doi:10. 11835/j. issn. 1008 - 5831. 2017. 01. 013

欢迎按以下格式引用:赵丽莉,钟晗. 论网络安全事件信息披露机制的建构[J]. 重庆大学学报(社会科学版),2017(1):109 - 114.

Citation Format: ZHAO Lili,ZHONG Han . Research on the construction of information disclosure mechanism of cyber security event[J]. Journal of Chongqing University(Social Science Edition),2017(1):109 - 114.

论网络安全事件信息披露机制的建构

赵丽莉[1],钟 晗[2]

(1. 新疆财经大学 法学院,新疆 乌鲁木齐 830012;2. 南京大学 计算机科学与技术系 江苏 南京 210023)

摘要:伴随互联网和信息化的迅猛发展,网络安全对国家经济、社会生活甚至国家安全的影响日益增强。与此同时,银行、电信网络、政府部门等关键基础设施、大型商业网站、云服务、工业控制系统均日益成为网络攻击重点;基础网络、重要信息系统、通用软硬件的漏洞攻击风险、大型网站数据和个人信息泄露现象严重,网络安全事件频发,信息披露诉求应运而生。网络安全事件信息披露机制可有效防控恶意软件、漏洞风险、数据泄漏等网络信息安全风险和威胁。为此,为进一步明确网络空间各主体有效管理和规制网络安全风险和威胁的责任,建构系统化的网络安全事件信息披露机制具有现实必要性。

关键词:网络安全;风险与威胁;信息披露;体系化

中图分类号:D922. 8 **文献标志码**:A **文章编号**:1008-5831(2017)01-0109-06

一、网络安全事件披露机制的提出与界定

(一)问题的提出

在互联网全面发展之际,互联网已深入国家政治、经济、文化、医疗、教育等社会生产、生活的各个领域,“互联网 +”新时代模式开启。然而网络欺诈,政府网站等关键基础设施被攻击,重要信息被泄露,恐怖分子等不法分子利用互联网策划组织暴力恐怖事件等网络安全事件频发。当频发的网络事件关乎信息系统和信息内容安全,使公民、组织的信息安全以及公共安全和国家安全被威胁时,为了能够实时控制网络安全应用过程,提高网络安全事件治理的透明度,适时的网络安全事件信息披露就显得非常必要。此外,网络安全事件产生因素多样,产生的风险具有不确定性、不可逆性,而且产生损害的时间非常短,若不能及时告知,则产生的损害将无法恢复和估计。在美国,已有 45 个州出台要求公司或政府机构披露入侵有关个人信息事件的法案[1]。2015 年 6 月 19 日《中国互联网协会漏洞信息披露和处置自律公约》签署,包括国家计算机网络应急技术处理协调中心(CNCERT)、重要行业部门、基础设施部门、软硬件厂商以及网络安全企业等在内的 32 家单位参与,该公约以行业自律方式规范网络安全事件之漏洞信息的披露工作。但中国文献鲜少研究不同部门、机构和人员的网络安全事件信息披露机制建构问题,而是更多地从技术角度关注安全事件的发现、处置,或者从宏观视角研究网络安全保障问题。当网络安全事件发现及预警通报的信息披露工作在应对网络安全威胁方面的作用日益凸显时,以网络安全治理视角探索系统化的网络安全事件信息披露机制建构问题就成为值得深思的问题。目前的立法并未对需披露的网络安全事件进行等级分类,也未涉及多大范围内

修回日期:2016 - 11 - 23

基金项目:2016 年度国家社会科学基金西部项目“网络时代暴恐信息传播法律治理创新研究”(2016XFX014)

作者简介:赵丽莉(1978 -),女,山西榆社人,新疆财经大学法学院副教授,法学博士,硕士研究生导师,西安交通大学信息安全法律研究中心兼职研究员,主要从事信息安全法、知识产权法研究,E - Mail:lilihellozl@ sina. cn。

