虚拟风险和恐怖主义风险

1. 虚拟风险（Cyber Risk Loss Exposure）：使用互联网会增加组织财产，净收入和责任损失的风险。
2. 财产损失：任何组织都应考虑其cyber risk导致的财产（包括有形财产和无形财产（tangible property and intangible property））损失。普通财险保单中对无形财产损失补偿限额通常不足。
3. 有形材产损失：有形财产包括计算机设备和相关媒介（软件和硬件），其他财产（如现金证券等）也暴露于虚拟攻击下，组织应识别外部攻击（通过email或员工访问外网导致）和内部攻击（员工破坏）。企业网络和软件通常易受攻击。其余有形财产损失还包括安全原因或未授权使用导致的硬件损失（此项可大幅增加企业成本）。
4. 无形财产损失：可分为电子数据（electronic data）损失，商誉（goodwill）损失和知识财产（intellectual property，有经济价值的知识）损失，还包括商标，著作权侵权以及恶意编程破坏（木马病毒）。
5. 净收入损失：企业可通过衡量业务减少量（相当于business interruption导致的decrease revenue and increase expense）来估计cyber risk对于net income的影响。Cyber risk导致的interruption不止影响企业本身，也影响重要客户和供应商。
6. Loss of Business Income: 分为net income和normal operating expense变动，企业应按时创建数据备份。非企业本地或本身的cyber risk对该企业也会有影响（因为其他企业遭受攻击而无法完成订单，此类属于或有损失contingent loss）
7. Extra Expense：除去业务暂停期间正常支出（如继续发员工工资payroll），企业还需发生extra expense来减少business interruption导致的损失，如雇佣额外的工人，购买额外软件硬件用于重建系统。
8. 责任损失：
9. Bodily injury and property damage liability: 可能因为软件问题原因导致身体损伤（如配药公司软件内部开发错误，网站上的健康信息错误）或财务损失（如更新软件导致电脑系统损坏）
10. Personal and advertising injury liability: 此类责任可来源于offense（网站上的语言，如malicious prosecution诉讼, slander, libel, defamation诽谤，disparagement蔑视，or false advertising）。一般cyber risk相关的personal and advertising injury liability 在基础保单中是除外或是受限的。此项案例包括网站广告对产品的不实宣传而导致被消费者起诉。
11. Intellectual property liability：此项责任会影响组织的版权，商标，专利及商业机密等。
12. Error and omission liability: 企业应随时注意其产品（尤其是软件产品）业务操作，起行为可能会导致E&O责任。
13. 虚拟风险损失控制及financing：虚拟风险迅速增长（发生率和损失程度均增长），从内外部影响企业发展（数据窃取损失已经超过physical theft）
14. 虚拟风险损失控制：损失控制的起点为衡量scope of the cyber risk loss exposure（需要风管人员协助）, 相对应的strategy需要符合企业经营和预算目标，并应包括合适的风控手段。此种战略课保护企业资源，减少损失严重程度，加速企业恢复。
15. 物理控制（Physical control）：在cyber criminal和their target之间放置屏障（如安置保安，中控系统，自动检测系统，设置物理接入权限（如针对重点防护区域使用工牌或生物识别biometircs授权）等）
16. 过程控制（procedural control）：用于预防或减少损失（主要是防黑客），主要为创建，实施和定期升级过程控制。此控制在于决定系统和数据如何被保护，应明确系统使用授权，系统接入等级，系统对未授权接入的反应。该控制的主要方式包括密码，杀毒软件，防火墙，数据（储存，传输过程中）加密encryption，防止员工非授权接入不相关网站，建立隐私政策并确定如何在网站发布信息（可防止企业遭受隐私方面诉讼及trademark和copyright方面诉讼）。
17. 人员控制（personnel control）：员工的attitude, performance, behavior可置企业于cyber attack之中（分为无意inadvertently或有意deliberately，但未必会遭到实际损失）。该控制方式包括雇佣前调查pre-employment screening，training, 向雇员明确不可接受的网络行为及相关后果，取消程序（取消授权或密码）。也包括如何处理企业的客户，供应商和邻居关系（防止这些人给企业造成危险，如客户进行病毒或denial-of-service attack）。
18. 管理控制Managerial Control：通过prevent或assist in detection来减小cyber loss，通过集中负责制（centralized responsibility）来进行（设置CIO，CRO，其职责包括检视企业运营的技术问题）。管理控制包括检查cyber risk security plan, ensuring compliance with risk control measure (包括备份文件创建，储存，隔离，防止个人获取整个系统权限)。企业还需不断评估并改进升级措施。
19. 调查和对cyber crime的起诉（prosecution）：企业一般因为害怕公众知道负面消息，担心竞争对手take advantage，认为司法机关不会对其进行协助而选择不报告cyber crime。大多数要求企业披露个人信息泄露或其它虚拟犯罪的情况。
