특집

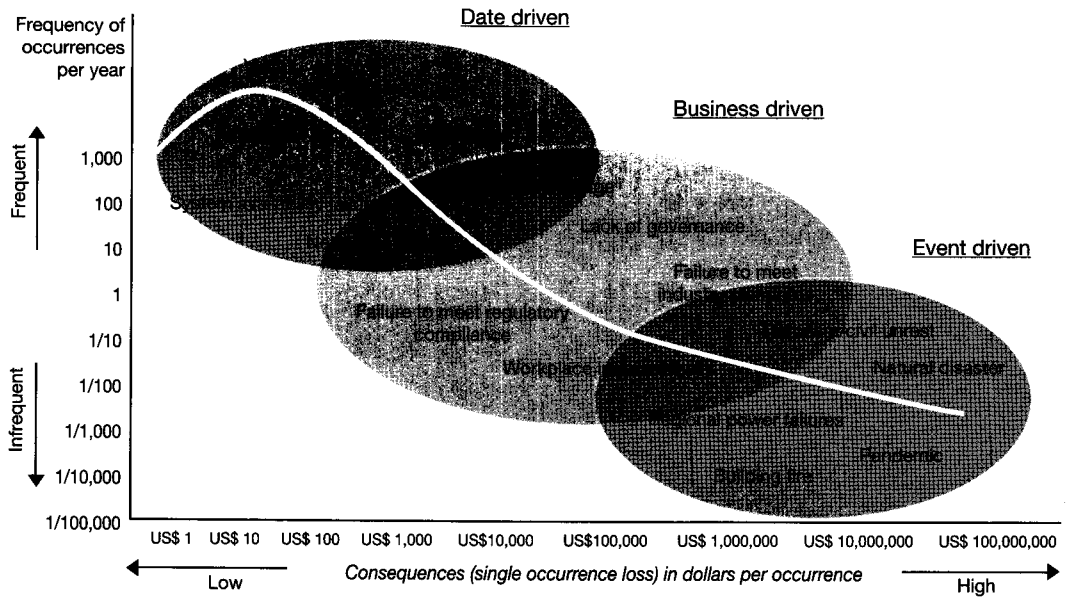
비즈니스연속성 확보의 핵심(核心)
- IT 재해복구(Disaster Recovery)

김정일(한국 IBM Global Technology Service), 유종기(안진회계법인)

Ⅰ. 서 론

정보시스템 도입 전의 수작업(manual processes)을 통한 업무수행이 이제는 극히 제한적인 수준에서 가능할 정도로, 컴퓨터시스템 장애가 일어났을 때 이를 복구하지 않고 전면 수작업으로 업무를 진행한다는 것은 상상도 할 수 없다. 이러한 이유로 정보시스템 즉 IT/기술적 환경(technology environment)의 복구라고 하는 IT 재해복구(Disaster Recovery)라는 개념과 서비스가 생겨났으며, 지난 9/11 테러 이후 이의 중요성은 지속적으로 증가되고 있다.

데이터센터(Data Center, 재해복구센터를 포함)가 존재하는 이유는 단 하나이다. 회사, 조직



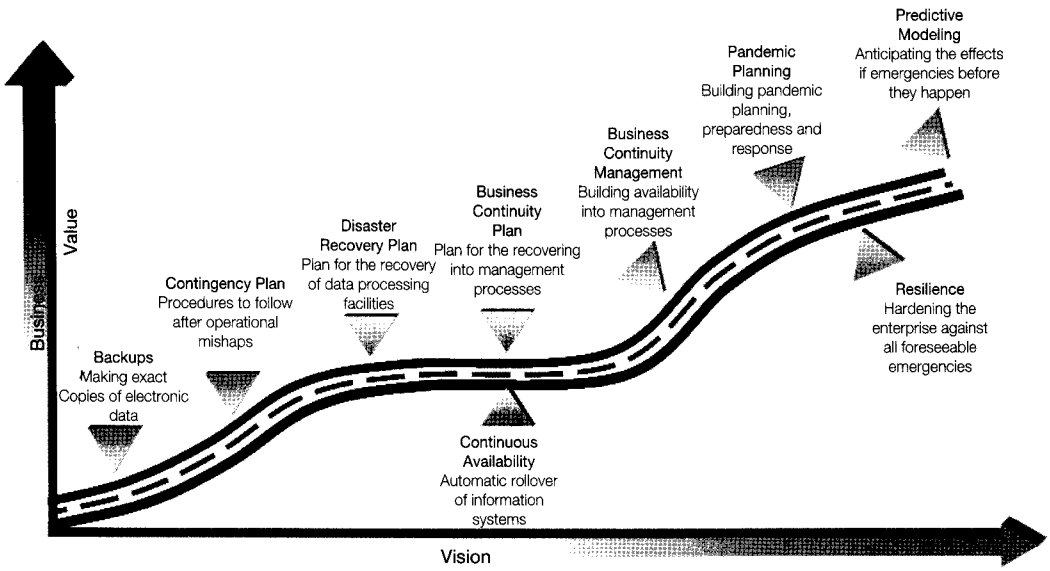
〈그림 1〉 기업에 노출되어 있는 IT 리스크 – Data Driven 영역
(출처 : IBM – enterprise resilience strategies in response to Risks)

