君合专题研究报告 JUNHE

2021 年 1 月 18 日

勿临渴而掘井—网络安全事件应急预案相关义务

随着5G、人工智能、大数据和工业互联网等为代表的“新基建”的深入推进，数字经济得以迅猛发展，但同时包括个人信息在内的各类网络安全事件频发，相关主管部门对于企业及时制定和运营网络安全应急预案的合规要求越来越高。

2020年7月，某快递公司因员工非法向第三人出租账号，导致40万条顾客个人信息泄露，受到所在地政府互联网信息办公室、公安部门等的联合约谈，被责令就信息泄露事件及时公开、正面应对[1]。而对于反复发生网络安全事件且拒不改正的相关企业，更有呼吁祭出“拒不履行信息网络安全管理义务罪”这一杀手锏予以严惩[2]。

事后控制不如事中控制，事中控制不如事前控制，网络运营者依照《网络安全法》及相关规范制定网络安全事件应急预案，以便在事件发生时立即启动、及时处理，便是事前控制的重要方式之一。本文拟就网络安全事件应急预案，从宏观上梳理其相关法律法规体系，微观上分析其结构内容、注意事项等，供相关企业参考。

一、网络安全事件应急处理相关法律法规体系概要

我国的网络安全事件应急处理主要以《突发事件应对法》及《网络安全法》为基本法律，以国家相关主管部门公布的管理办法、标准指南、蓝本为主要依据，通过工业制造、电信互联网、公安、水利等不同部门/行业规范，在各地开展运用（具体如下表所示）。

发布日期	发布部门	规范名称
法律		
2007 年 8 月 30 日	全国人大常务委员会	突发事件应对法
2016 年 11 月 7 日	全国人大常务委员会	网络安全法
主管部门规定要求		
2017 年 10 月 25 日	国务院办公厅	突发事件应急预案管理办法
2017 年 1 月 10 日	中央网络安全和信息化领导小组办公室	国家网络安全事件应急预案
2007 年 6 月 14 日	国家质量监督检验检疫总局、国家标准化管理委员会	信息安全技术信息安全事件分类分级指南（GB/Z 20986-2007）
2020 年 4 月 28 日	国家市场监督管理总局、全国信息安全标准化技术委员会	信息安全技术 网络安全事件应急演练通用指南（GB/T 38645-2020）
其他部门、地方政府组成部门的规范性文件等（例示）		
2017 年 7 月 1 日	工业和信息化部	工业控制系统信息安全事件应急管理工作指南
2017 年 11 月 14 日	工业和信息化部	公共互联网网络安全突发事件应急预案
2017 年 8 月 9 日	工业和信息化部	公共互联网网络安全威胁监测与处置办法

[1] http: /news.jstv.com/a/20201129/1606616376487.shtml。

[2] https://www.sohu.com/a/434203956_100069650。

发布日期	发布部门	规范名称
2018 年 6 月 27 日	公安部	网络安全等级保护条例（征求意见稿）
2017 年 12 月 29 日	水利部	水利网络安全事件应急预案
2009 年 10 月 22 日	北京市应急办、经济和信息化委员会	北京市网络与信息安全事件应急预案
2019 年 10 月 30 日	上海市互联网信息办公室	上海市网络安全事件应急预案（2019 年版）

二、网络安全事件分类及相关案例

《网络安全法》第53条规定，网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。根据中央网络安全和信息化领导小组办公室印发的《国家网络安全事件应急预案》，网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。具体可分为以下几类：

编号	事件类型	具体类型	相关案例
1	有害程序事件	分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。	2020 年 2 月，黑客利用新冠肺炎疫情，制造传播系列计算机病毒，病毒文件名均带有“冠状”、“病毒预防”、“肺炎病例”等热门字样，通过邮件、社交网络等方式，感染后可导致计算机被远程控制、信息被窃取等[3]。
2	网络攻击事件	分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。	2019 年 1 月，国内知名电商平台被曝出现重大漏洞，用户可领 100 元无门槛券。后公司发布官方回应称，有黑灰产团伙通过过期的优惠券漏洞盗取数千万元平台优惠券，进行不正当牟利[4]。
3	信息破坏事件	分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。	2019 年 2 月，国内著名短视频分享平台向海淀警方报案，称其 App 受到他人千万级外部账号密码恶意撞库攻击[5]。
4	信息内容安全事件	系指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。	/
5	设备设施故障	分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。	2019 年 3 月，国内著名云储存平台出现宕机，致使用其云服务的企业网站、App 无法正常使用。后官方回应称原因是华北地域某部分服务器等出现服务器磁盘读写过慢故障，经紧急排查处理后逐步恢复，公司表示将根据协议尽快处理赔偿事宜[6]。
6	灾害性事件	系指由自然灾害等其他突发事件导致的网络安全事件。	/
7	其他事件	系是指不能归为以上分类的网络安全事件。	/

