



# 中华人民共和国国家标准

GB/T 45576—2025

## 网络安全技术 网络安全保险应用指南

Cybersecurity technology—Guidelines for application of cybersecurity insurance

2025-04-25 发布

2025-11-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布



目 次

前言..... III

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 网络安全保险应用概述..... 2

    4.1 目的和作用..... 2

    4.2 主要角色与责任..... 2

    4.3 基本应用流程..... 4

5 网络安全保险保障范围..... 5

    5.1 概述..... 5

    5.2 事件类型..... 5

    5.3 损失类型..... 6

6 投保前风险评估..... 6

    6.1 确定保险需求..... 6

    6.2 实施风险评估..... 7

    6.3 保险核保与定价..... 9

7 保险期间风险控制..... 9

    7.1 日常风险管理..... 9

    7.2 保险人风险控制..... 9

    7.3 实施风险控制..... 10

8 出险后事件评估..... 10

    8.1 应急响应与索赔..... 10

    8.2 实施事件评估..... 11

    8.3 保险理赔..... 11

附录 A(资料性) 网络安全保险需求及应用场景..... 13

    A.1 网络安全保险需求分析..... 13

    A.2 网络安全保险必要性..... 13

    A.3 网络安全保险应用场景及示例..... 14

附录 B(资料性) 保险业务活动与网络安全..... 16

附录 C(资料性) 网络安全保险其他考虑事项..... 17

    C.1 保险金额..... 17

    C.2 免赔额和免赔期间..... 17

    C.3 常见除外责任..... 17

附录 D(资料性) 基于风险场景的量化分析方法.....18

    D.1 风险场景示例.....18

    D.2 风险量化分析示例.....18

参考文献.....20

## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京源堡科技有限公司、国家工业信息安全发展研究中心、中国电子技术标准化研究院、中国人民财产保险股份有限公司、中国信息安全测评中心、公安部第一研究所、国家计算机网络与信息安全管理中心、公安部第三研究所、国家信息技术安全研究中心、国家信息中心、中国网络空间研究院、中国科学院信息工程研究所、中国信息通信研究院、中国太平洋财产保险股份有限公司、中国平安财产保险股份有限公司、中国财产再保险有限责任公司、中国人寿财产保险股份有限公司、建信财产保险股份有限公司、国任财产保险股份有限公司、诚泰财产保险股份有限公司、前海再保险股份有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、北京中测安华科技有限公司、中电长城网际系统应用有限公司、蚂蚁科技集团股份有限公司、北京京能信息技术有限公司、深信服科技股份有限公司、广州竞远安全技术股份有限公司、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司、北京天融信网络安全技术有限公司、国网思极网安科技(北京)有限公司、北京威努特技术有限公司、远江盛邦(北京)网络安全科技股份有限公司、长扬科技(北京)股份有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司。

本文件主要起草人：陈幼雷、梁露露、韩冰、李强、孙倩文、王秉政、王惠莅、王建勇、刘敏、王海洋、宋璟、姜伟、胡光俊、李秋香、韩煜、刘明、陈妍、曹岳、王笑强、王佳慧、宋首友、刘玉岭、廖剑、孟楠、戴方芳、雷兴华、刘愉、刘怡、周俊华、李君杰、房珊、李萌、沈铭新、吕晔楠、袁捷、邱勤、韩浩、常文娟、张兴、赵远杰、李季、胡维、何武红、丁雨晗、李森、白晓媛、殷国强、孔勇、何刚、欧阳周婷、刘玉荟、张静、李祉岐、李之云、权晓文、任高锋、汪义舟、安锦程、来泽枫。



# 网络安全技术 网络安全保险应用指南

## 1 范围

本文件描述了网络安全保险的目的和作用、主要角色和责任,给出了基本应用流程、保障事件类型和损失类型,提出了网络安全保险应用各阶段的方法。

本文件适用于组织购买和使用网络安全保险以及网络安全保险机构开展网络安全保险业务,应用网络安全保险的其他相关方参考执行。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改版)适用于本文件。

- GB/T 20984—2022 信息安全技术 信息安全风险评估方法
- GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
- GB/T 22081—2024 网络安全技术 信息安全控制
- GB/T 36687—2018 保险术语

## 3 术语和定义

GB/T 36687—2018 界定的以及下列术语和定义适用于本文件。

### 3.1

#### 网络安全保险 **cybersecurity insurance**

承保因发生网络安全事件所造成的经济损失以及需承担的法定赔偿责任的一种财产保险。

注:网络安全保险属于广义的财产保险范畴,数字资产等无形资产可作为该险种的保险标的。

### 3.2

#### 保险人 **insurer**

与投保人订立保险合同,并按照合同约定承担赔偿或者给付保险金责任的保险公司。

[来源:GB/T 36687—2018,2.4]

### 3.3

#### 投保人 **applicant**

与保险人签订保险合同,并按照保险合同负有支付保险费义务的主体。

[来源:GB/T 36687—2018,2.5,有修改]

### 3.4

#### 被保险人 **insured**

与保险人分担网络安全风险的主体,其财产受保险合同保障,享有保险金请求权。

[来源:GB/T 36687—2018,2.6,有修改]

注:投保人可以为被保险人。

### 3.5

#### 保险标的 **subject of insurance**

作为保险对象的财产及其相关利益或在保险合同中所载明的对象。

[来源:GB/T 36687—2018,2.22,有修改]

3.6

**财产保险 property insurance**

以财产及其有关利益为保险标的的保险。

[来源:GB/T 36687—2018,2.2]

注:财产保险包括财产损失保险、责任保险、信用保险、保证保险等。

3.7

**服务方 service provider**

为网络安全保险业务提供风险评估、风险管理、安全检测、应急响应、事件评估、理赔查勘、法律咨询等专业服务的机构。

注:在网络安全保险业务中,保险人或被保险人均可根据实际需求委托服务方开展相关服务。

3.8

**网络安全保险单 cybersecurity insurance policy**

网络安全保险合同成立后,保险人向投保人签发的保险合同的正式书面凭证。

[来源:GB/T 36687—2018,5.3.1,有修改]

3.9

**第三者 the third party**

除了投保人、被保险人、被保险人的高级管理人员和任何雇员以外的其他自然人或法人。

**4 网络安全保险应用概述**

**4.1 目的和作用**

网络安全保险是一种风险处置手段,其目的是帮助组织管理风险、增强风险应对能力,对组织因网络安全事件导致的经济损失进行补偿。网络安全事件所造成的经济损失既包含组织自身的损失,也包含对第三者的赔偿责任。

