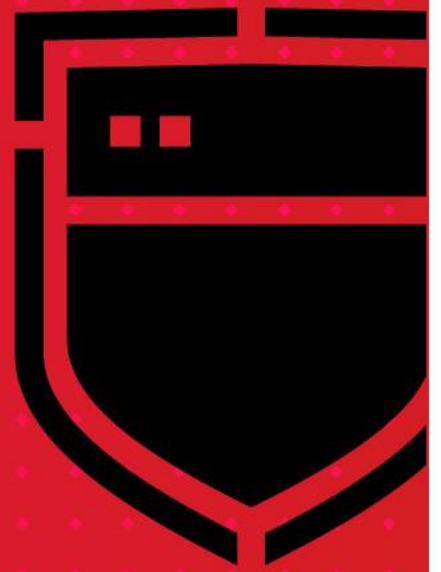
VERITAS PRESENTS:

RANSOMWARE'S GREATEST FEARS

글로벌 랜섬웨어 동향 및 실제 적용 사례



보호, **탐지**, **복구**를 통한 Best Practices

VERITAS™

RANSOMWARE'S GREATEST FEARS

복구 관점에서 랜섬웨어 공격 동향

탐지와 예방을 넘어서는 공격

Prevention is a Myth:

- 기업화, 지능화, 진화된 랜섬웨어 공격
- 공급망공격, Log4J등 지속적인 취약점 발생등

다중 협박 전략의 증가

이중, 삼중, 다중 협박 공격:

- Multi-Faceted Extortion Attacks의 증가와 진화
- 해킹 그룹들간의 협업과 전문화 추세

백업인프라를 직접 공격

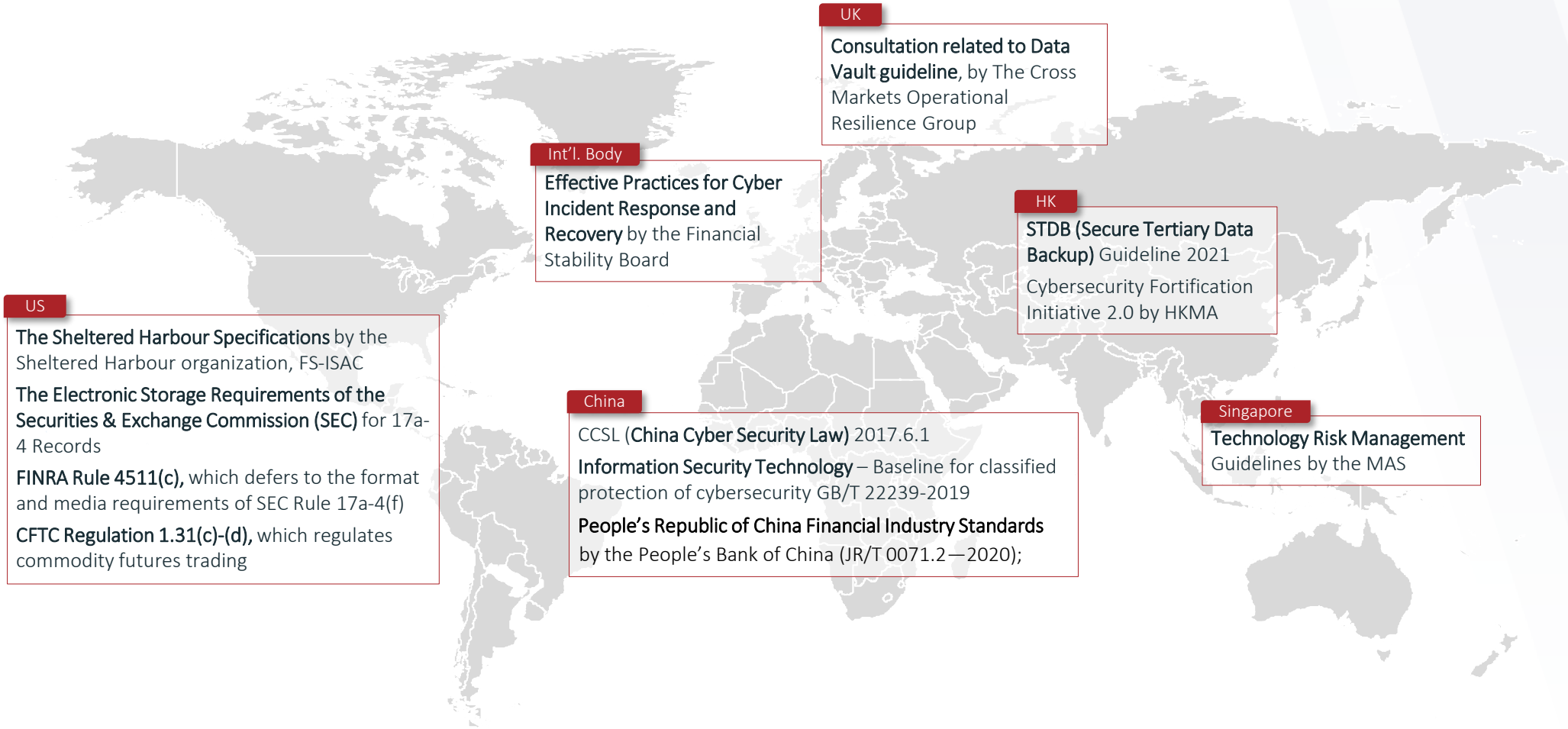
백업 전문가 수준의 공격:

