Business Continuity Plan

Grande empresas possui uma equipe que é responsável pela criação e manutenção do plano de continuidade de negócio (Businesse Continuity Plan – BCP). Esta política define como a organização manterá o que é aceitável em termos de normalidade para o seu dia a dia caso um incidente de segurança ou outro evento disruptivo aconteça ao negócio. A importância do BCP não pode ser minimizada, pois ele é necessário para garantir que o negócios continue funcionando e possa operar em um nível mínimo aceitável durante um desastre. Um BCP é feito para garantir que os sistemas vitais, serviços e documentos que suportam o negócio permaneçam disponíveis para alertar os stakeholders principais e recuperar os ativos mesmo quando um bando de sistemas críticos estejam inoperantes.

Quando fala-se de BCP, logo fala-se de Plano de Recuperação de Desastre (Disaster Recovery Plan – DRP). Este documento descreve uma política que define como o pessoal e ativos serão protegidos em um evento de desastre e como estes ativos serão restaurados ao seu nível operacional uma vez que o desastre acabe. O DRP normalmente incluirá uma lista de indivíduos responsáveis pelo qual serão envolvidos num processo de recuperação, um inventário de hardware e software vitais, os passos para realizar e endereçar as interrupções, e como reconstruir os sistemas afetados.

Suportando a Continuidade de Negócios e a Recuperação de Desastre

Muitas técnicas podem ser usadas para manter a organização funcionando e minimizar o impacto de um desastre quando ele ocorrer.

Tolerância a falha é a habilidade de resistir a potenciais falhas enquanto prover algum serviço. Enquanto este serviço não estiver otimizado, ele deve ser capaz de manter as operações do negócio mesmo que não esteja no nível normal de performance. Mecanismos de tolerância a falha incluem duplicação de serviços e infraestrutura.

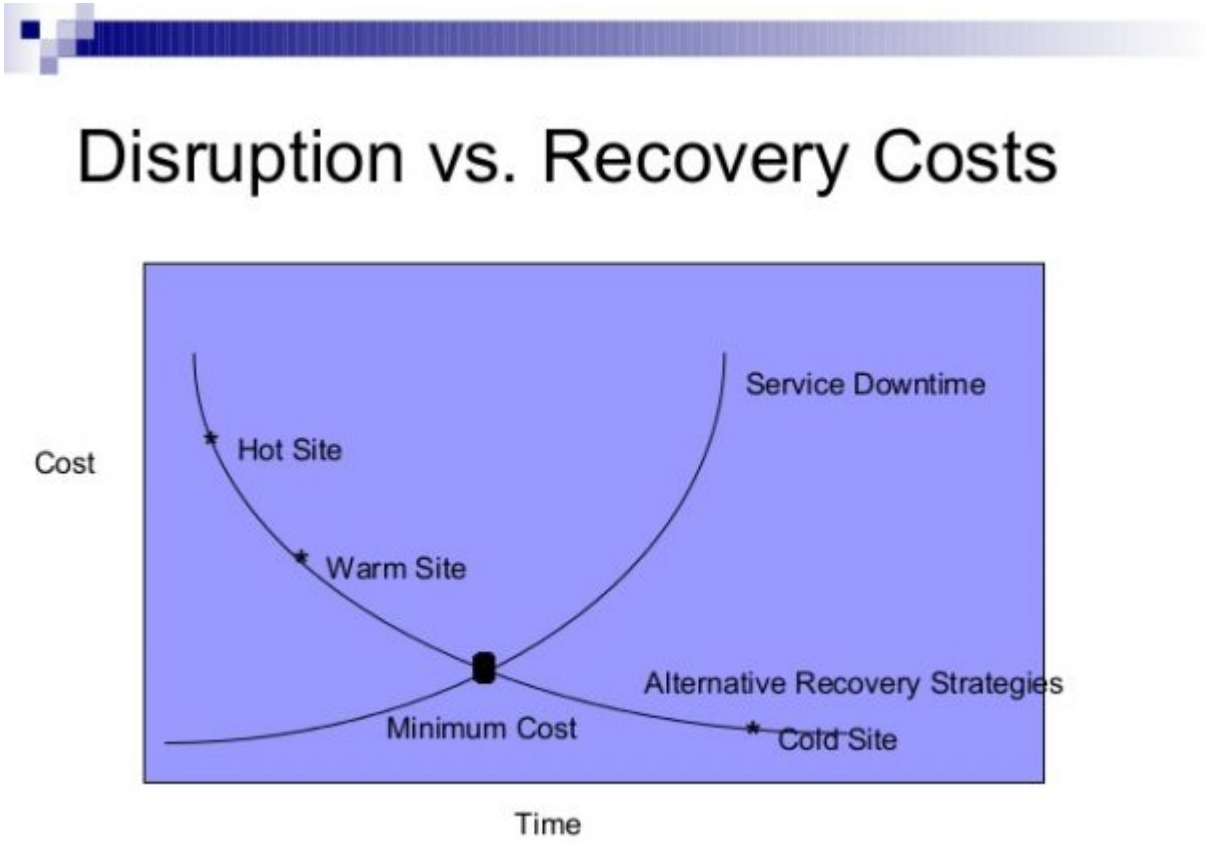
Outro mecanismo usado pelas empresas é a arquitetura de alta disponibilidade (high-availability – HA). É uma forma de mensurar o quão bem os sistemas estão provendo seus serviços, especificamente quão disponível o sistema está. Em um mundo ideal, um sistema deveria estar disponível 100% do tempo, mas isto é praticamente impossível por longos períodos. HA simplesmente mensura, em porcentagem, o quão disponível o sistema está, então, quanto mais próximo de 100% de disponibilidade, menos tempo ele passou offline. HA pode ser obtido através de sistemas redundantes ou sistemas de backups confiáveis. Quando implementados apropriadamente, isto significa que os serviços que você depende para trabalhar e prover os serviços para os clientes estarão disponíveis e prontos para usar pelo maior tempo possível.