与传统财产保险以有形财产及其相关经济利益为保险标的不同,网络安全保险的保险标的既包括有形财产,也包括无形财产。网络安全保险主要承保网络空间的安全风险,如遭受网络攻击、恶意程序(病毒)感染、数据泄露、系统功能错误或失效等。

网络安全保险的作用如下所述:

- a) 补偿网络安全事件所导致的经济损失,降低潜在影响;
- b) 预防和减少网络安全事件所造成的损失和危害;
- c) 为应急响应及恢复提供资金支持;
- d) 协助组织恢复正常运行;
- e) 提高对网络安全风险的抵御能力;
- f) 降低网络安全风险管理的总体成本。

网络安全保险需求和应用场景见附录 A。为方便表述,以下将组织称为投保人或被保险人。

**4.2 主要角色与责任**

**4.2.1 主要角色**

网络安全保险应用主要角色及相互关系如图 1,具体如下所述。

- a) 保险人:

保险人承保被保险人或投保人网络安全风险,并为其提供相关服务,宜包括风险评估和核保,协助



被保险人进行风险控制、应急响应、事件评估、理赔勘察等服务；同时保险人宜接受服务方的服务，保险人通常是指保险机构。

b) 投保人：

投保人投保网络安全保险，向保险人支付保费，宜接受保险人和服务方的服务，当投保人为自己投保时，投保人即被保险人，投保人为其他法人主体投保时，投保人和被保险人是不同法人主体。

c) 被保险人：

被保险人与保险人分担网络安全风险，有保险金请求权，宜接受保险人和服务方的服务。

d) 服务方：

宜为保险人、被保险人或投保人提供网络安全保险应用相关服务；服务方宜受保险人或被保险人委托；根据服务内容宜将服务方划分不同角色，包括为保险人或被保险人提供风险评估、应急响应、事件评估、损失评估和法律咨询的服务方，以及作为独立第三方角色的检测或仲裁机构等服务方；服务方宜满足相关资质或标准，如提供网络安全服务参考 GB/T 32914—2023。

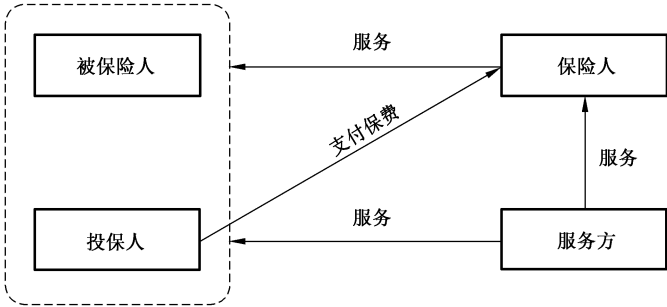


图 1 网络安全保险应用主要角色及相互关系

4.2.2 主要责任

4.2.2.1 保险人

保险人的责任宜包括以下内容。

- a) 对所承保的风险进行核保和定价，在保险期间依据保险合同规定的责任和义务提供服务。
- b) 依据保险合同双方的约定开展风险管理，如协助被保险人实施风险控制，当风险发生显著变化时，通知被保险人并提供处置建议。
- c) 在出险理赔时协助被保险人开展应急响应、事件评估、理赔勘察等服务，并向被保险人说明需要提供的信息。
- d) 对被保险人的相关信息负有保密责任。

4.2.2.2 被保险人

被保险人的责任宜包括以下内容。

- a) 确认网络安全保险需求。
- b) 配合保险人或其委托的服务方实施风险评估。
- c) 保险期间开展必要的风险管理活动。
- d) 出险后开展必要的应急响应工作，避免损失扩大。
- e) 向保险人提供事件评估结果及相关日志等数据。
- f) 出险后在约定时间内通知保险人。

4.2.2.3 投保人

投保人的责任宜包括以下内容。

- a) 根据网络安全保险合同,按期缴纳保险费。
- b) 保险人对保险标的的情况进行询问时,如实告知。


4.2.2.4 服务方

服务方的责任宜包括以下内容。

- a) 对保险标的进行风险评估,支持保险人开展核保和定价。
- b) 协助保险人进行风险控制,如进行风险监测和预警。
- c) 协助被保险人进行事件的应急响应。
- d) 协助保险人对事件进行技术评估和损失影响分析。
- e) 对保险人、被保险人的相关信息负有保密责任。
- f) 提供其他法律诉讼、公关咨询等服务。

4.3 基本应用流程

网络安全保险基本应用流程如图 2,具体如下所述,保险业务中的与网络安全相关的活动可参见附录 B。

- a) 投保前风险评估,此阶段宜包括以下内容。
  - 1) 确定保险需求:被保险人确认保险需求,包括投保的风险和损失类型、保障的额度以及保险费用预算等。
  - 2) 实施风险评估:服务方实施风险评估,被保险人宜配合提供必要支持。
  - 3) 保险核保与定价:保险人根据风险评估结果进行核保并制定保险方案,包括保障范围、保险额度、保险费用等。当保险人拒绝承保时,被保险人根据风险评估结果进行整改或调整保险需求。
- b) 保险期间风险控制,此阶段宜包括以下内容。
  - 1) 日常风险管理:被保险人开展日常风险管理活动,对相关风险进行监测和处置;保险期间被保险人及时告知风险状况信息,履行风险控制义务。
  - 2) 实施风险控制:服务方实施风险控制,协助被保险人进行风险管理。
  - 3) 风险控制:保险人主动开展风险监测和预防管理等相关活动。
- c) 出险后事件评估,此阶段宜包括以下内容。
  - 1) 应急响应及索赔:被保险人开展应急响应工作,并根据损失情况发起索赔请求。
  - 2) 实施事件评估:保险人委托服务方对网络安全事件进行评估,确定事件责任和实际损失。
  - 3) 理赔:保险人根据评估结果做出赔偿决定,履行保险人的赔偿责任。