20. 时候快速回复系统（Post-Cyber incident rapid recovery program）：通过恢复运营来减少企业cyber loss severity（主要针对preserve and sustain net income），具体包括在另外地点进行系统全备份（网站，邮件，链接），重要法律技术文档等需要存储于防火，off-site仓库（如独立的数据公司），建立预防性措施（contingency measure，包括提供设备，软件及人力进行分析，修复，清洗和恢复受损文件），还应包括维护好公众关系（public relationship）
21. 虚拟风险损失financing：risk-financing包括事前（pre-loss）和事后(post-loss)安排。主要包括insurance，noninsurance risk transfer和自留（retention）
22. 保险：cyber risk cost很高，保险保单处于发展过程中。
23. 非保险风险转移：合同和协议中需要谨慎措辞以防止其损失，如hold-harmless agreement, indemnity agreement。软件厂商常用liability disclaimer（安转软件前用户必须同意或电子签名。无法完全转移其风险，但可限制其liability scope）。
24. 自留：主要好处为鼓励risk control（防止道德风险），坏处为损失不确定性可能严重影响企业财务情况。自留应将风险限制在企业可接受的范围内，超出承受范围的使用其他方式（如保险）转移。
25. 虚拟风险保险保单：传统保单不承保cyber risk或不能提供足额保障。保险公司开始在管理责任保单中提供网络责任保障。各公司保单不一致，但一般都提供first-party-only coverage (property and theft)和/或third-party-only (liability)保障。First-party-only难遇衡量cyber risk且难于quantify，所以普边度不高。
26. Insuring Agreement：各家公司的保障范围也不同，释义也有区别，需要根据客户实际情况进行改变，有的保险人提供标准化模板并包含可选保障。一般包含如下几项保障：
27. 电子数据保护：承保复原数据的成本
28. 虚拟敲诈（cyber extortion）：承保network kidnap/ ransom event导致的费用损失
29. cyber crime：承保theft of money/ security and intangible property损失，一般由computer attack/ fraud导致
30. 通知及补救（notification or remediation）：承保cyber risk loss之后危机公关相关费用
31. 业务中断（business interruption）：承保loss of business income, loss of contingent business income and payment of extra expense损失，有时只承保business income loss。
32. 网络安全责任：承保被保险人网络安全问题（如被恶意malware入侵，denial-of-service）而导致的责任风险。
33. 隐私责任：承保未授权公开或使用隐私信息（即被保险人未能遵从隐私协议或法案，如Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act or any anti-identity theft legislation）的责任风险，此风险通常由netwrok security breach or unauthorized access or use information导致。
34. Electronic Media Liability：承保被保险人电子内容（邮件，网站，BBS消息）导致的责任。此项责任可分为口头或书面发生的error and omission.
35. 技术error and omission责任：承保被保险人产品或服务因为negligent act, error, omission导致的责任损失。根据具体承保协议，此项责任也适用于被保险人的independent contractor’s employee.
36. Intellectual property liability：承保被保险人未能按授权使用约定被保险人商标，商业机密，著作权或专利而导致的责任损失。
37. Terrorism coverage：cyber risk保单必须承保certified act of terrorism (defined in TRIA)，保险人也可扩展恐怖责任。
38. Coverage Trigger：cyber risk保单触发机制通常为claim-made（即被保险人或正常人第一次知晓保险事故发生开始），所以保单通常会有回溯期（retroactive date，可保单中约定或根据批单添加）。Media liability, intellectual liability, technology-related coverage一般采用发生制。
39. 除外责任：各家公司均不一样，但一般分为如下几类：
40. 一般除外：其他error and omission专业保单中也可出现的除外责任，如dishonest, fraudulent, criminal, malicious act, intentional act, SEC violation, unfair competition, punitive damage
41. 产品相关除外：不承保被保险人生产或提供的服务，如产品recall, defect in design, bodily injury, property damage, breach of warranty.