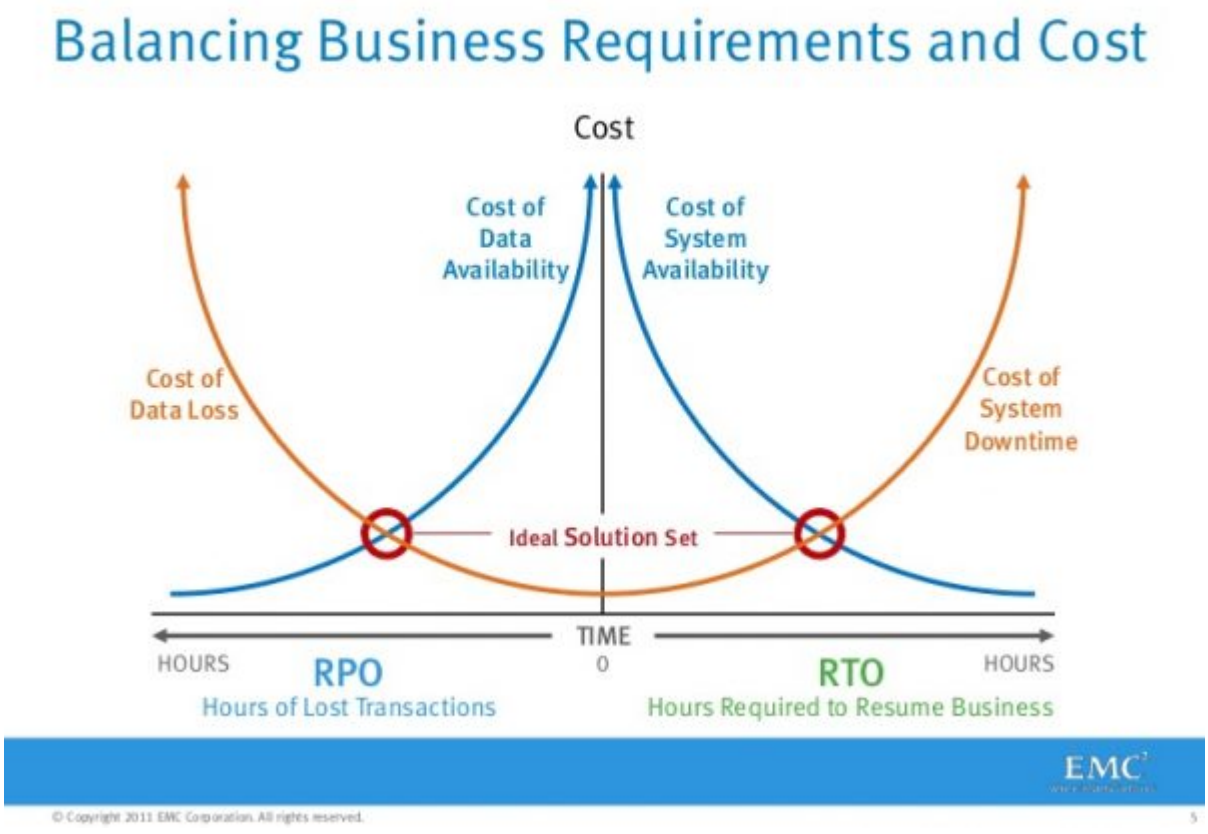
Um documento comum a ser mencionado quando falamos de HA e tolerância a falha é o service-level agreement (SLA). Este documento diz quais as obrigações do provedor de serviços para o cliente. SLA é um contrato legal que diz o serviço que será prestado e qual é o seu nível de performance, e os passos que serão em um evento de falha. Um exemplo comum de SLA são os de servidores de hospedagens de sites, onde ele informa detalhes sobre o quão disponível o serviço está garantido e as possíveis multas caso o provedor de serviço não consiga obter.