의 주요업무가 중단 없이 수행될 수 있는 비즈니스연속성을 확보해주기 위한 것이다. 피할 수 없는 위기 상황에도 끄떡없이 비즈니스 활동을 영위할 수 있도록 기업들이 사전에 철저히 대비하고 적절한 IT 환경을 구축하는 것은 당연한 일이며 최고경영진의 의무이다. 비즈니스에 기우(杞憂)란 있을 수 없기 때문이다.

재난/재해나 테러 상황에서도 회사의 핵심 업무가 재개될 수 있는 기업의 위기관리 능력의 기준과 지표로 국내에 소개된 BCM(Business Continuity Management, 비즈니스연속성관리)는 "조직(기업)을 위협하는 잠재영향을 파악하고, 주요 이해 관계자의 이익, 조직의 평판, 브랜드 및 가치창출활동을 효과적으로 보호하기 위해 필요한 대응 및 복원역량 확보를 가능케 해주는 체계 제공의 통합 경영 프로세스"로 정의될 수 있다.

IT없이 기업 비즈니스 운영을 논하는 것이 절대 불가능할 정도로 기업 내에서 IT가 차지하는 비중, 의존도는 매우 증대되었다. 그러나 앞에서 정의한 BCM 프로그램 에서는 IT DR(Disaster Recovery, 주로 정보시스템 재해복구를 의미)이 차지하는 중요성에 비해 실제로 상세한 지침, 내용을 가이드하고 있지는 못하다. 이는 IT DR 계획수립, DR시스템 구축과 관련된 내용은 상당히 기술적이고 이 주제 자체만으로도 상당히 방대하기 때문이기도 하다.

하지만 고무적인 것은 현재 BCM 프로그램 테두리 내에서 IT 시스템 Continuity에 특화된 내용에 대한 표준화 작업이 계속 구체화되고 있으며, 올해 안에 BS 25777로 명명된 IT 시스템에 대한 Continuity Management 규격이 최종 발표될 예정이라고 한다. 한편 Information Security 영역에서 세분화되어 BS 24762라고 하는 Guidelines for Information and Communications



〈그림 2〉 비즈니스연속성(Business Continuity)의 진화 및 목표
(출처 : Deloitte – The future towards "Resilience Enterprise")

Technology Disaster Recovery Services 규격도 올 2월에 발표된 바 있다.

본고에서는 비즈니스연속성을 이야기 할 때 가장 중요한 요소의 하나인 IT 재해복구체계 수립을 위한 구성요소와 이의 실행가능성을 확보하기 위해 수립하는 재해복구계획에 필요한 고려사항을 짚어보고 앞으로 이러한 IT 재해복구가 어떤 식으로 융합, 발전해 나갈 것인지에 대한 고찰을 해보고자 한다.

II. IT 재해복구체계의 구성요소

정보시스템 Information Technology (IT)[1]을 대상으로 하는 재해복구체계를 수립하기 위해서는 구현 방법론과 같은 단계별 접근이 필요하며, 위험과 주요시스템 식별로부터 출발하여 복구를 위한 전략과 관련 서비스 제공을 하는 외부업체 등 고려해야 하는 점들을 충분히 반영해야 한다. 네트워크와 시스템, 데이터에 대한 복구 역량 확보를 우선적으로 고려하되 이와 관련된 정보보호관리도 빼놓아서는 안되는 요소이며, 정보시스템이 위치하는 시설과, 재해복구센터 등 대체운영, 업무장소도 고려해야 한다. 마지막으로 이러한 전략, 조직, 계획, 시설 등의 체계가 실행가능성과 완전성을 확보하기 위한 주기적인 검토와 모의훈련에 대한 방안 및 지속적인 운영과 개선(continuous improvement)이 체계화되어 있어야 한다.