- 엔터프라이즈 백업에 대한 준비된 공격
- 전반적인 복구 분야에 대한 이해도가 급상승함

VERITAS

RANSOMWARE'S GREATEST FEARS

해외 관련 법규 및 업계 규정 동향



UK

Consultation related to Data Vault guideline, by The Cross Markets Operational Resilience Group

Int'l. Body

Effective Practices for Cyber Incident Response and Recovery by the Financial Stability Board

HK

STDB (Secure Tertiary Data Backup) Guideline 2021

Cybersecurity Fortification Initiative 2.0 by HKMA

US

The Sheltered Harbour Specifications by the Sheltered Harbour organization, FS-ISAC

The Electronic Storage Requirements of the Securities & Exchange Commission (SEC) for 17a-4 Records

FINRA Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f)

CFTC Regulation 1.31(c)-(d), which regulates commodity futures trading

China

CCSL (**China Cyber Security Law)** 2017.6.1

Information Security Technology – Baseline for classified protection of cybersecurity GB/T 22239-2019

People's Republic of China Financial Industry Standards by the People's Bank of China (JR/T 0071.2—2020);

Singapore

Technology Risk Management Guidelines by the MAS

VERITAS

RANSOMWARE'S GREATEST FEARS

해외 관련 법규 및 업계 규정 동향

백업, DR등 일반적인 단순한 내용이 아니라, 매우 구체적으로 업데이트됨

WORM스토리지, RBAC, 에어갭, 탐지와 예방 등 백업 인프라에 대한 최신 기술들로 업데이트됨

단순한 백업과 복구 기술 요건이 아니라, 전략과 프로세스를 포함한 포괄적인 원칙들이 소개됨

Cyber resilience over Cyber security

VERITAS

RANSOMWARE'S GREATEST FEARS

실제 랜섬웨어 복구 사례에서의 시사점

1. 복구 관점에서 인시던트 대응 프로세스의 필요성

- 복구팀에서의 랜섬웨어 인스던트 대응 프로세스가 필요함.
- 이중 삼중 협박 전술의 랜섬웨어 공격의 경우, 개인정보 유출사고로 이어질 수 있고, 이로 인한 복구 지연 발생될 수 있음.

2. 백업 인프라에 대한 탐지와 예방 프로세스 부재

- 백업 인프라에서 발생되는 의심스러운 행위가 탐지되지 않음
- IPS/IDS, 암호화, MFA, RBAC등의 많은 보안 수단들이 백업에 맞게 적용되지 않고, 디테일이 떨어짐.

