It can even offer increased availability during peak usage periods since it runs at the same time.
2. “Warm Site” options encompass the availability to fire up readied backup servers which can be implemented within hours of a loss of service. Some warm site options can be stored locally on hardware provided on-site or we may utilize a separate vendor than Amazon S3 buckets to provide vendor diversity in the event that Amazon in particular suffers a loss of service.
3. Cold Site options are least expensive but would only offer the ability to start operations from a backed up state. This would only require a location to operate with access to adequate power and equipment. This option would be the most cost effective but offer substantial downtime and the possibility of unforseen difficulties due to the lack of practice with running equipment.

Risk Analysis Concerns

Some of the risks that can be observed from the operations described at MyFoneApp are the singular storage of data within Amazon S3 buckets. Even though these are

neatly spread throughout multiple regions, it is not stated that the data stored is a complete collection of all Data in each region. If so, that would be recommended. However, there is also the possibility that a catastrophic event that affects Amazon web servers could be a problem. This could be mitigated by utilizing an additional vendor such as Microsoft Azure or Google Cloud Platform for instance.

There is a concern about management all being centered in New York where employees and call centers are located in Tempe Arizona since the time difference could catch management unavailable. Malicious actors often operate during time periods which offer the best opportunity to catch targets in a less than favorable position to respond. In the case of management for a company that requires 100% available up-time, There must be personnel who are designated to be on-call and easily accessible for any disaster.

A large degree of concern is the available on-call personnel's ability to access the system from where they are at the time of a disaster. In the case that they are working remotely, often service outages can prevent them from responding efficiently. Also, certain new types of risks are apparent. Reliance on personal computers, routers and other devices that could be infected with malware, but are difficult for corporate IT personnel to manage and secure. Another threat in this context is an employee's need to access or send data over public internet connections when connecting to systems or storage resources that exist in their companies' offices. If that data is not properly secured, third parties could eavesdrop on the connections and steal sensitive information in a way that would be much more difficult to do when all data remains inside corporate networks. Remote access is a very convenient feature for employees that must be carefully managed and monitored due to the hazards of Cyberattack. If a remotely connected device were compromised, (lost, hacked, etc.) access to company systems could be controlled by a malicious actor. Measures to prevent compromised remote devices from accessing the network must be implemented.

Threats that are present in traditional work environments can be exploited in new ways from work-from-home settings. For example, phishing attacks are not a unique risk for

employees who work remotely, but they may be easier to execute when employees are out of the office, less cognizant of threats and using personal devices to connect to corporate resources.

Malware attacks pose a greater risk when employees are working from personal devices whose software is less likely to be patched against the most recent security threats than they would be if they were working from company-owned devices that are centrally managed and updated by a professional IT team.

Although remote work may be beneficial or necessary for a company to carry out its operations, it's apparent that one of the major tradeoffs is the inherent security risks it carries. Fortunately, companies can manage these risks by adhering to best practices for keeping their systems and data secure even when employees are working from outside the office. The following considerations and steps must be made.

1) Assume threats will occur

The most basic best practice for securing remote access is to accept that threats exist.

This can be a difficult mindset to acknowledge, especially for companies that do a good job of securing their on-premises infrastructure. It can also be tempting to ignore the security risks of remote-access setups because there is less visibility into the systems that employees use when working from home, and therefore less opportunity to identify the risks.

Nonetheless, the reality is that vulnerabilities almost certainly exist within the infrastructure and applications that employees use to work remotely. IT teams should assume that those risks are present, even if they can't see them.

2) Create a telework policy

Setting clear rules to govern how employees work remotely is another basic step toward managing remote access threats. We should develop telework policies that specify items such as:

- Whether employees are allowed to use personal devices when working remotely.
- Which data employees can download to personal devices, and which needs to stay in the office.
- Whether employees are allowed to install non-work related software on devices that they use for remote access.
- How employees should report suspected attacks when they are working remotely and unable to interact with the IT team in person

Guidance such as this goes a long way toward mitigating the security risks associated with remote access systems.

3) Encrypt sensitive information

Data encryption is always a best practice from a security standpoint. But it is even more critical when employees work remotely, due to the risk that devices could be lost when being used outside of a corporate setting or that sensitive data could be intercepted while traveling over the internet.

Toward that end, be sure that all data exchanged between company-owned systems and remote work locations is encrypted while it travels over the network. A simple way to do this is to require employees to connect to remote systems using VPNs, which provide built-in encryption. Ensuring that remote-access tools like RDP clients are up to date is important as well because outdated clients may not encrypt data by default.

4) Designate and secure specific remote work devices

Ideally, employees will not use personal devices when working remotely, and policy should dictate as such. In the MyFoneApp case this was not mentioned. Companies should instead provide employees with specific devices to use for remote work. Those devices should be managed by the corporate IT team to ensure that they are properly updated and do not contain any unnecessary software or data that could pose a security risk.

5) Employ user authentication

When accessing company resources remotely, employees should be subject to strict access control, including multi factor authentication. Although it may be tempting to make resources like file servers accessible to anyone in order to simplify access, this is a major security risk. Instead, a best practice is to adopt the principle of least privilege, which means that access for all users should be blocked by default and enabled only for the specific accounts that require it. This will require more configuration, but it is well worth the added security benefits.

6) Set up a VPN

VPNs provide three main benefits: They make it possible to access resources remotely that would otherwise be inaccessible from offsite locations, while also encrypting connections and providing some access control for corporate networks. Setting up a VPN and requiring all remote connections to pass through it is a basic best practice for keeping resources secure when employees work remotely. It is important to note that a VPN is not a complete solution. It mitigates the risks of some types of attacks, such as data sniffing, but it does little to protect against threats like phishing. Plus, it may contain

its own set of vulnerabilities to be exploited by attackers. Think of a VPN as one layer of defense for remote-access security, but not a complete solution.

7) Manage sensitive data securely

Sensitive data is important to always secure via encryption and access control. But when employees work remotely, it becomes especially critical to make sure that they work with sensitive data properly. If your company is subject to compliance rules that require data to remain on certain servers, make sure employees cannot download copies of the data to the devices they use when working remotely. Even if compliance is not an immediate concern we should establish policies on whether and how employees can copy data onto remote devices.

*The measures listed within this report encompass a summary of industry-standard accepted best practices according to multiple security publications. However, the level of security can impose a certain degree of inconvenience to Users. Administrators can implement additional stronger measures if the tradeoff is deemed acceptable and necessary.