1) 위험 식별 Identification of risks

- 복구 시 데이터 정합성 이슈 식별(points of consistency of data for recovery), 영향을 받지 않은 시스템의 운영재개로 인한 결과식별, 주요시스템 식별 (해당 시스템의 복구절차 등 내역이 계획이 반영되어야 함)

2) 주요시스템 식별 Identification of critical IT

- 핵심 IT 시스템과 인프라를 파악하기 위해 IT 시스템 손실에 대한 상세 영향 분석 수행
- IT 시스템 중단에 따른 임계도(criticality, 위험한 상태)를 지속적 분석, 문서화
- IT 시스템의 주요 영역에 대해서 체계적인 의존도 분석을 수행하여 개별 IT 시스템 중단 영향 평가

3) 복구전략 Recovery Strategy (IT 재해복구계획에 포함되어야 하는 내용 포함)

- 비즈니스상황에 따른 모든 IT 시스템 복원 (복구우선순위 상세절차 포함)

1) 영국금융감독원에서 60개의 영국 금융회사를 대상으로 해당 회사에서 진행되고 있는 BCM 활동을 조사하여 5가지 주제(연속성 Corporate Continuity, 위기관리 관련 Corporate Crisis Management, IT 시스템 관련 Corporate Systems, 시설 관련 Corporate Facilities, 임직원 관련 Corporate People)로 분류, 분석하여 표준모범사례로 정리한 내용이다. BS25999 등의 표준, 가이드라인에서 제시하고 있는 구현방법론을 현실에서는 어떻게 해석하여 적용하고 있는지 감을 잡을 수 있어, 금융기관이 아니더라도 BCM 도입, 구현을 위한 좋은 길잡이 역할을 할 수 있는 자료 중 일부 인용 - 원문은 www.fsa.gov.uk 에서 다운로드 가능(Business Continuity Management Practice Guide (2006.11)

- IT 시스템 복구 소요시간
- 주요시스템 복구에 대한 상세내역
- 개발환경(운영환경에 추가적으로)에 대한 복구계획도 존재
- 주요 시스템과 관련 하드웨어의 복구(테스트포함)
- 미러 시스템(mirror systems)이 구축되어 있는 경우, 주 시스템 중단 시 복제 시스템으로부터 백업을 받을 수 있도록 백업관리에 대한 준비
- WAN 복구를 위한 재해복구사이트로의 상설연결 망(permanent connections) 구축
- 전체 시스템의 정상 복구
- 원래 장소로의 IT 운영의 환원(원복)

4) 서비스 제공업체 Providers

- 중요사이트에 대해서는 음성, 데이터 통신 제공을 위해 복수의 통신 사업자를 이용 (통신서비스 제공업체의 네트워크 아키텍처와 연결성 등에 대한 복원력, 그리고 IT 서비스 제공업체의 재해복구 역량을 확인 및 상세검토 수행)
- 복수의 서비스수행 상황발생시 관리 절차가 존재하고 이에 대한 협의 수행
- WAN 분할/구분 서비스(separacy/diversity services) 제공이 가능한지 여부 확인

A. Corporate Continuity	B. Corporate Crisis Management	C. Corporate Systems	D. Corporate Facilities	E. Corporate People
A.1 Business continuity planning	***B.1 Culture***	***C.1 Information Technology (IT)***	***D.1 Planning***	***E.1 Staff***
A.1.1 Risk assessment	B.1.1 Strategy	C.1.1 Identification of risks	D.1.1 Planning	E.1.1 BCP awareness
A.1.2 BCP strategy	B.1.2 Audit and review	C.1.2 Identification of critical IT	D.1.2 Energy	E.1.2 Training
A.2 BCP design	B.1.3 Accessibility	C.1.3 Recovery	D.1.3 Water	E.1.3 Staff planning
A.2.1 Critical suppliers	B.1.4 Senior management	C.1.4 Providers	D.1.4 Security	E.1.4 Key staff
A.2.2 Responding to requests for BCP information from third party organisations	***B.2 Team***	C.1.5 Network resilience	D.1.5 Evacuation	E.1.5 Checks
A.2.3 Outsourcing contract providers	B.2.1 Crisis management team	C.1.6 IT resilience	D.1.6 Emergency services	E.1.6 Tests
A.2.4 Critical paper assets	B.2.2 Team activation	C.1.7 Data	D.1.7 Testing	***E.2 Crisis management***
A.3 Resources	B.2.3 Team attributes	C.1.8 Security		E.2.1 Contacting staff
A.3.1 BCP team	B.2.4 Team support	C.1.9 Site		E.2.2 Staff welfare
A.3.2 Staff and BCP	B.2.5 Facilities	C.1.10 Alternate site		
A.3.3 Third parties and BCP	***B.3 Communications***	C.1.11 Review, audit and changes		
A.4 Plan review	B.3.1 Communication strategy	C.1.12 Testing		
A.4.1 BCP audit	B.3.2 Internal and external communications	***C.2 Telephony***		
A.4.2 BCP changes		C.2.1 Recovery		
A.4.3 Testing		C.2.2 Site		
A.4.4 Documentation		C.2.3 Testing		
A.4.5 Recovery service providers				
A.5 Recovery times for critical functions				
A.5.1 Trade clearing				
A.5.2 Settlement				
A.5.3 Wholesale payments				

〈그림 3〉 비즈니스연속성관리 실무가이드 – IT BCP/DR(Corporate Systems: Information Technology, Telephony)
(출처 : Business Continuity Management Practice Guide, Financial Supervisory Services, U.K.)