VERITAS

RANSOMWARE'S GREATEST FEARS

실제 랜섬웨어 복구 사례에서의 시사점

3. 실전 같은 복구 연습의 부재

- 일반적인 재해 시나리오가 아닌 랜섬웨어 공격에 대한 구체적인 복구 프로세스가 없는 경우 빠른 대응과 복구가 어려움
- 싱글 시스템 restore 테스트가 아닌, 실전 같은 대규모 리허설이 필요함

4. 멀티레이어드 보호 전략의 부재

- 기본적인 Protection룰과 프로세스 준수의 중요성
- WORM 스토리지와 Isolated Recovery Environment이 클린 백업 카피, 에어갭 등과 같이 구축되어야 함

VERITAS

RANSOMWARE'S GREATEST FEARS

실제 랜섬웨어 복구 및 구축사례

해당 케이스

랜섬웨어 복구 및 구축

인더스트리

IT업종

고객사

270곳이상의 글로벌 오피스, 30만명 이상의 직원, $16.13 billion 연매출액.

사건 개요

2020년 상반기 데이터센터에 랜섬웨어 공격 발생함.

백업 환경(DR 포함)에도 피해 발생함. (NBU Appliance를 제외한) 복구에 상당한 시간 소요

최대 7,000만 달러 손실 예상됨

진행 과정

피해 발생 이후 외부 보안업체를 통한 컨설팅 진행

백업, 보안관제 및 방어, Compliance가 통합된 관리 체계 필요성 인식함.

백업체계를 NetBackup Appliance로 전환 결정함

To-Be 아키텍쳐

- 백업 스토리지 공격에 대한 완벽한 에어갭 솔루션
- 3rd-party가 아닌 자체 WORM 기능
- 백업 인프라에 대한 불변성
- 랜섬웨어 분석 기반 복구
- 대규모 시스템에 대한 즉각적 복원
- 고가용성을 통한 백업 인프라 확장 및 복원력 유지

결과

- 100% 백업 Coverage
- 백업성공률 95% 이상
- 불변성 스토리지, 자동화 에이캡 구축
- 체계적이고 신속한 복구 체계 구축

VERITAS

RANSOMWARE'S GREATEST FEARS

맺음말

멀티레이어드 보호 기반의 솔루션과 복구 전략 수립

- 랜섬웨어에 준비된, Protect, Detect, Recover 에 이르는 멀티레이어드 보호 솔루션과 전략이 최선의 랜섬웨어 대응책입니다.

포괄적인 사이버 레질리언스 프레임워크의 활용

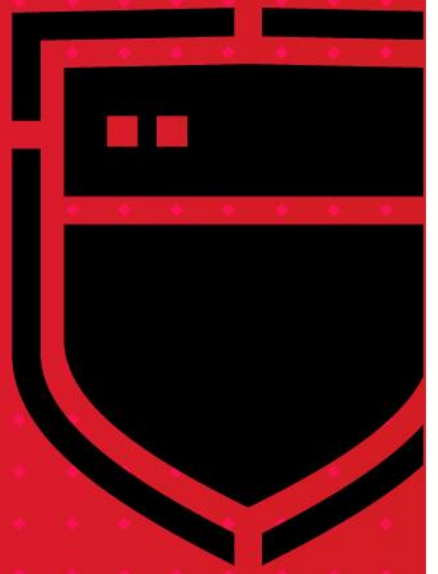
- 전략, 프로세스, 피플, 기술 등 글로벌 베스트프렉티스 기반의 프레임워크를 통해 포괄적인 취약점 개선과 기본적인 Protection룰과 프로세스를 준수할 수 있습니다.

랜섬웨어 대응 및 복구 전문가 그룹의 지원

- 베리타스는 랜섬웨어 대응 및 복구에 있어 수많은 복구 경험과 기술 전문가들로 구성된 글로벌 전문가 그룹입니다.

VERITAS

THANK YOU



VERITAS™