42. 服务及安全相关除外：不承保contractual liability, performance delay, security breach, failure to prevent virus spreading, data theft
43. cyber risk相关除外：通常出现在tech-oriented that have website ownership or as primary operation focus的企业保单中，除外责任包括personal injury, advertising injury, intellectual property and adverse effect on goodwill (商誉)
44. 保险限额：若保单无年限额（annual aggregate limit），则每项责任有单独的限额。有年限额情况下，每项责任也可有单独限额。保单免赔额一般适用于每项责任，每次事故（针对模块化保单）。抗辩费用（defense expense）在保单限额内支付（减小了整体保单的limit）。有的保险人会提供blanket limit用以解决被保险人不知道最大可能风险的问题。
45. 承保区域：所有cyber risk保单承保地区均为全球（单个别保单会不一样，如起诉地会有限制等）。
46. 恐怖主义保险法案（Terrorism Risk Insurance Act, TRIA）：911之后保险人和再保人在商业保单中把恐怖主义列为除外风险。2002年TRIA法案颁布（减轻urban economic instability, lack of growth, job loss），提供terrorism loss federal reinsurance. 2005年TRIA做出修订并通过TRIEA延长2年。2007年TRIEA过期之前，Terrorism Risk Insurance Program Reauthorization Extension Act (TRIPRA)被延长7年执行期。
47. TRIA目的和期限：恐怖主义威胁过于不可估量无法定价，保险人放弃恐怖主义保障。即使有承保价格也极贵。联邦政府要求保险公司进行承保，同时联邦政府建立TRIA（后经TRIEA修改）作为联邦再保计划（但allotted for insurer to find long-term solution被证明不充足）。TRIA通过TRIPRA扩展了7年（TRIPRA应于12/31/2014过期），此期间用于保险业和政府探索管理恐怖风险的替代方式。
48. Certified Act of Terrorism：经Secretary of Treasury（不能将此认证权指定给其他组织）会同Secretary of State and US Attorney General认证才能算做Certified Act of Terrorism。需要满足的条件包括：必须为暴力行为（Violent）或对人身，财产或基础建筑危险的行为；必须导致美国本土或属地内（含波多黎各）的损失；必须对美国民众造成威胁或影响美国政策或政府行为；所造成的财产损失超过5 million美元。2007年扩展法案约定恐怖袭击包括国内恐怖袭击和foreign act of terrorism in US.若国会（congress）已经宣战（war declared）的不作为恐怖行为。TRIA不要求保险人提供nuclear, biological, chemical or radiological (NBCR)保障（此类风险无法准确预知其长期影响）。TRIPRA还包括对NBCR风险的研究需求。
49. TRIA不适用的产品线：除去如下业务，其他所有业务TRIA法案均适用。不适用的产品线包括：商业车，专业责任（但是D&O适用TRIA），burglary and theft, farmowner multi-peril, crop, private mortgage, medical malpractice, financial guarantee, life and health, flood coverage under NFIP, reinsurance, surety
50. Make-available条款和disclosure requirement：TRIA包含make-available条款（需要保险人必须提供未免除恐怖袭击风险的条款（即可承保恐怖风险的条款）at the time of initial offer, purchase and renewal of insurance）。为遵从此条，保险人必须告知policyholder承保恐怖风险的价格，同时告知保险人和联邦政府对certified act of terrorism的总责任限额不超过100 billion/年，如果当年赔付额超过此总限额则被保险人的coverage将会下降。
51. Federal Participation Trigger：只有自然年度内行业对单一certified act of terrorism累计赔付超过100 million时，联邦才会启动reinsurance程序（certified act需要满足赔付超过5 million，但只有赔付超过100 million时，保险人才能从联邦政府得到补偿）