披露和披露什么内容以及披露时间等具体规定。

(二)网络安全事件信息披露机制界定

网络安全事件主要涉及影响互联网安全运行的事件、波及较大范围互联网用户事件和涉及政府部门和重要信息系统的事件,事件类型主要包括漏洞、网页仿冒、网页篡改、恶意程序、网站后门、网页挂马、拒绝服务攻击等方面。网络安全事件信息披露机制作为广义信息披露的一种,其披露的信息范围即是与特定网络安全事件相关的风险信息,主要包括信息系统功能性风险和信息安全内容风险。功能性风险主要指针对信息系统实体安全和信息系统运行安全两个方面。前者指信息系统设备、设施免受破坏;后者指防止信息系统被非法侵入,信息系统因病毒等破坏性程序的感染或其他非法攻击而遭受损害,网络或通信服务被非正常中断,使信息网络或通信系统不能正常运行等危害。网络安全内容风险则主要包括重要信息泄密、暴力恐怖音视频内容的网络传播等。

网络安全事件信息披露本身可以被视为将风险信息公知化的过程,但基于网络安全事件信息的敏感性,这一公知过程可能产生潜在的负面影响。为此,网络安全事件信息披露需要在有效机制的规范下予以实施。网络安全事件信息披露机制即是网络安全事件信息披露的约束性框架,是对可能造成特定信息系统和信息内容安全减损,影响用户合法权益,造成人身或财产损失,或可能产生其他严重危害后果的事件信息进行公知活动的系统性规范,包括披露主体、披露内容、披露程序、披露时间、披露对象、相关责任和例外规定等,进而有效规范网络安全事件信息披露活动。

二、网络安全事件信息披露机制建构的价值基础

法律制度应当具备应有的价值基础,客观反映为其意欲实现的法益追求和规范目标,这也构成形成社会公众“规范性期待”的前提条件。网络安全风险无法避免,因此有效的风险管理措施非常必要。其中,披露被认为是风险控制的中心环节,对于降低风险和分化风险起着至关重要的作用[2]。网络安全事件披露机制建构是加强网络安全保护工作的重要组成部分,其价值基础可以归纳为两个方面:(1)有助于防控网络安全威胁,可使用户清晰认知网络安全事件风险,并充分利用披露的信息及时采取预防和控制措施,有效预防网络安全事件风险的产生,降低或阻止威胁的扩大化;(2)可强化国家安全基础数据保障的综合能力,有效协调创新发展与用户安全保障矛盾。

(一)防控网络安全威胁

随着信息网络渗透于人类生产和生活的方方面面,人类政治、经济、军事、科技、文化生活、环境等各个方面对信息网络的依赖性越来越强,个人、企业、民族、国家乃至人类的安全也建立于互联网中,网络安全已成为关乎个人乃至整个国家的重要问题。CNCERT 报告显示,仅 2015 年 8 月即收到网络安全事件达9 655 件①,[3]。诸如针对信息系统的安全威胁:2014 年“全国 DNS 大劫难”事故中超过 85% 的用户遭遇了网速变慢和网站打不开的 DNS 故障,国内 2/3 网站因此受影响;OpenSSL 公布的重大安全漏洞显示,该安全漏洞正被网络威胁和网络攻击所利用而成为新的威胁,该漏洞可使任何人读取系统运行的内存,安全行业人士实践利用此漏洞可实时获取网站、电商、网上支付等网站用户账号和密码,并实现成功登陆[3]。该漏洞已使网站、即时聊天、服务器系统、网络设备、防火墙等系统遭受安全风险和威胁。美国《福布斯》网站报道一款漏洞“可被黑客利用在不被检测情况下实现对全球八成个人电脑、网络应用或者云端虚拟机实现监控”[4]。国家计算机网络应急技术处理协调中心 2015 年度《中国互联网网络安全报告》显示,诸多网络安全威胁伴随信息化的不断发展而产生,包括重要信息系统、基础网络、智能终端领域软硬件漏洞攻击;重要网站域名解析篡改攻击;工业控制系统、移动应用程序恶意软件攻击;分布式反射性的拒绝服务攻击;网站数据和个人信息泄漏等方面[5]。2016 年该工具被爆出的 DROWN 安全漏洞又使国内 10 万余家网站受影响。另据国家互联网应急中心(CNERT/CC)2016 年第 39 期发布的互联网安全威胁报告显示,仅 2016 年 9 月 19 日至 25