5) 네트워크 복원력 Network resilience

- IT 계획서에 최근 내용이 반영된 네트워크 구성
- 네트워크 연속성 관련 모든 고려사항을 사전적으로 다루고, 반영
- 단일시점실패(SPOF, Single Points of Failure, 네트워크의 한 구성요소 또는 영역의 마비, 중단이 전체 네트워크의 성능과 연속성에 영향을 미치는 리스크를 의미)가 발생하지 않도록 네트워크 이중화
- 네트워크 가용성 지표 모니터링
- WAN에 대한 전체적인 통제와 가시성 확보
- 1시간 (또는 목표복구시간) 이내에 WAN 통신이 대체업무복구장소서 복원 가능

6) 전화통신(음성통화 중심) Telephony-Recovery 복구를 위해서는 다음 내용이 포함

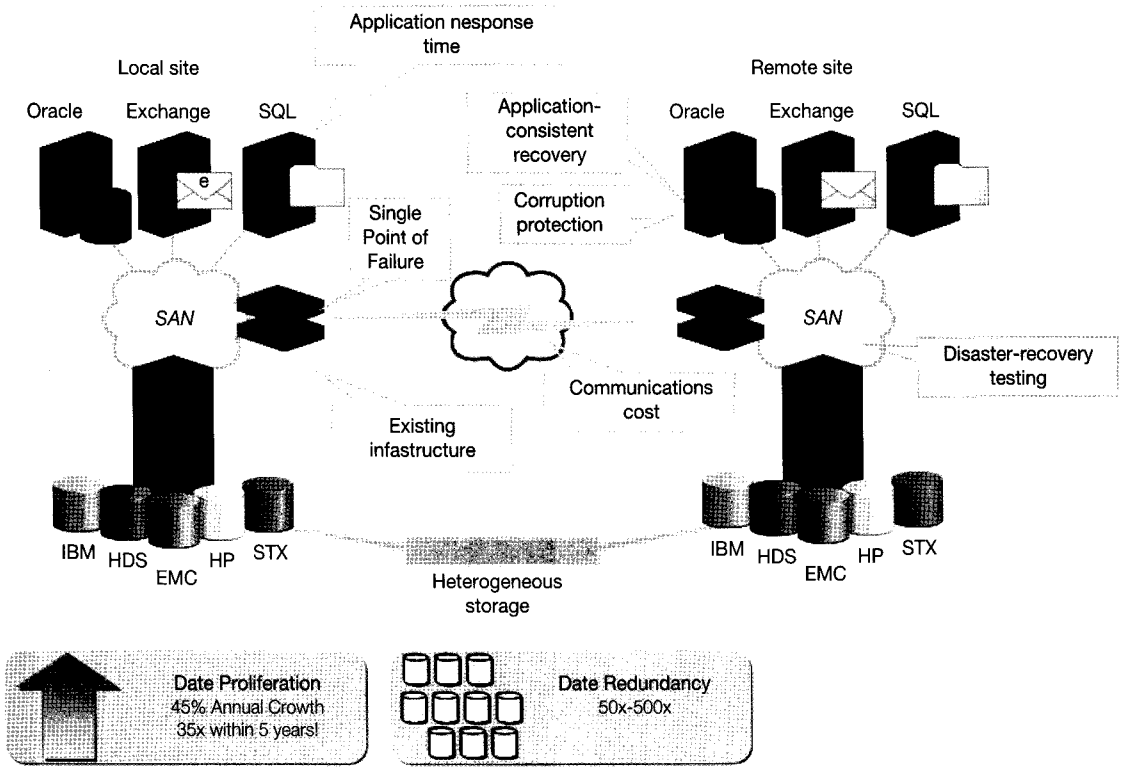
- 전화통신 복원력과 통화 전환에 대한 복구 상세전략
- 콜 센터 복(ACD, IVR and turrets in call centre restoration, where applicable)
- 전화(음성통화)회의시스템 복구
- 비지역(전국공통 번호, 예. 1588-) 수신전화 번호로 전화착신 기능
- 재해복구사이트에 팩스장비(fax facility) 구축
- 음성통신 복구 전략 (재해복구 가동 후 2시간(또는 목표시간) 이내)
- 24시간 이내에 음성통화라인이 재해복구사이트, 콜 센터 등으로 분산, 착신
- 재해복구사이트에서의 (팩스, 모뎀 포함) 통화처리량이 정상환경 수준으로 운영
- 관련 시설, 물리적 공간 - (가능하면) 모든 사이트에 음성통신케이블 용으로 두 개 이상의 인입지점 설치에 대한 정책 수립, 각 주요 사이트에 대해서 복수의 외부전화교환실 설치
- 모의훈련 - 주기적(또는 연1회) 각 주요 사이트 별로 전화통신 복구 테스트를 수행 하며 다음 사항들을 테스트를 통해 확인: 재해복구사이트에서의 무선전화 수신, 재해복구사이트에서의 전화통신 착신, 재해복구 시 사용되는 자동구내 교환기(PABX)에 대한 프로그래밍, 주요 전화통신 복원(the restoration of critical telephony).