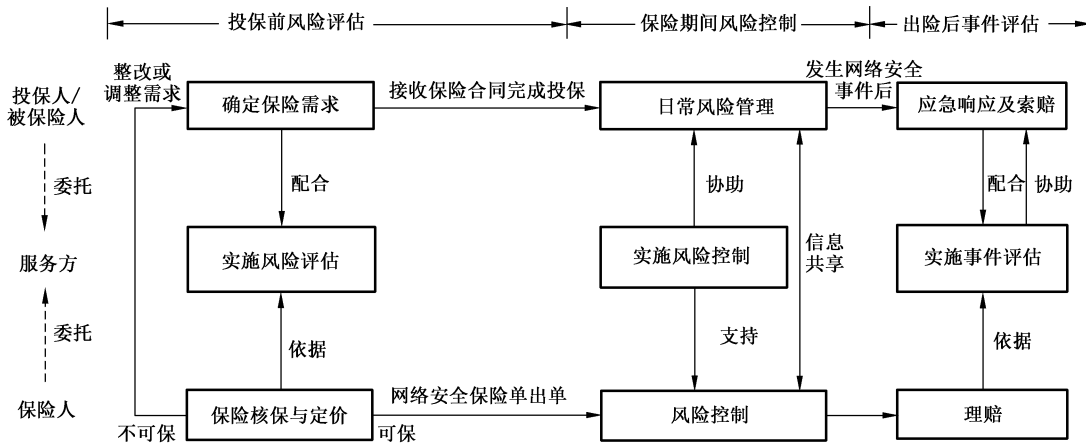


图 2 网络安全保险基本应用流程

5 网络安全保险保障范围

5.1 概述

网络安全保险保障范围包括可承保的网络安全事件和损失类型。只有当发生在保险保障范围内的网络安全事件和损失时,即构成保险事故,才能通过保险进行赔偿。

网络安全事件宜包括恶意程序事件、网络攻击事件、数据安全事件、违规操作事件等,具体事件类型宜参考 GB/T 20986—2023。损失类型宜包括第一方损失和第三者责任,第一方损失包括被保险人自身造成的直接经济损失以及应急响应所产生的费用等,第三者责任包括被保险人因网络安全事件引发的对第三者(例如受影响个人或机构等)的法定赔偿责任。

保险保障范围在网络安全保险单中说明,网络安全保险其他考虑事项见附录 C。

5.2 事件类型

网络安全保险可承保的事件宜包括以下类型。

- a) 恶意程序事件:指因蓄意制造或传播恶意程序,使被保险人的系统造成损害,导致其业务损失或其他经济影响的事件,包括计算机病毒、网络蠕虫、木马、勒索软件、挖矿病毒事件等。
- b) 网络攻击事件:指因通过网络实施的攻击或入侵行为,使被保险人的系统造成损害,导致其业务损失或其他经济影响的事件,包括网络扫描探测、网络钓鱼、漏洞利用、后门利用、拒绝服务、信号干扰、域名劫持、供应链攻击事件等。
- c) 数据安全事件:指因对数据实施的攻击行为,使被保险人的数据造成损害,导致其业务损失或其他经济影响的事件,包括数据篡改、数据假冒、数据泄露、数据窃取、数据滥用、隐私侵犯、数据投毒、数据丢失、数据损坏事件等。
- d) 违规操作事件:指因人为意外或无意的行为,使被保险人的系统造成损害,导致其业务损失或其他经济影响的事件,包括误操作或其他违规操作事件等。
- e) 其他可能造成系统或资产损失的事件,包括设备设施的技术故障、网络欺诈、媒体侵权、电信诈骗事件等。

通常不可承保的事件类型见 C.3。

### 5.3 损失类型

#### 5.3.1 第一方损失

##### 5.3.1.1 业务中断损失

业务中断损失指因网络安全事件导致的停产、停业或经营受到影响而面临的预期利润损失及必要的费用支出。业务中断损失还包括因运营效率降低导致延迟交付所产生的经济损失。

##### 5.3.1.2 应急响应费用

应急响应费用指在网络安全事件发生后所执行的应急响应活动产生的费用,宜包括以下内容。

- a) 事件评估费用:如聘请服务方对事件发生原因进行评估所产生的费用。
- b) 数据和系统恢复费用:对事件中受影响的数据和系统进行恢复、更新、重建或替换等活动所产生的费用。
- c) 危机公关费用:为减少声誉影响所产生的危机公关的费用,如聘请公共顾问的咨询费用和进行沟通的成本等。
- d) 通知费用:当事件造成个人信息泄漏、篡改、丢失的,由被保险人通知受影响的个人或组织所产生的费用,包括通知的人工成本及呼叫中心运营成本等。
- e) 法律咨询服务费用:当事件涉及法律和监管要求,被保险人聘请法律顾问进行咨询所产生的费用。
- f) 其他必要合理费用:如管理应急响应流程所投入的运营成本以及可能产生的人员更换等费用。

##### 5.3.1.3 网络勒索损失

网络勒索损失包括被保险人因遭受勒索软件事件后所产生的损失和相关费用,宜包括数据恢复、事件评估、谈判及其他合理必要的处置等费用。

#### 5.3.2 第三者责任

网络安全事件导致被保险人对第三者损失的赔偿责任,宜包括但不限于以下内容。

##### a) 数据泄露责任

因网络安全事件,导致用户数据泄露,需要承担的赔偿责任、相关法律诉讼等费用。

##### b) 网络安全责任

因网络安全事件,导致其合作伙伴或所服务用户发生经济损失,需要承担的赔偿责任、相关法律诉讼等费用。

##### c) 媒体责任

因网络安全事件,导致被保险人发布在线媒体内容(包括网站、博客和社交媒体等)存在不当行为,被第三者提出索赔而产生的法律费用、赔偿及公关费用等损失。

### 6 投保前风险评估

#### 6.1 确定保险需求

##### 6.1.1 风险自评估

被保险人在投保前宜开展风险自评估,针对网络安全保险保障范围中的事件类型和损失类型,评

估网络安全事件发生可能性和损失大小。风险评估结果是制定风险转移策略的依据。

被保险人若不具备风险自评估能力,宜根据保险人的风险评估结果确定保险需求。

### 6.1.2 制定风险转移策略

被保险人宜制定风险转移策略,确定适合通过保险转移的风险,主要考虑以下因素:

- a) 风险容忍度,选择对业务影响较大的,超出承受范围的风险;
- b) 高额损失优先原则,选择发生概率低,但损失较大的风险;
- c) 风险处置的总体成本,风险转移策略应使总体成本更优。

### 6.1.3 确定保险需求

被保险人宜根据风险转移策略提出保险需求。保险人宜根据已有的网络安全保险产品制定保险方案,如果网络安全保险产品无法满足保险需求,被保险人宜与保险人协商,根据需求开发新的网络安全保险产品。保险人宜根据确定的保险需求对被保险人实施风险评估。