①国家互联网应急中心《CNCERT 互联网安全威胁报告》(2015 年 08 月)。

日一周内“境内感染网络病毒主机数 59.1 万;网站被篡改数量为 2 477 个,包括政府网站 53 个;新增信息系统安全漏洞 257 个,其中,高危漏洞 146 个;处理各类网络安全事件 622 起,包括跨境案件 158 起”[6]。

此外,近年来针对网络信息内容的安全威胁事件亦处于频发状态,且影响后果越来越大:诸如 2014 年 4 月黑客利用快递公司官网漏洞入侵网站,1 400 万条用户个人信息被非法窃取,2014 年 12 月 25 日中国大型交通购票网站 12306 网站中约 10 万多条用户数据被泄漏,包括用户账号、密码、身份证号、手机号码以及电子邮箱等重要信息[7]。据国家计算机网络应急技术处理协调中心报告显示,2015 年,该中心抽样监测发现的恶意软件程序转发用户信息邮件超过 66 万封,大量个人隐私信息可通过邮件被发送到指定邮箱[8]; 2015 年发生约 10 万条应届高考生信息泄漏事件,而 2016 年更发生多名学生更因个人信息泄漏而引发学费被骗事件。2016 年信诚人寿保险公司被曝其平台面临客户银行卡号、密码、身份证等重要敏感信息被泄漏的风险。目前,由于教育、金融、医疗、物流行业、政府等都与互联网密切相关,这一方面网络安全威胁已对各领域重要信息系统安全、公共网络环境安全造成威胁,产生重大突发网络安全事件风险。此外,“暴恐音视频”的网络传播威胁则可在“意识形态领域、文化领域”冲击国家安全和社会稳定,这已成为一些特定区域网络安全威胁的主要内容。在国内破获的各种暴力恐怖犯罪,其涉案人员几乎均观看收听了包括宣扬暴力恐怖、宗教极端、民族分裂等暴力恐怖音像视频,其中,互联网成为获得、传播、观看和组织实施恐怖活动的重要渠道。

有鉴于此,频发的网络安全事件无论是针对网络运行系统安全,还是网络信息内容安全都已成为关乎互联网健康发展乃至国家安全和社会稳定的重大问题,而有效的网络安全治理机制尤显必要和紧迫。鉴于网络安全风险和威胁的动态性,目前的网络安全事件治理缺乏一种动态的机制以实现对网络信息安全事件的前期控制,于是“确立以预防与控制为核心的治理理念和机制极为必要”[9]。而网络安全事件信息披露机制的建构即可体现这种预防与控制的理念,而且“管理和披露信息安全风险也被认为是网络时代一些主体的责任”[10]。面对不断增长的网络安全事件威胁,有效的信息披露机制确立可使用户及时预判,并因此而防范和控制风险和威胁的产生,从而确保网络安全。

(二) 协调创新发展与安全保障之间的矛盾

随着新一代网络技术的发展,人们的日常社会生活方式正在发生巨大的变化。新一代网络技术已延伸到国家政治、经济、军事、科技和文化等各个方面,渗入到人们的日常生活、社会活动、经济行为和国家安全的各个领域,极大地改变了社会生产生活方式。诚然,互联网的不断发展创新着各领域产业的发展,推动了社会进步。然而,互联网应用云化以及计算机等终端通信设备的普及化也使影响国家安全、社会稳定和个人隐私安全的网络安全事件和行为陡增。因此,在网络时代,在广泛关注创新发展的同时,当面临网络安全事件以及因此而影响到用户合法权益、社会秩序以及公共利益时,我们不得不正视创新与安全间的冲突[11]。这就需要加强对网络安全的防控,而确立有效的信息披露机制则成为能够协调创新发展和安全保障的重要防控举措。例如,Microsoft Windows 任务管理权限提升等漏洞可引发漏洞相关的网络安全事件,导致用户计算机被控制。由于包括政府部门、重要信息系统部门以及大量用户都使用 Windows 系统,一旦该漏洞被利用而引发网络安全事件,那么网络运行系统,甚至工业控制网络、关键基础设施部门以及大量公共、私人用户网络均可遭受攻击,导致运行系统和信息内容遭受安全威胁。而一些公司的恶意软件或者漏洞已经造成了实际的和潜在的损害,这种损害不仅仅使用户暴露于攻击之下,也使公司名誉受损,更严重的是技术保护措施所造成的损害不是单一的。因为信息技术设施分布式的本质,整个网络安全部分涉及成千上万的私人电脑,对个人电脑的攻击,通过延伸必然涉及网络本身,而受攻击的系统可包含公司、大学、政府或军事网络。然而,在具体实施中,必然会面临创新发展与安全的矛盾性。在损害尚未发生前,一些主体担心一旦及时告知用户可能造成用户的恐慌,这不仅危及权利主体自身利益,影响产业的发展,而且也使安全问题的解决陷于困境。于是一些企业基于信誉和名声以及影响发展的考虑会选择隐瞒相关信息,其结果可能导致损失的无限扩大。而事实上,很多私营部门网络攻击入侵的防御体系不完备[12]。尽管安全披露义务可增加企