7) 시스템 복원력 IT resilience

- 재해 시 주요 시스템에 대한 복구 작업이 한 개인에 집중되지 않도록 함
- 주요IT 시스템은 여러 지역에 분산 구축, 운영
- 건물, 업무내용, 복제되지 않은 데이터가 손실되더라도 일주일 이내의 backlog(미처리 업무)를 발생시키는 정도여야 함
- 가장 중요한 IT 사이트에 영향을 미치는 사고 발생 시에도 영향/충격을 받은 주요 IT 시스템은 재해복구시작 4시간(2시간 또는 복구목표시간) 이내에 복구
- 재해복구 시스템으로 운영되는 경우, 양쪽 사이트(예 : 주 전산센터와 이중화한 제2센터)가 다 영향을 받는 경우에도(재해복구센터를 통해 지속적으로) 해당 시스템에 대한 복구 가능

8) 데이터 Data

- 모든 중요정보는 원격지에 복사/복제되어 보관



〈그림 4〉 시스템/데이터 복잡성 증대와 IT 재해복구시스템 과제
(출처 : Oliver Wyman, formerly Mercer - System Architecture Gains in Complexity as Does Recovery)

- 원격지에 보관되어 있는 중요정보의 복구는 1시간 이내(또는 목표복구시점 /시간)

9) 정보보호 Security

- 주기적인 모의테스트를 통해 방화벽 운영을 확인하고 있으며 회사의 보안정책을 준수
- 대내외간 주요 통신에 대해서는 암호화를 적용
- 노트북, PC 사용 시 외장하드와 같은 휴대용 저장미디어의 사용을 금지(또는 승인 받은 일부 기기에 대해서만 사용가능)하고 바이러스백신프로그램을 설치
- 외부 네트워크 접점 특히 메일서버, 노트북, PC에는 반드시 바이러스 백신프로그램을 설치
- 바이러스백신프로그램을 자동 업데이트 시켜 신종 바이러스 등에 대한 대응이 가능
- IT 보안담당 부서에서 허가하지 않은 노트북, PC에 대해서는 사내 네트워크에 접속하지 못하게 함
- 상용 OS(운영체계) 패치의 설치는 미리 테스트를 거친 후에 적용여부를 결정
- 주요 소프트웨어에 대한 에스크로우 협약(Escrow agreements)을

- 문서화된 정보보안정책이 갱신되어 최신화 되어 있어야 하고, 정보보호관리체계 표준인 ISO 17799에서 요구하는 통제항목 준수

10) 시설, 물리적 공간 Site

- IT 환경에 물리적 접근제어가 존재
- 주요 시스템에 대한 전력공급은 UPS와 발전기로 보호
- 습도, 환기, 온도조절 등 공조(HVAC, Heating, Ventilating, and Air Conditioning) 관련 적절한 IT 환경이 제어
- IT 환경에 대한 소방, 화재진압, 침수, 누수 방지

11) 대체사업장소 Alternate site

- 주 센터로부터 최소 10km 이상 떨어진 곳에 대체사이트(전용공간) 마련
- 재해복구사이트에서도 핵심시스템에 대한 소스코드의 접근 가능
- 재해복구사이트와의 적절한 통신망 확보(24시간 이내에 100% 네트워크 대역이 확보되어 재해복구사이트에 연결 가능)
- 주 센터에서 재해복구사이트로 통신망을 switchover하는 상세내역이 재해복구계획에 포함
- 재해복구사이트도 주/부로 나뉘어 주 재해복구사이트 가동불가 시 대체 가능한 사이트 존재
- 주 재해복구사이트 가동불가 시 대체사이트를 가동하는데 필요한 체계 존재