被保险人宜根据保险人提供的保险方案确定保险需求。

## 6.2 实施风险评估

### 6.2.1 评估范围

风险评估范围与保险标的相关,保险标的通常是被保险人的全部信息系统或资产,或者是被保险人选定的特定系统或资产。保险人宜委托服务方实施风险评估,实施风险评估时宜围绕保险保障范围列明的事件类和损失类型,评估网络安全事件发生的可能性及其带来的损失大小。

### 6.2.2 评估内容

#### 6.2.2.1 网络安全能力

宜评估被保险人实施安全控制措施的效果,以及法律法规方面的符合情况。被保险人开展的网络安全认证、检测和风险评估等活动的结果宜作为网络安全能力评估的参考。安全控制措施直接影响发生网络安全事件的可能性和损失大小,通过网络安全能力评估能够衡量被保险人风险防范水平。

#### 6.2.2.2 网络安全风险

网络安全风险评估宜围绕保险保障范围中的第一方损失和第三者责任,评估可能造成不同类型损失的各类网络安全事件发生的可能性以及损失大小。评估网络安全风险时,宜同时考虑数据安全风险,识别数据资产和数据处理活动中的威胁和控制措施等风险要素,分析数据安全事件发生的可能性以及损失大小。

#### 6.2.2.3 行业风险水平

宜评估被保险人所属行业的宏观风险状况,包括行业信息化程度、网络安全威胁程度、业务特点等间接影响风险发生的可能性和损失大小。行业风险水平评估宜包括但不限于以下内容:

- a) 行业面临的网络安全威胁特征;
- b) 行业不同规模企业的安全能力水平;
- c) 行业不同规模企业的信息化程度和业务活动特征;
- d) 被保险人组织规模、业务规模在行业中所处的位置;
- e) 被保险人的安全风险水平在行业中所处的位置;

- f) 被保险人受行业监管的要求等。

### 6.2.3 评估方法

#### 6.2.3.1 概述

投保前风险评估方法宜参考 GB/T 20984—2022,包括风险识别、风险分析、风险评价等主要过程。在风险分析环节,宜采用定量分析方法,通过评分或货币化等数值方式表示风险大小,满足保险核保和定价要求。在评估与数据安全事件等相关的安全风险时,宜根据数据安全风险评估方法,对数据资产和相关处理活动等进行要素识别和风险评估。

#### 6.2.3.2 风险识别

风险识别的内容宜包括以下内容。

- a) 识别资产、脆弱性、威胁主体、攻击方法等风险要素;涉及数据安全风险的考虑数据、业务、数据处理活动等风险要素。
- b) 识别安全控制措施及其有效性,通过问卷、访谈、检查、测试等方式进行识别;识别控制措施参考 GB/T 22081—2024,并重点识别与风险场景相关的控制措施。
- c) 识别风险场景,风险场景由威胁主体、资产、脆弱性、攻击方法、安全事件等要素组成,风险场景与网络安全保险保障范围相结合;识别风险场景时参考保险保障范围中列明的损失类型,如业务中断、数据泄露、网络勒索等,具体示例参考附录 D 的 D.1。
- d) 识别行业风险数据,包括被保险人所属行业的资产和业务特征,历史安全事件及损失数据,对行业影响较大的威胁和脆弱性等。

#### 6.2.3.3 风险分析

##### 6.2.3.3.1 网络安全能力分析

在安全控制措施识别的基础上,宜对不同的控制措施项进行赋值并计算安全能力值。安全能力宜通过评分或等级等形式表示,评分或等级越高代表安全能力水平越高,发生网络安全事件可能性越低。

宜通过分析控制措施的有效性为各评分指标赋予分值和权重,结合被保险人行业、规模等因素,计算安全能力评分。网络安全相关测评、认证或资质等宜作为安全能力分析的参考因素。

##### 6.2.3.3.2 网络安全风险分析

在识别资产的基础上,宜采用安全评级的方式,定量分析被保险人网络安全风险。安全评级一般通过非侵入式或侵入式手段收集资产及脆弱性等数据,采用大数据分析及威胁情报等技术,从网络、应用、数据等多个维度,计算安全风险的评分。安全评级结果反映了被保险人风险暴露状况,便于保险人进行风险筛选和核保。

##### 6.2.3.3.3 行业风险水平分析

行业风险水平分析宜采用统计方法,对不同行业、不同规模样本企业进行安全评级分析,结合行业风险数据,评估行业风险水平。行业风险水平分析宜采用风险象限图或行业风险地图等形式,从行业、规模维度进行行业风险水平划分。行业风险水平分析结果宜作为核保和定价参考因素。

##### 6.2.3.3.4 风险量化分析

在风险识别的基础上,宜对所建立的风险场景进行风险分析和计算。风险量化分析宜通过货币化



数值的形式衡量风险大小。

风险量化分析宜根据国家网络和数据安全相关法律、法规及政策要求,参考具有相关资质的第三方专业机构开展的网络安全认证、检测及风险评估的结果。

风险量化分析宜对构成风险场景的要素和损失进行赋值,并通过量化分析模型分析各风险场景发生的概率和损失大小,计算各场景的风险值,再对各风险场景聚合计算整体风险值。一种基于风险场景的风险计算示例见 D.2。风险量化分析结果宜用于保险核保和定价。

#### 6.2.3.4 风险评价

风险评价是对风险分析的结果进行等级、排序、统计等评价的过程,以便应用于保险核保和定价中。风险评价宜包括下列方式。

- a) 等级划分:汇总资产风险、业务风险及相关工作文档,对风险分析结果进行等级划分,为保险人根据风险等级进行核保时提供参考。
- b) 风险排序:对风险分析结果按照数值大小进行排序,根据风险场景的量化分析结果进行排列,保险人根据结果确定主要风险场景的风险大小,为不同场景下损失赔偿限额提供参考。
- c) 统计分析:对风险量化分析结果进行统计分析,如损失的概率分布和损失大小百分位统计等,为保险人确定保障限额和保费提供参考。

### 6.3 保险核保与定价

保险人宜根据风险评估结果开展保险核保与定价,判断是否承保相关风险并确定保费及保障限额。保险人自身风险偏好,被保险人的网络安全能力、网络安全评级以及行业风险水平等评估结果宜作为保险人核保和定价的重要参考。