Locais alternativos são outro meio usado em um evento de falha de sistema ou desastre. A ideia é ter um outro local para continuar operação de seu negócio no caso de desastre. Em condições ideais, todas as operações serão movidas para um local alterantivo caso o local primário não esteja mais disponível para prover os serviços. Nem todos os locais

alternativos são criados de forma igual. Basicamente existem três tipos:

1. **Cold site** – É o tipo mais básico de local alternativo e o mais barato de operar. O cold site, pela definição normal, não inclui cópias de backup dos dados ou arquivos de configuração do local primário. Também não possui qualquer tipo de hardware configurado no local. Devido a falta disto tudo, o cold site é a opção mais barata, mas também contribui para situações de falhas por um longo período de tempo, pois toda a infraestrutura deverá ser remontada e os dados restaurados para voltar a funcionar.
2. **Warm site** – É a opção intermediária, oferecendo um equilíbrio entre custo e tempo para colocar tudo no ar. Um warm site normalmente tem algum (não todos) hardware no local, junto a outros itens como energia e conectividade com a internet já estabelecida. Este tipo de site também tem backup em mãos, mesmo que esteja desatualizado por alguns dias ou semanas.
3. **Hot site** – Esta é a opção ideal, pois oferece pouco downtime, mas por outro lado, é a opção mais cara. Este tipo de alternativa tem uma sincronização com o local primário, o qual praticamente tudo é duplicado. A configuração de tudo requer uma complexidade de conexão de rede e outros sistemas e serviços que são desenhados para manter esta sincronia. Este nível de complexidade adiciona um custo enorme ao local, mas tem a vantagem de reduzir substancialmente (ou eliminar) o downtime.





Antes do local alternativo poder trabalhar, a empresa deve ter um backup dos dados, e este deve ser mantido de forma segura,

pois contém informações sobre a empresa, seus clientes e sua infraestrutura. Backups devem ser armazenados de forma segura, com cópias mantidas no local da empresa e fora dela também, dando uma proteção extra. Para complementar, eles devem ser armazenados em mídias separadas e trancados em um local fora do local primário. Manter eles criptografados é uma forma de garantir uma proteção extra contra vazamento de informações, caso ele seja roubado. Outras medidas de proteção devem ser estabelecidas contra fogo, inundação, terremotos, tsunami, etc.

Planejamento para Desastre e Recuperação

A fim de planejar de forma apropriada para uma recuperação de desastre, você precisará entender onde a sua empresa se encontra, o quão preparada ela está para este tipo de situação. É necessário avalia-la e entender o que você precisa fazer para que a empresa esteja pronta este tipo de situação.

Algumas boas práticas são:

- Uma vez que a organização tenha estabelecido um BCP, é importante para este plano manter ele regularmente testado e revisado. Considere conduzir simulações ou exercícios para avaliar a eficiência do plano. Se a empresa não teve seu BCP testado recentemente, é importante começar por aí;
- Sempre considere e avalie as medidas de redundância de forma apropriada para todso os recursos críticos. Busque as proteções adequadas para sistemas como servidores, roteadores e outros dispositivos em um evento que eles serão usados em caso de emergência.
- Checar todos os provedores de serviços críticos que eles tenham tomado as precauções adequadas para garantir que os serviços providos estejam disponíveis;

- Checar pela existência ou a possibilidade de obter hardware extra quando necessário. Garanta que os dispositivos não são só apropriados para uso, como também para ser obtidos de forma rápida em uma emergência;
- Avaliar os SLA existentes e saber se eles constituem um nível aceitável de downtime;
- Estabelecer mecanismos de comunicação que nã necessitem de recursos da companhia, os quais possam estar indisponíveis. Alguns canais de comunicação devem também levar em conta a falta de energia;
- Garantir que o hot site designado pela empresa possa ser colocado online imediatamente;
- Identificar e documentar qualquer e todos os pontos de falhas;
- Garantir que o armazenamento redundante da empresa esteja seguro.

Referência: Certified Ethical Hacker version 9: Study Guide. Sybex. 2016.