[3] http://www.xinhuanet.com/2020-01/30/c_1125512722.htm。
[4] https://www.sohu.com/a/290312379_100238339。
[5] https://xw.qq.com/cmsid/20190621A0EZSE/20190621A0EZSE00。
[6] http://finance.sina.com.cn/roll/2019-03-03/doc-ihsxncvf9471164.shtml。

三、应急预案的制定义务与违规风险

（一） 网络经营者制定应急预案的法定义务

《网络安全法》第25条规定，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

可见，制定网络安全事件应急预案属于网络运营者的法定义务。由于网络运营者的范围广泛，包括网络（包括互联网、工业网以及内网）的所有者、网络管理者和网络服务提供者，因此在生产经营过程中使用网络的企业均应事先制定应急预案，并在发生网络安全事件时立即启动预案。

（二） 未制定预案的法律责任及风险

首先，关于行政责任，作为保障网络安全措施的一环，对应急预案制定工作的忽视可能会被认为是未完全履行网络安全保护义务。根据《网络安全法》第59条，网络运营者不履行网络安全保护义务时，将受到有关主管部门责令改正，给予警告的行政处罚；经责令后拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。而对于关键信息基础设施的运营者，相应的处罚额度将升格为，对企业等处十万元以上一百万元以下罚款，对其直接负责的主管人员处一万元以上十万元以下罚款。根据我们通过公开渠道检索，确有不少网络运营者（包括生产型企业、贸易型企业、电商平台企业、酒店、酒吧、网吧等）因未制定应急预案而受到所在地网络信息办公室、公安部门的警告或者罚款等行政处罚。

其次，在民事责任方面，企业发生网络安全事件且因缺乏应急预案未能及时处理时，极有可能会被认为对相关网络安全事件、损失的产生存在过失，进而面临网络用户提起的违约或侵权诉讼、被合作伙伴或投资方起诉，被要求承担相应的民事损害赔偿责任。我们注意到，2020年2月下旬某大型网络服务提供商发生“删库”事件，导致300万家商户无法使用其网上服务产品，最终该服务提供商除向商户提供1.5亿元损失赔偿之外，其公司市值也受到巨大损失，在5个交易日内估价缩水超过30亿港元[7]。

再次，对于网络服务提供者而言，如果其不履行法律、行政法规规定的信息网络保护义务，且经监管部门责令采取改正措施而拒不改正，有下列情形之一的，将构成刑法第286条规定的拒不履行信息网络安全管理义务罪：“（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。”

需要注意的是，依据刑法第286条，网络服务企业等单位构成拒不履行信息网络安全管理义务罪时将面临双重刑事处罚，即对企业判处罚金，并对其直接负责的主管人员和其他直接责任人员，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。而且，近年来，对于相关企业不依法遵守网络安全保护义务导致的个人信息泄露等安全事件的反复发生，学界以及社会舆论强烈要求相关机关适用“拒不履行信息网络安全管理义务罪”予以处罚[8]，相关企业应充分重视并未雨绸缪。

四、应急预案的常见结构及内容

参照《国家网络安全事件应急预案》以及有关部门、单位、企业等公布的应急预案内容，结合网络安全事件的相关处理实务，以下梳理应急预案常见结构、以及内容及注意事项，以供参考：