## 7 保险期间风险控制

### 7.1 日常风险管理

保险期内,被保险人宜开展日常风险管理,维护保险标的安全。被保险人宜通过风险管理技术手段及时了解保险标的的风险变化情况,及时发现新增风险并进行处置。

被保险人在业务系统发生变更、信息系统更新,系统出现重大安全漏洞等情况时,宜及时关注风险变化情况,通过日常风险管理手段控制风险。

被保险人宜自主或委托保险人或服务方开展日常风险管理。

### 7.2 保险人风险控制

保险人宜主动开展风险监测和预防管理等风险控制活动,保险人经被保险人同意,协助被保险人控制或管理风险,维护保险标的安全。保险人宜委托服务方或自行开展风险控制活动,具体包括以下内容。

- a) 识别风险变化:通过风险监测等技术手段持续跟踪保险标的的风险状况,识别新增风险或显著变化的风险。
- b) 风险预警和告知:对新增风险、显著变化的风险等情况进行预警,及时通知被保险人进行应急处置。
- c) 风险预防管理:为被保险人提供风险管理咨询、风险排查等服务,协助被保险人开展风险预防管理活动。

## 7.3 实施风险控制

### 7.3.1 风险监测

#### 7.3.1.1 监测对象

风险监测对象宜包括保险标的相关的资产,以及其他对保险标的风险产生较大影响的资产,如供应商和云租户资产等,供应商或云租户发生安全事件也可能导致被保险人的损失。

#### 7.3.1.2 监测内容

风险监测内容宜包括影响保险标的风险变化的因素。实施风险监测的保险人或服务方宜与被保险人协商风险监测内容,以满足风险控制需要。风险监测内容具体如下所述。

- a) 资产:信息系统的重大变更,新系统的部署和运行等。
- b) 威胁:恶意网络资源、攻击方法或漏洞利用手段等。
- c) 脆弱性:重大漏洞或配置不当等。
- d) 暴露面:人员信息、邮箱、代码、互联网协议地址、端口、应用服务等在互联网的暴露情况等。
- e) 行业风险态势:行业重大安全事件,行业相关重大漏洞等。
- f) 其他可能导致风险变化的情况。

#### 7.3.1.3 监测方法

风险监测宜采用不影响被保险人信息系统及业务运行的方式进行,如利用威胁情报分析、资产探测、脆弱性扫描、行业信息收集等技术手段,结合风险分析方法和大数据分析技术,及时分析发现潜在风险变化情况。

### 7.3.2 风险预防管理

风险预防管理是为预防风险发生以降低潜在损失所采取的安全活动,如安全检测、安全意识培训、风险评估、渗透测试、漏洞扫描等。服务方式宜采用远程或现场服务方式。服务方宜确保服务人员、过程和工具的安全可控。

### 7.3.3 风险信息告知

被保险人宜向保险人或服务方告知可能引起风险变化的相关信息,以便保险人开展风险控制活动。风险信息严格用于风险控制活动中,保险人和服务方宜确保信息的安全。主要包括以下风险信息:

- a) 被保险人在保险期内自行开展或购买的网络安全服务,如网络安全认证、安全检测和风险评估等;
- b) 被保险人重大的系统变更、更新和维护信息;
- c) 被保险人供应链服务或系统的重大变更;
- d) 被保险人业务范围、组织架构、网络拓扑等重大变更;
- e) 其他可能影响被保险人网络安全风险变化的信息。

## 8 出险后事件评估

### 8.1 应急响应与索赔

被保险人出险后宜及时开展应急响应工作抑制事件的影响,降低损失,并在约定的时间内向保险



人提出赔偿请求。具体包括以下内容。

- a) 开展应急响应:及时开展应急响应工作,降低事件所造成的损失,并分析事件原因和影响。
- b) 提出赔偿请求:在约定时间内向保险人通知网络安全事件的信息,提出赔偿请求。
- c) 配合保险人理赔:配合保险人进行事件评估,提供应急响应工作说明或日志等信息。

被保险人在投保前宜与保险人沟通明确理赔流程,包括约定的时间和其他需要提供的信息。被保险人宜自行或委托服务方开展上述工作。

## 8.2 实施事件评估

### 8.2.1 安全事件分析

保险人宜针对被保险人报告的保险事故进行分析评估,包括事件溯源以及影响分析等,并出具分析报告。保险人宜根据分析结果确定保险责任,并为损失赔偿提供参考。

事件分析报告宜包括以下内容。

- a) 发生时间:确定事件发生的时间是否在网络安全保险合同有效期内。
- b) 发生地点:确定事件发生的地点是否在网络安全保险合同规定的范围内。
- c) 发生原因:确定事件发生的原因,并分析是否在网络安全保险合同规定的保障范围内。
- d) 事件发生后的应急响应及处置的情况。
- e) 与事件相关的安全防护措施的有效性评估。
- f) 事件对被保险人造成的影响。
- g) 其他网络安全事件信息。

当保险事故存在多个原因时,保险人宜根据近因原则确定保险事故原因,也即造成损失最直接、最有效,起主导作用的原因。保险人承担赔偿责任的范围限于近因造成的损失。因此在事件评估中,宜对造成事件的威胁主体、攻击方法、攻击路径等进行分析,协助保险人判断并确定事件产生的直接原因,以支持保险人做出合理的赔偿决策。若存在被保险人故意等原因导致的保险事故,保险人宜根据除外责任拒绝赔偿。

### 8.2.2 损失影响分析

损失影响分析是通过技术手段收集安全事件对被保险人造成影响的信息,以支持保险人进行损失评估,确定赔偿金额。损失影响分析宜根据事件分析结果确定损失的原因,与事件相关的损失和损失程度,并排查不在保险保障范围内的损失。损失影响分析宜由具有相关资质或能力的第三方专业机构实施。

损失影响分析宜包括以下内容。

- a) 损失项:与安全事件相关的所有类型的损失项,如因系统宕机造成业务无法开展所导致的经营损失,以及所付出的修复成本等。
- b) 损失原因:分析与网络安全事件相关联的损失,排查不相关的损失。
- c) 损失程度:分析并收集与损失程度相关的信息,如缓释和控制风险的费用支出证明和相关工作文件,开展应急响应相关的工作文件和费用支出证明等。

保险人在赔付被保险人的损失后取得追偿权。保险人宜通过事件的溯源分析确定事件责任主体,在保留日志等相关证明材料后,向其追讨赔偿。例如由于竞争对手对被保险人发起网络攻击造成其业务中断损失,保险人宜向其竞争对手追讨赔偿。