12) 검토, 감사 및 변경관리 Review, audit and changes

- BCM은 회사의 공식 변경관리 프로세스의 일환으로 보고 있으며 변경이 일어나기 전에 고려사항 검토
- 매 6개월마다 IT 시스템의 위험도 검토
- IT 시스템이 아웃소싱 되고 있는 경우 아웃소싱업체의 BCM 역량 검토
- 모든 변경사항은 협의, 승인절차를 거치도록 함

13) 모의훈련 Testing

- 최악의 시나리오(worst-case scenario)를 기반으로 IT 재해복구 테스트를 수행하여 모든 주요 시스템이 동시에 복구
- 주기적(예로써 6개월)에 한번씩 주요시스템에 대한 복구테스트 수행
- 실제 환경과 아주 유사하게(또는 완전히 동일한 환경으로) 테스트 환경 구성
- 일부 IT 기능이 아웃소싱 되는 경우에는 주요 IT 아웃소싱업체가 테스트에 참여
- 아웃소싱되는 IT 시스템에 대해서는 아웃소싱업체의 IT 재해복구 역량을 테스트하는 것을 규정하는 정책 존재
- 다음의 내용들을 테스트 함 - 주요 응용프로그램 또는 하드웨어/소프트웨어 키(Identified critical application or hardware and/or software keys), 재해복구사이트에서의 시장 데이터 피트(data feeds)/시스템, 재해복구사이트에서 마켓 데이터, 주요 제3자 데이터 피트에 대한 테스트, 클라이언트 또는 데스크톱 환경 재구성, 원격지/재택근

무 가능성/역량 확인, 주요 응용프로그램에 대 한 복 원 (Restoration of critical applications: live tests from mirrored systems or backups on an un-configured system are run.), 미러시스템, 주요 백업에 대한 복원테스트, 원격지에 소산 보관되어 있는 중요데이터의 복구, 목표복구시간 내에 복구가능성

III. IT 재해복구계획 (DRP) 수립

앞에서의 재해복구체계의 구현에서 언급한 목표와 전략을 현실적으로 구현하고 실행계획을 구체화하기 위해서는 IT 재해복구계획(Disaster Recovery Planning, DRP)이 제대로 작성되어야 한다. 여기서는 계획서 작성 시 언급되어야 하는 구체적인 고려사항(분석, 테스트/유지보수, 시스템구축 활동 등은 제외)을 정리하였으며, 이를 통해 IT DR 계획에 기술 적용을 준비할 수 있다.

1) 비즈니스기능과 정보시스템을 매핑 Mapping Business Functions to Infrastructure

- 하드웨어자산(hardware asset), 소프트웨어(software), 응 용 프 로 그 램 (business applications) 에 대한 현황파악(inventory)
- 데 이 터 흐 름 (data flow)과 스 토 리 지 (storage) 및 인프라환경에 대한 상위수준 아키텍처(high-level architecture) 파악
- 시스템간의 의존도(dependencies between systems) 파악 - 시스템, 네트워크 서비스, 보안, 응용프로그램 등에 대한 시스템간 (inter-system) 의존도 및 응용프로그램, 서비스의 대외(external) 의존도

2) 사용자 복구 계획수립 Planning User Recovery

- (최종)사용자 컴퓨터(end-user computing) 용도파악(단순 웹 브라우저, 주요시스템 접근을 위한 터미널, OS 운영시스템 등) 및 이에 따른 대응방안 마련
- 사 용 자 의 사 소 통 채 널 (end-user communications) 요건(음성통신/사서함, 이메일, 팩스, 문자 메시지전송 등) 파악 및 대응방안 마련

3) 시설(주로 전산실/센터) 보호 및 복구계획 수립 Planning Facilities Protection and Recovery

- 전산실 관련 시설(processing facilities) 보호 (물리적인 접근통제, 전력공급, 소방, 화학/유해물질 관리, 침수 대응) 방안 마련
- 대체장소 마련 (alternate processing site) - 핫, 콜드, 웜사이트에 대한 의사결정 및 주 전산시설과의 위치, 백업방식 등 선정 및 구현