52. 风险共担条款和项目上限（program cap）：TRIA的Loss-sharing明确了保险人和政府各自责任（明确保险人需要赔偿一定额度后，联邦才开始进行补偿。免赔额以下保险人负担，免赔额之上，保险人和政府按quota-share进行风险分担）。具体分担条款为：保险人的免赔额为其上年度direct earned premium的20%；保险人赔付超过免赔额之后的15%，政府赔付超过免赔额之后的85%；保险人及政府加总的总限额为100 billion；Treasury Secretary必须开发一套在赔付超过100billion之后决定100billion之下的损失分配额（按pro-rata）的机制（process）（此项会减少被保险人的保障）；保险市场总自留额为27.5billion（包括所有免赔额和quota-share额度）。Secretary of Treasury 必须在总赔付限额即将超过100 billion前15天通知国会。若一个自然年度内赔付额不到保险市场总自留限额，则保险人需要将联邦损失限额进行扣减。
53. 恐怖主义批单-针对财产和责任险保单：ISO发展出多个针对commercial coverage的批单，National Council on Compensation Insurance (NCCI)发展出多项针对worker compensation的批单
54. Disclosure批单：出新保单或续保时，TRIA要求保险人向policyholder告知terrorism保障的成本和限制，其中包括：告知分摊到恐怖风险上的保费并列明相关保险责任，告知联邦政府对恐怖风险承担的责任（保险人免赔额超出后，联邦承担85%的责任直到到达项目总限额），告知TRIA项目总限额（100billion）并必须告知如果总限额超出后赔付额会减少。对于ISO保单，policyholder可拒绝恐怖保障并可寻求保险人提供的其他恐怖风险批单。
55. Cap批单：ISO commercial line manual需要保险人增加告知gap批单。该批单明确告知作为certified act of terrorism的条件（同TRIA中描述），告知若自然年度上限（100billion）到达保险人的赔付责任将终止，同时Treasury Secretary将强制根据pro-rata计算限额下每个被保险人的赔付额（此项有可能降低policyholder的保障），告知该项目限额不适用于未被认定为certified act of terrorism的恐怖袭击。
56. Certified Act Exclusion批单：若被保险人拒绝了保险人提供的TRIA保障，则其即使受到certified act of terrorism袭击也不受保障（但未certified的恐怖袭击还是可保的）。Standard Fire Policy（SFP）不包含在该批单内，所以是可承保
57. NBCR除外批单：该批单用于除外由NBCR（nuclear, biological, chemical, radiological）直接或间接导致的损失，若被保险人拒绝certified art of terrorism保障后，保险人可出示此批单。
58. Limitation批单：policyholder拒绝certified act of terrorism保障后，保险人可出示词批单用于减少保险限额从而减少policyholder的保费负担
59. Aggregate Limit批单：用于特定的commercial liability coverage，此项先定了保险人的风险并提供有限限额，用以降低policyholder保费负担（只能在其拒绝certified act of terrorism保障后出示）。该批单用于commercial general liability/ farm liability保单时，限额适用于bodily injury, property damage, personal and advertising injury, medical payment；该批单用于product/ completed operation liability保单时，限额仅适用于bodily injury and property damage；该批单用于其他保单时，限额仅限于general aggregate and product/ completed operation aggregate limit,原分项保额不变。
60. Punitive Damage除外批单：除外恐怖相关的惩罚性损失
61. 其他行为除外批单：用于除外非认证的发生在美国之外的恐怖袭击，只用于commercial liability保单。该除外批单必须满足如下之一：所有损失（包括营业终端）超过25million；50个及以上人员伤亡；恐怖行为涉及核武器（辐射污染），生物化学武器
62. Auto Coverage批单：TRIA不适用于车险。该批单用于承保或除外恐怖行为
63. Worker compensation批单：TRIA适用于Worker Compensation，且各州禁止将恐怖风险在worker compensation保单中除外或作限定，所以很少有恐怖危险相关的批单。NCCI开发的此批单用于告知policyholder恐怖风险保费，告知被保险人的损失为恐怖袭击导致的任何损失，告知保险人的免赔额。