[7]http://www.xinhuanet.com/tech/2020-03/03/c_1125654827.htm。

[8] https://www.sohu.com/a/434203956_100069650。

项目	具体内容	内容及注意事项
总则	编制目的	• 预防和减少网络与信息安全突发事件的发生，控制、减轻和消除突发事件引起的危害及造成的损失，规范突发事件预防和应对活动等。
	编制依据	• 《中华人民共和国网络安全法》、《中华人民共和国突发事件应对法》、《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007）、相关主管部门、地方规定等。
	适用范围	• 网络安全事件的预防与处置工作。
	工作原则	• 统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置； • 根据自身实际情况，提炼工作原则。
组织体系	领导机构 职能部门 专家咨询机构	• 结合自身的组织架构和部门职能，明确承担包括监测预警、应急处理、事后处理等责任的部门和人员，同时建议在应急预案中明确人力资源部门、公关部门、法务部门等支持部门的配合义务，且应加强支持部门与技术部门的交流与合作，以确保较为准确地对事件进行理解和说明。
预防预警	预防 预警分级 预警监测 预警信息发布 预警响应 预警解除	• 预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件； • 企业应根据自身的实际情况，建立适合合适自身的监测预警机制，如选择适当的技术手段和工作方式，明确监测人员的职能并将责任落实到人。
应急响应	信息报告 响应等级 应急处置 技术实施 信息发布	• 内容通常包括网络安全事件发生后，信息报送、响应程序、应急状态解除、恢复与重建、总结、评估和改进工作等，应根据自身的实际情况，明确网络安全事件发生后，企业内部的应急响应流程和报告内容，以及向有关部门报告的流程、内容等。 • 此外，企业在平时工作中，即应强化与各监管部门的沟通。一旦发生安全事件，要及时向监管部门报告，争取监管部门的支持和指导。
后期处置	/	
应急保障	机构和人员 物资保障 通信保障 经费保障 责任与奖惩	• （一）对涉密信息建立严格的信息保障措施。 （二）中心机房需配备核心网络、应用系统或重大风险系统的容灾备份。 （三）建立跨部门的应急保障队伍。 （四）组织开展应急运作机制、应急处理技术、预警和控制等研究。 • 为确保落地实施，建议根据自身的实际情况，在预案中明确设备、技术资料、经费、人力支持等保障措施，同时明确奖惩制度。
附则	预案解释 预案修订 预案实施	• 根据实际情况变化，适时评估修订本预案。

我们建议，网络运营者在制定应急预案时，应结合自身的业务形态，充分考虑到自身通常面临的事件类型的特殊性。在参考国家、地方、行业相关应急预案的基础上，结合自身实际情况制作应急预案，最重要的是符合自身实际情况以及运营需求，做到充分保障、切实可行。

应当注意的是，根据相关规定，各主体制定的网络安全应急预案通常是适用于各自领域（或所在部门体系内）的网络安全事件的预防和处置工作，而有关信息内容安全事件的应对，通常需另行制定专项预案。

五、网络安全应急演练

根据《网络安全法》第34条，对于公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施的运营者，除了制定应急预案外，还有义务定期进行应急演练。

在电信领域，《公共互联网网络安全突发事件应急预案》第7.2条（应急演练）规定了特定电信企业参加应急演练的要求。即，基础电信企业、大型互联网企业、域名机构应当积极参与电信主管部门

组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向电信主管部门报告。

此外，尽管尚未正式制定、生效，公安部公布的《网络安全等级保护条例（征求意见稿）》第32条规定："第三级以上网络的运营者应当按照国家有关规定，制定网络安全应急预案，定期开展网络安全应急演练"。

由此可见，对于关键信息基础设施的运营者、特定电信企业（以及网络安全保护等级在第三级以上的网络运营者）而言，开展应急演练是法定义务，必须定期开展。目前法规还没有明确演练频率，结合相关规定看，可能至少每年需要组织一次，等级更高的网络可能需要半年组织一次。

我们认为，金融机构、从事大规模数据业务的互联网企业等属于风险高发企业，无论是否属于法定范围，都建议制定应急预案，组织应急演练。另外，从测试、完善应急预案、提高企业有效应对突发网络事件能力、防止出现严重后果方面看，我们建议网络经营者定期执行。根据我们的经验，在企业和有关人员因网络安全事件被追究责任时，应急预案和演练记录可以证明企业的合规意愿和实际行动，有利于减轻或避免企业和相关个人的法律风险。

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.comd
高　健　律　师　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com
黄海凡　律　师　电话：86 21 2208 6237　邮箱地址：huanghf@junhe.com