4) 시스템, 네트워크 복구 계획수립 Planning System and Network Recovery

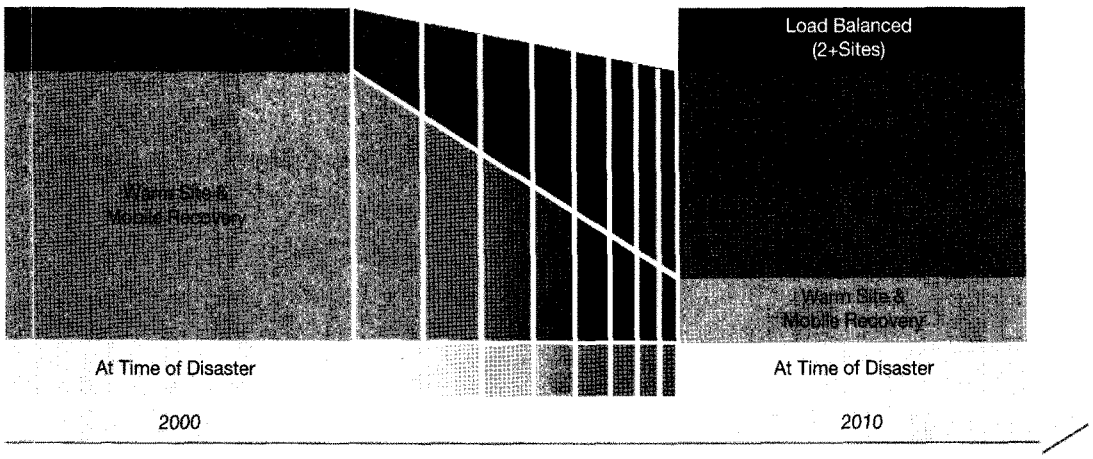
- 시스템 (server computing) 운영/복구 - 목표복구수준(RTO, RPO 등) 결정, 시스템아키텍처/구성(H/W, OS, 리소스, 네트워크, 보안, 권한/접근관리 등) 결정, 신규시스템 구축역량 고려/확보, 분산시스템환경 고려,

응용프로그램 아키텍처 고려, 시스템통합 이슈

- 네트워크 (Network Infrastructure) 운영/복구 - 응용프로그램 인터페이스 업그레이드, 클러스터(server clustering - active/active, active/passive, geographically distributed clusters) 구현 및 클러스터/스토리지 아키텍처 고려, 음성통신(voice communications) 네트워크 고려

5) 데이터 복구 계획수립 Planning Data Recovery

- 응용프로그램 데이터 복구 방법(백업, 스토리지, 복제/미러링(replication and mirroring), 전자금고(electronic vaulting) 등) 및 보관위치(원격지(off-site) 보관 등) 결정
- 어플리케이션(비즈니스 데이터로서, applications as another form of business data) 복구 - 계획수립 시 고려사항(version, patches/fixes, configuration, users and roles, interfaces, customizations, pairing with OS and database versions, client systems, network considerations, change management, configuration management)



For agility, clients will invest in fundamental IT capabilities to increase the stanbility, "auditability" & security

- Through 2009, more than 50% of Global 2000 users will utilize a single "hardened" date center augmented by third-party services to deliver traditional, cost-effective disaster recovery services (48-72 hour recovery)
- Need will increase for internal recoverability architectures

- By 2009 45% of Global 2000 users will utilize two data centers to deliver continuous availability
- 25% of dual-data center users will support real-time recovery
- 90%+will deliver recovery point objectives approaching 0 for about 20% of the workload(2008), growing to 30% by 2010

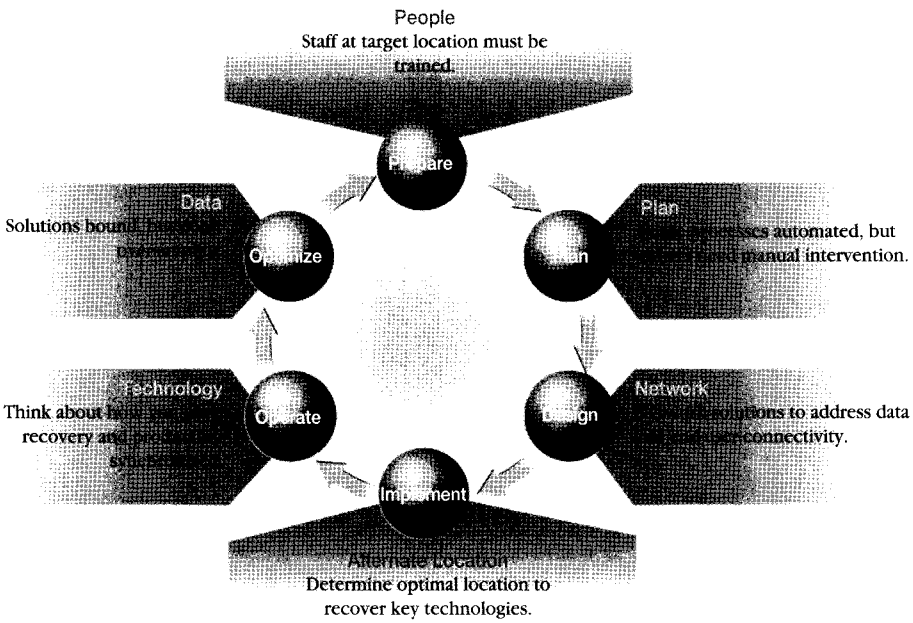
〈그림 5〉 IT 재해복구의 변화
(출처 : Gartner Research – Changing Dynamics of IT Recovery)

IV. 결 론(A Way Forward)

9/11 테러 이후 많은 글로벌 기업들은 이러한 발생가능성은 적지만 기업 비즈니스에 치명적인 영향을 줄 수 있는 리스크관리를 위해 IT 재해복구에서 대폭 진화된 개념인 BCM에 대한 도입이 이제는 보편화 되어가고 있으나 국내에는 아직도 이의 도입이 지지부진 하고 중요성에 대한 인식이 부족한 실정이다.