## 8.3 保险理赔

保险人在理赔中主要确定事件责任是否属于保险保障范围,并评估损失金额及确定赔付金额。保

险人宜依据事件评估结果进行理赔决策。

保险人在理赔中宜提供相关服务,如应急响应支持、法律支持或公共关系管理等,协助被保险人开展应急响应工作,降低事件影响。保险人宜自行或委托服务方开展保险理赔中的相关工作。

## 附录 A

(资料性)

## 网络安全保险需求及应用场景

## A.1 网络安全保险需求分析

网络安全保险需求来源主要包括以下几个方面。

## a) 作为完善风险管理体系的手段

网络安全风险不能完全消除,网络安全保险是完善风险管理体系的必要手段,能够帮助企业建立风险管理闭环,优化资源配置,降低总体成本。企业在实施风险管理活动中,根据风险评估结果,制定风险转移策略,明确适合通过保险转移的网络安全风险,从而形成网络安全保险投保需求。

对于风险管理意识强,风险防范措施完善的中大型企业,通常考虑将网络安全保险纳入风险管理体系,应用网络安全保险来进一步增强自身的风险抵御能力。

## b) 作为网络安全建设的补充手段

网络安全事件一方面给企业造成直接经济损失,如重要系统中断造成营业收入损失;另一方面企业投入应急处置、恢复经营、处理赔偿和解决法律诉讼案件时会产生高额费用。对于网络安全建设投入相对有限的中小型企业而言,一次严重的网络安全事件造成的损失可能导致企业生存危机或直接倒闭。因此,中小型企业能够通过网络安全保险补充网络安全建设的投入,防范较为严重的网络安全风险。在保险保障期间,中小企业通过保险公司提供的风险管理服务,获得风险监测和预警的能力,也是对自身安全建设的一种补充手段,帮助企业形成相对低成本的安全解决方案。

对于网络安全建设能力不足或投入相对有限的中小型企业,可通过网络安全保险补充网络安全建设投入,当发生较严重的网络安全事件时提供风险保障,降低损失。

## c) 合同要求购买网络安全保险

当企业对外提供产品或服务时,采购方在合同中基于保障自身风险管控的需要,明确要求服务或产品提供方购买网络安全保险。因此服务方为满足合同要求,需要购买网络安全保险。通常在采购电商平台、数据产品等服务时,会存在合同约定的保险要求。

对于具有大量供应商的大型制造业企业,由于供应链引入的安全风险往往对于企业自身造成较大的风险管理成本,因此企业出于自身风险管控的需要,将网络安全保险作为供应链准入的合同要求之一。一旦因供应链安全风险导致企业自身的损失和影响,企业可向供应链企业索赔,此时供应链企业购买的网络安全保险将覆盖该赔偿损失,从而降低了采购方企业的风险。

## d) 为网络安全产品提供信誉保障

网络安全企业为用户提供网络安全产品或解决方案的同时,为网络安全产品或服务投保网络安全保险,当用户因产品防护不当发生网络安全事件所造成的损失,可由网络安全保险赔偿。网络安全企业通过为产品购买网络安全保险的方式,为使用产品的用户提供了额外的风险保障能力,从而增强了用户使用安全产品的信心,提高了安全产品竞争力。

典型面向网络安全产品的保险包括针对勒索软件防护的产品和针对 DDoS 攻击的防护产品等,如勒索软件安全防护保险,保障使用防勒索软件产品的用户在遭受勒索软件攻击时,产生的应急响应费用或处置费用等;DDoS 攻击损失补偿保险主要保障采用抗 DDoS 产品的用户遭到 DDoS 攻击而产生的业务中断损失和应急响应额外费用。

## A.2 网络安全保险必要性

网络安全保险是企业防范风险的有效手段之一,通过损失补偿功能降低企业风险损失,健全企业

网络安全风险管理体系,优化资源配置,降低风险管理总体成本。当前我国处于数字经济高速发展时期,网络安全保险对于保障经济发展、维护社会稳定,防范数字经济风险,具有如下重要意义。

a) 提高社会整体风险管理意识和风险防范能力

网络安全保险产业发展在帮助企业构建完善的风险管理体系的同时,通过风险管理策略制定、风险评估以及风险控制等服务的开展,对企业风险管理意识和风险管理能力提升有极大促进作用,从而提高社会整体风险防范能力。

b) 提高企业经营效率,优化社会资源配置

网络安全保险具备传统财产保险的风险管理和成本管理专业能力,能够为企业提供全面的网络安全风险应对方案,保护核心资产并优化资源配置,帮助企业在最优成本下最大程度防范安全风险,确保企业经营效率的最大化。

c) 促进网络安全新业态发展,提升社会网络安全治理能力

网络安全保险能够满足企业多样化的风险保障需求,进一步促进网络安全产业发展,形成新的网络安全服务和产业生态,扩大网络安全市场规模。网络安全保险市场的发展,使得投保企业、安全厂商、技术服务商和保险机构都能够参与到网络安全产业链中,提高网络安全产业融合发展能力,提升全社会网络安全治理能力。

A.3 网络安全保险应用场景及示例

网络安全保险应用场景及示例如下所示。

a) 企业根据风险管理要求为自身或特定重要业务系统购买网络安全保险

企业根据自身风险管理情况、运营情况、行业安全风险等因素制定网络安全风险转移策略,形成保险需求。保险公司依据自身风险偏好、法律规定、市场惯例等因素为企业多种类型保险产品以满足企业需求。企业根据不同保险产品之间的差异性选择最佳的网络安全风险转移策略。表 A.1 列举了典型的网络安全保险产品和示例。

表 A.1 典型网络安全相关保险产品和示例

保险产品类型	保险保障范围	投保人	被保险人
网络安全财产损失保险	主要承保被保险人因网络安全事件导致的直接经济损失,一般称为“第一方损失”	单独法人单位	投保人同时作为被保险人;或 投保人自身及其相关联公司作为共同被保险人(被保险人不限制数量,在保险单列明即可);或 投保人相关联公司作为被保险人(被保险人不限制数量,在保险单列明即可)
网络安全责任保险	主要承保被保险人因网络安全事件引发的对第三方(受影响个人或机构)的法定赔偿责任,一般称为“第三者责任”		
网络安全综合险	可同时承保被保险人因网络安全事件导致的第一方损失以及第三者责任		

b) 企业为安全产品购买网络安全保险保障使用该产品的用户

网络安全企业为提高安全产品的信誉和竞争力,通过为产品购买网络安全保险的方式,为使用产品的用户提供了额外的风险保障能力。目前市场上典型的可投保的网络安全产品包括防勒索产品、DDoS 攻击解决方案、数据防泄露产品等。网络安全企业将保险作为产品附带的风险保障手段,当使用产品的用户发生网络安全事件产生实际损失后,针对用户可能发生的网络勒索损失、业务中断损失、