业防御网络安全风险的成本,一定时期内需要牺牲其发展利益,但是不能以牺牲网络安全为代价而换取行业或产业创新发展,再者信息安全披露义务也加强了相关行业和产业防控网络安全风险的能力。为此,有必要在发现漏洞时及时披露信息以及明确相应漏洞修补程序强制性义务。

三、网络安全事件信息披露机制的建构

网络安全事件信息披露机制的确立具有现实必要性,而披露义务的行使单纯依靠行业协会的自律并不足以应对,“法的功能在于调节、调和与调解各种错杂和冲突的利益,以便使各种利益中大部分或我们文化中最重要的利益得到满足,而使其他的利益最少的牺牲”[13]。因此,建构系统化的信息披露机制制度是形成网络安全保障体系的重要组成部分,也应是互联网立法中的应有内容。

(一)信息披露的主体

国家互联网应急中心网站显示,包括通信管理局、基础电信运营企业、非经营性互联单位、安全企业及其他一些地方和行业互联网协会承担向国家互联网应急中心通报网络信息的工作,但是这并非强制义务,并非所有主体应承担强制性信息披露义务。具体而言,在网络安全事件中,具体的披露主体至少应包括以下几类:(1)软硬件厂商,包括发布网络安全方面软硬件的企业。作为软硬件的直接权利主体以及直接掌握这些技术措施信息的主体,理应在发现安全风险时及时披露,他们有义务在向用户提供服务时标识采取的技术特征信息,包括使用范围、使用限制、运行环境的要求以及运行后可能存在的风险,并在征得用户完全同意的情况下方能下载或安装。当发布的产品是众所周知的能够引起或可能对用户系统造成功能性伤害时,应发布安全通知,告知通过检测所合理预测的信息安全问题或别的风险的存在;(2)政府相关网络安全管理部门。作为专门的网络安全管理部门,承担安全保障的重要职能,在发现网络安全事件时及时向社会发布其评估监测的内容是其职责范围之事;(3)涉及重要信息泄露的重要行业部门,诸如基础电信部门、医疗、金融、教育等关乎大量个人重要信息和重要产业信息的部门。由于网络安全事件可能波及大量重要信息系统和信息内容的泄漏,因此一旦发现入侵、攻击、泄漏等风险应及时披露相关信息。

(二)信息披露的对象

网络安全事件信息披露应当有具体的披露对象,具体而言:一是各类产品的直接用户。由于用户是这些产品的直接使用者,也是风险发生后的直接受害者,依据《消费者权益保护法》《合法同》等相关法律,他们具有对商品或提供服务的知情权,因此应当作为直接披露对象。与此同时,接受信息的用户可及时采取措施针对类似网络攻击的网络安全事件作出反应,诸如下载补丁程序,或者控制或破坏攻击病毒,这被认为“应对网络攻击的重要反应,也是规制网络安全的重要环节”[12]。

二是网络安全的主管机构。由于各部门在各自领域内开展相应工作,而网络安全领域问题涉及面宽且复杂,可能同时涉及不同的工作部分。信息网络环境下,网络安全复杂性较强,公民、法人和其他组织的合法权益与社会利益、公共安全以及国家安全威胁可能同时存在,当涉及由行政机关依法执行维护国家安全所保护的网络安全及其他相关事项产生安全风险时,相关主体应及时对各相关主管机关披露。中国对网络安全监管采取的是分业纵向监管模式,主管机关有:国务院信息化工作领导小组及其办公室、公安部公共信息网络安全监察部门、信息产业部、国务院信息产业主管部分、国家密码管理机构和国务院其他有关部门,它们在各自领域承担相应的网络安全监管职责。为此,网络安全事件可及时向网络安全的主管机构披露,而各网络安全主管机构之间应实现信息共享并及时协调,向社会发布相关信息和防控措施。