국내기업의 경우 2008년 3월 삼성생명과 IBK 기업은행의 전산정보부 업무(데이터센터, 재해복구센터 포함)이 국내 최초(세계에서는 4번째)로 IT 리스크관리 능력을 인정받은 BCM 국제인증을 취득했다. 화재, 테러 등 대형재해나 위기상황 발생시에도 회사의 핵심업무인 IT 시스템과 관련 서비스가 지속적으로 제공될 수 있는 역량확보 및 대응체계구현을 위한 BCM의 영국표준인 BS 25999에 부합하는 체계를 평가 받은 것이다.

취약한 노출 리스크수준과 충족해야 하는 규제요건(compliance) 및 감내, 용인할 수 있는 업무중단에 따른 손실 정보, 처리량 및 기존 IT 인프라의 특성을 면밀히 고려하여 합리적인 재해복구전략을 수립해야 한다. Mission Critical 한 기업 내 정보, 데이터는 기업의 이익과 직결되는 중요한 자산이며, 이러한 자산이 보관, 운영되고 있는 IT 시스템의 중단없는 가용성(High Availability)을 확보하고 전체 시스템에 큰 영향을 줄 수 있는 리스크에 대응하는 것이 비즈니스 연속성 구현이 핵심이다.



〈그림 6〉 IT 재해복구 체계 구현을 위한 성공요소
(출처 : Deloitte-Successful IT Recovery(Data Center Resilience) Requires a Resilient Organization)

참고문헌

[1] The Next Level of Disaster Recovery, John, Lindeman, Disaster Recovery Journal, 2007년

[2] BS 25777: Code of Practice for Information and Communications Technology Continuity, Draft for Public Comment (DPC version) 2008년 8월

[3] BS 24762: Information Technology - Security Guideline - Guidelines for Information and Communications Technology Disaster Recovery Services, 2008년 2월

[4] Using Virtualization for Disaster Recovery, Gartner Research Report, 2008년 10월

[5] What Your Business Can Learn About DR from Financial Institutions, Forrester Research, 2008년 7월

[6] Business continuity and resiliency services - Helping business stay in business, IBM Global Technology Services, 2008년 발표자료

[7] IBM - Virtualization on the IBM Family of Servers, Software and Storage

[8] BCM, 비즈니스연속성관리(Business Continuity Management): A Practical Guide, FKI미디어, 2008년

[9] BCP(Business Continuity Planning) 구축전략, 김정일, 김주희, 유종기, FKI 미디어, 2005년

저자소개

김 정 일

1965년 경동고등학교
1971년 경희대학교 정경대학 상학과 학사
1974년 Montclair State University in New Jersey, USA 석사(Matriculated in Business Education)
1975년 Rutgers University, MBA Candidate
1982년~1987년 Citibank, NA, USA, 수석 컨설턴트
1987년~2001년 12월 Merrill Lynch, Princeton, NJ, USA, 부사장 (PMO & GCP)
2002년~2004년 PPMC Korea 한국 대표, CEO
2004년~현재 한국 IBM Global Technology Services 상무
주관심 분야 : 비즈니스 연속성관리(Business Continuity Management, BCM), 정보시스템 재해복구(IT Disaster Recovery), IT Outsourcing 관리, 운영, 전략, ISO (Intl. Standard Organization)

저자소개

유 종 기

1997년 한양대학교 상경대학 경제학과 학사
1999년 고려대학교 국제대학원 국제경영 석사 (정보경제 Information Economy)
1999년~2000년 전국경제인연합회 산업조사본부 조사역 (IT/통신산업 전문)
2000년~2006년 IBM Global Technology Service. Managing Consultant
2006년~현재 Deloitte 안진회계법인 Enterprise Risk Services. Manager
2007년~현재 영국 Business Continuity Institute(www.thebci.org) 한국대표
주관심 분야 : 비즈니스연속성관리(Business Continuity Management, BCM), 정보시스템 재해복구(IT Disaster Recovery), 정보보호(Information Security), IT 가버넌스 (Governance)