应急响应费用、数据安全责任等损失提供补偿。表 A.2 列举了典型保险产品和示例。

表 A.2 典型保险产品和示例

安全产品种类	保险产品类型	保险保障范围	投保人	被保险人
防勒索软件产品	勒索软件安全防护保险	保障被保险人在安装了经保险公司评估认可的防勒索软件的情况下,仍遭受勒索病毒攻击,并由此产生的应急响应费用或勒索处置费用等	销售防勒索软件的安全服务公司;或 购买防勒索软件的最终企业用户	购买防勒索软件的最终企业用户
抗分布式拒绝服务攻击(DDoS)产品或解决方案	DDoS 攻击损失补偿保险	主要保障被保险人遭到基础防护之上的 DDoS 攻击而产生的业务中断损失和为减少业务中断而产生的抗 DDoS 费用	销售抗 DDoS 产品或解决方案的法人单位;或 购买抗 DDoS 产品或解决方案的最终企业用户	购买抗 DDoS 产品或解决方案的最终企业用户



**附 录 B**  
**(资料性)**  
**保险业务活动与网络安全**

网络安全保险的应用与传统财产保险类似,通常包括展业、投保、承保、防灾、理赔等主要业务活动,其中与网络安全相关的活动进行如下简要介绍。

a) 投保

投保也称购买保险,投保人通过保险公司业务人员或保险中介购买保险。网络安全风险评估是投保过程中的重要环节,投保人根据风险评估结果制定风险转移策略,形成网络安全保险实际需求;保险人则根据评估结果判断是否承保相关风险,并为投保人设计满足其风险管理需求的保险方案。一般来说,投保人确定保险需求的首要原则是“高额损失原则”,即某一网络安全事件发生概率较低,但造成的损失较大,应优先投保;相反,如果网络安全事件发生的概率很高,但造成的损失并不严重,则更适合采取网络安全措施降低其风险。

b) 承保

承保是指保险人与投保人双方通过协商,对保险合同内容达成一致并签订的过程。通常保险人需要审核投保人的保险需求,只有符合条件的风险,保险人才同意承保。通过承保过程,保险人能够筛选不可保风险或不合格的保险标的,合理分散风险。承保的目的除了满足保险人自身风险管理要求之外,通过风险识别和筛选,也间接促使被保险人采取措施减低风险,以满足承保要求。因此,保险人在承保时需要详细了解保险标的的风险状况以及可能发生的损失大小等,为决策是否承保以及确定保险方案提供依据。

c) 防灾

防灾是指保险期间的防灾防损活动。保险人与投保人对所承保的保险标的采取措施,减少或消除风险发生的因素,防止或减少网络安全事件造成的损失。网络安全保险中防灾防损的对象是保险标的,防灾防损的方法包括法律、经济、技术等多种手段。在网络安全保险中,由于网络安全风险动态变化特性,对保险标的进行风险监测和预防管理是防灾防损的重要技术手段。在保险期内,网络安全风险可能因为内外部环境变化或技术发展而发生变化,保险人需要采取风险监测和预防管理等技术措施,及时了解被保险人的风险变化情况,并要求被保险人采取相应措施将风险变化控制在合理范围。

d) 理赔

理赔是指保险人在保险标的发生网络安全事件后,对被保险人提出的索赔请求进行处理的行为。网络安全保险中的理赔需要确定引起网络安全事件的原因以及所造成的损失是否在保险保障范围内,同时需要评估损失的金额。在网络安全事件发生后,保险人需要对网络安全事件进行评估,确定损失原因、损失程度、认定求偿权利,并根据评估结果做出赔偿决定,履行保险人的赔偿和给付保险金的责任。





## 附录 C

(资料性)

## 网络安全保险其他考虑事项

## C.1 保险金额

针对网络安全保险保障范围,对其中的每一项内容,投保人或被保险人需仔细确定并考虑要获得多少保障额度,它也是计算保险费的依据。投保人或被保险人能够获得的网络保险保障额度取决于其营业额、行业、运营和该项保障范围的风险大小。

## C.2 免赔额和免赔期间

投保人需要了解网络安全保险中的免赔额和免赔期间,每次事故免赔额(率)和免赔期间由投保人与保险人在签订保险合同时协商确定,并在保险合同中说明。

## C.3 常见除外责任

网络安全保险并不能覆盖所有风险情况,一般通过保险合同条款中的除外责任来约定不可保的事件或损失,常见除外责任包括但不限于以下内容。

- a) 身体伤害和有形的财产损失:自然人的身体伤害或精神损害,以及有形的物质财产损失一般被排除在网络保险保障范围之外,但保险人与被保险人可以在保单中约定将有法院判决的精神损害纳入到保单保障范围中。
- b) 网络战争:通常与网络战争相关的行为,或针对网络的恐怖主义行为等所导致的损失及赔偿责任会被排除在外。
- c) 不当行为:包括被保险人高级管理人员及其雇员所做的任何不诚实、欺诈或故意的不当行为,或其他能够让被保险人得到原本依照法律法规、被保险人经营规则或其他相关规定不能获得的利益的行。
- d) 违法行为:因被保险人违反法律或法规要求的行为而引起的网络事故损失除外。
- e) 惩罚责任:由于网络安全事件,国家行政机关对被保险人的罚金、罚款或惩罚性赔偿等惩罚责任不在保单保障范围内。
- f) 侵犯知识产权或商业秘密责任:被保险人侵犯知识产权或商业秘密的责任由其他保险产品覆盖,不在网络安全保险单承保范围内。
- g) 自然灾害和不可抗力:自然灾害、不可抗力或超出双方合理控制范围的特殊事件或情况,如洪水、地震、泥石流、雷击、台风、海啸、火灾以及罢工、暴动、犯罪、流行性疾病等通常被排除在网络安全保险保单承保范围之外。

## 附录 D

(资料性)