(三)信息披露主要内容及时间

信息披露内容和时间是信息披露机制中的重要内容。网络环境使网络安全事件造成的损害具有不可逆性,损害后果严重,这要求披露义务主体首先在网络安全事件风险产生之前,为防范安全风险以及降低损害程度,对于已监测的网络安全风险和威胁信息,有关部门、机构和人员应及时发布预警,告知相关用户隐藏的安全风险,包括发生的可能性、潜在影响范围和危害程度。诸如近年来,大量基于网络应用、安全产品、应用程序、操作系统、数据库、网络设备的网络安全漏洞事件曝光,危害影响可涉及电信、移动互联网、工控

体系等不同行业以及其他公私用户网络与信息安全,于是对漏洞信息适时的、负责任的信息披露就显得很有必要。

当网络安全事件发生后,诸如发生危害社会公共秩序,突发重大社会安全事件时,相关主体应及时(可理解为合理时间范围内,需要依据实际情况判断)披露网络安全事件发生、发展情况;实际产生的安全损害是什么;产生安全风险和威胁的影响范围是什么以及相应事件信息的分析评估与结果等方面的内容。此外,在披露安全风险和威胁信息时应发布避免和减轻危害的必要解决措施,以使用户和相关主体能进一步评估其所面临的风险,进而采取相应措施应对产生的风险和威胁,控制损失的扩大化。而对于部分不可提前预测的安全风险和威胁,也应在实际发现或威胁实际产生时及时予以披露,以阻止损失发生。当然,当及时披露妨害执法机关执法取证,涉及到危及公众利益、影响相关产业发展时,披露应暂缓公告。

(四)信息披露要求和责任

按照信息披露机制的要求,对于网络安全事件的披露应是足够的和有效的,而且"风险披露内容应该是特殊的和具体的"[9],即体现披露的充分性。这里的足够和有效的通知必须使普通用户能够充分认识到网络安全事件的风险和威胁,因此上述通知应以能够帮助用户更容易观察和阅读的方式发布,描述的信息能使使用者在使用产品时合理地保护自身信息系统功能和信息内容安全,避免众所周知的和可能的伤害产生。这一要求显示对于具体的信息披露表达应在显而易见的地方,并且是令人信服的。对于司法实践而言,如果不是轻易地被看见,通常应视为经营者没有向用户提供他们的明确通知,因此不是可执行的[14]。比如通过不清楚的链接、不显眼的字体(如脚注字体)、在灰色背景上的灰色类型、不清楚的链接标签意图去警惕用户关于披露的存在。对于法庭而言,它判断的标准不是双方通常对信息披露内容的理解,也不是用户的实际理解,而是这一披露是否被以明显的方式显示。比如,对于安装的各类软硬件产品,或者网站的漏洞风险应在其产品或者平台显眼位置发布明确而详细的说明,并获得用户的明确同意后予以安装。与此同时,对于发生的网络安全事件解决方案的披露除及时外,也应当具体和具可操作,如此方可实现防控风险和威胁的目的。

当承担披露义务的主体不履行披露义务致使公私财产和信息安全受到影响或者不及时、不充分实施披露行为致使损害扩大时,立法应规定罚则,要求相应主体承担相应的法律责任,包括民事、行政和刑事法律责任。诸如美国加州 2012 年通过的 S. B. 1386 法案即明确了保存公民信息的机构有义务向受害者披露信息泄漏事件,否则可因民事诉讼而承担赔偿责任。