## 基于风险场景的量化分析方法

## D.1 风险场景示例

典型的网络安全事件风险场景如下所示。

## a) 网络攻击导致业务中断的风险场景

黑客组织(威胁)利用信息系统访问未进行流量控制(脆弱性)的弱点,对投保人实施拒绝服务攻击(攻击方法),造成投保人业务系统(资产)无法正常访问(安全事件),从而给投保人造成业务中断的影响(损失);该风险场景代表了典型的网络攻击事件造成业务中断的风险,而识别风险场景中所涉及的不同要素的组合,能够建立与网络攻击事件相关的风险场景,从而能够评估网络攻击风险的大小。

## b) 恶意程序导致网络勒索的风险场景

黑客组织(威胁)通过发送带有勒索病毒附件的钓鱼邮件(攻击方法),内部人员因安全意识薄弱(脆弱性)点击附件导致终端及内部重要系统遭受勒索病毒攻击(安全事件),导致投保人重要业务系统及运行数据(资产)被加密,造成投保人的业务系统无法正常访问,影响投保人的正常工作效率,同时产生系统恢复费用(损失);该风险场景代表了典型的恶意程序事件造成的网络勒索或业务中断的风险,识别风险场景中所涉及的不同要素的组合,能够建立与恶意程序事件相关的风险场景,从而能够评估恶意程序风险的大小。

## c) 数据安全事件导致数据泄露的风险场景

内部运维人员(威胁)配置访问控制策略不当(脆弱性),导致内部普通员工能够访问客户数据(资产),内部员工直接访问并拷贝客户数据(攻击方法)造成投保人客户数据泄露,导致投保人承担客户索赔,同时带来声誉受损以及相应的危机公关成本(损失);该风险场景代表了典型的数据安全事件造成的数据泄露的风险。

## D.2 风险量化分析示例

风险量化分析主要包括以下过程。

a) 构建风险场景集合:根据被保险人风险识别的情况,构建风险场景集合  $S=(S_1, S_2, S_3 \cdots S_n)$ 。

## b) 计算单个风险场景风险量化值,包括如下过程。

- 1) 对风险场景集合中单个风险场景的各风险要素赋值,风险场景  $S_n=(\text{威胁、资产、脆弱性、攻击方法、安全事件})=(T, A, V, M, E)$ ,其中资产中包含了作用于其上的相关控制措施,用  $C$  表示,由于控制措施与具体保护的资产相关,所以不直接在风险场景要素组合中显示。
- 2) 计算风险场景发生的可能性,风险场景的发生代表该风险场景对应的安全事件已实际造成损失,因此风险场景发生的可能性也即造成损失的安全事件发生的可能性,称为损失事件,计算损失事件发生的可能性包括下面三个步骤。
  - i. 根据该风险场景所对应的威胁,资产,脆弱性,攻击方法等赋值,计算威胁事件发生的可能性:威胁事件发生的可能性  $= TP(\text{威胁赋值,资产,脆弱性,攻击方法}) = TP(T, A, V, M)$ ,在威胁事件发生的可能性计算中,要综合考虑威胁主体实施攻击的能力、资产属性(资产的重要性以及资产所具有的控制措施)等因素判断威胁事件发生的可能性。
  - ii. 计算威胁事件转化为损失事件的可能性:转化为损失事件的可能性  $= P(\text{威胁赋值,}$



控制措施,脆弱性,攻击方法) $=P(T, C, V, M)$ ,在转化为损失事件可能性的计算中,要综合考虑攻击者技术能力(利用该攻击方法的熟练程度),脆弱性被该攻击方法利用的难易程度,以及控制措施对该攻击方法的防范能力。

- iii. 最后计算损失事件发生的可能性:损失事件发生的可能性 $=L$ (威胁事件发生的可能性、转化为损失事件的可能性) $=L(TP, P)$ 。
- 3) 计算风险场景造成的损失,根据资产价值,以及安全事件类型和损失类型,计算损失事件一旦发生后的损失大小,损失事件造成的损失 $=F$ (资产价值,安全事件) $=F(A, E)$ ,其中资产价值对损失的程度有影响,事件类型则决定会产生哪些类型的损失,并在计算中将安全事件相关的所有损失项进行累计。
- 4) 计算风险场景的风险值,根据计算出的损失事件发生的可能性以及损失事件造成的损失,计算该风险场景的风险值,风险场景风险值 $=R$ (损失事件发生的可能性,损失事件造成的损失) $=R[L(TP, P), F(A, E)]$ 。
- c) 计算总体风险量化值:根据每个风险场景所计算的风险量化值  $R_i$ ,再对风险场景集合中所有风险场景值进行聚合计算,形成总体风险值  $R$ ,总体风险值  $R=RA$ (风险场景 1 风险值,风险场景 2 风险值,⋯,风险场景  $n$  风险值) $=RA(R_1, R_2, \dots, R_n)$ ,其中  $RA$  表示风险聚合函数,根据集合中风险场景之间的关系确定计算方法,对所有评估的风险场景的风险聚合结果反映了整体风险大小。



## 参 考 文 献

- [1] GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分:事件管理原理
- [2] GB/T 20985.2—2020 信息技术 安全技术 信息安全事件管理 第2部分:事件响应规划和准备指南
- [3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- [4] GB/T 24364—2023 信息安全技术 信息安全风险管理实施指南
- [5] GB/T 25069—2022 信息安全技术 术语
- [6] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
- [7] GB/T 32914—2023 信息安全技术 网络安全服务能力要求
- [8] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南
- [9] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南
- [10] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
- [11] ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls
- [12] ISO/IEC 27003:2010 Information technology—Security techniques—Information security management system implementation guidance
- [13] ISO/IEC 27004:2016 Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation
- [14] ISO/IEC 27005 Information technology—Security techniques—Information security risk management
- [15] ISO/IEC 27102 Information security management—Guidelines for cyber-insurance
- [16] ISO 30301 Information and documentation—Management systems for records—Requirements
- [17] ISO 31000 Risk management—Principles and guidelines
- [18] ISO/IEC 27072 Information technology—Security techniques—Guidelines for information security management systems auditing
- [19] ISO/IEC/TS 27082 Information technology—Security techniques—Guidelines for the assessment of information security controls
- [20] 中华人民共和国保险法[2015年4月24日第十二届全国人民代表大会常务委员会第十四次会议通过《全国人民代表大会常务委员会关于修改〈中华人民共和国计量法〉等五部法律的决定》(主席令第二十六号)]
- [21] ITU-T X.1061 Information and network security—Security management—Cyber insurance acquisition guidelines
-