(五)信息披露的例外

虽然网络安全事件相关主体应当承担一定的信息披露义务,但是这一披露义务并非是绝对的,具体在披露内容上需要掌握可披露的度,既保障公众的知情权,又兼顾网络安全、社会秩序稳定以及国家安全。信息披露例外机制的确立非常必要,它是披露机制体系的重要组成部分,这也是现行网络安全立法所缺乏的。具体而言:披露的信息内容应该是被分类的,一些未授权的敏感信不在披露范围之内[15]。当披露的内容将涉及违反其他法律规定、机密信息、妨害执法或损害国家利益以及公共利益、损害其他特定的公有或私营企业的合法商业利益时,可不承担信息披露义务。总之,立法应明确规定网络安全事件信息披露的相应例外条款,保障信息披露机制建构的完整性。

参考文献:

[1]马民虎. 网络信息安全保障的法律监管研究[M]. 西安:陕西科学技术出版社,2007.

[2]张乐,郝文江,武捷. 美国网络入侵信息披露制度简介[C]//全国计算机安全学术交流会论文集(第二十五卷). 合肥:中国科学技术大学出版社,2010:121.

[3]李国敏. 2014 年重大网络安全事件回顾[N]. 科技日报,2014 - 12 - 24(11).

[4]佚名. 美发现新浏览器攻击模式:可监控全球八成 PC[EB/OL]. [2015 - 04 - 24]. http://www. cnnic. net. cn/gjymaqzx/aqgg/aqggaqsj/201504/t20150424_52123. htm.

[5]国家计算机网络应急技术处理协调中心.2014 年中国互联网网络安全报告[M].北京:人民邮电出版社,2015:15.
[6]国家互联网应急中心.网络安全信息与动态周报(2016 年第 39 期)[EB/OL].[2016 - 09 - 30].http://www.cert.org.cn/publish/main/upload/File/2016CNCERT39.pdf.
[7]肖前忠.年终盘点:2014 年国内和国际网络信息安全大事件[EB/OL].[2015 - 03 - 10].http://www.d1net.com/security/news/326109.html.
[8]国家计算机网络应急技术处理协调中心. 2015 年我国互联网网络安全态势综述[EB/OL].[2016 - 05 - 01].http://www.cert.org.cn/publish/main/upload/File/2015%20Situation.pdf.
[9]赵丽莉.基于过程控制理念的网络安全法律治理研究——以"风险预防与控制"为核心[J].情报杂志,2015(8):177 - 181.
[10]TROPE R L,HUGHES S J. The SEC staff's "Cybersecurity Disclosure" guidance: Will it help investors or cyber - thieves more?[J]. Business Law Today,2011:1 - 4.
[11]赵丽莉.论版权技术保护措施信息安全遵从义务——以法国《信息社会版权与邻接权法》第 15 条为视角[J].情报理论与实践,2012(12):32 - 36.
[12]SALES N A. Regulating cyber-security[J]. Northwestern University Law Review,2013,107(4):1508 - 1564.
[13]罗斯科·庞德.通过法律的社会控制——法律的任务[M].沈宗灵,董世忠,译.北京:商务印书馆,1984:42.
[14]MATWYSHYN A M. Hidden engines of destruction: the reasonable expection of code safety and the duty to warn in digital products[J]. Florida Law Review,2010(62):109 - 157.
[15]DYCUS S. Congress's role in cyber warfare[J]. Journal of National Security Law & Policy,2010,4(1):155 - 171.

Research on the construction of information disclosure mechanism of cyber security event

ZHAO Lili[1],ZHONG Han[2]

(*1. School of Law, Xinjiang Finance and Economic University, Wulumuqi 830012, P. R. China*;
2. Department of Computer Science & Technology, Nanjing University, Nanjing 210064, P. R. China)

Abstract: With the rapid development of Internet and information technology, cyber security has more and more influence on national economy, social life and even national security. At the same time, banking, telecommunications networks, government departments and other key infrastructure, large-scale commercial websites, cloud services, industrial Internet are increasingly becoming the focus of cyber attacks; and cyber security and security incidents of basic network, important information systems, common software and hardware vulnerabilities, large web sites and personal information leakage are serious, which has threatened data and personal information security, social stability and national security. Cyber security event information disclosure mechanism can effectively prevent and control the risk and threat of cyber information security, such as malicious software, vulnerability risk, data leakage and so on. "Cyber Security Act" (Draft) established the corresponding information disclosure provisions. Therefore, to further clarify the responsibility of the main body of the cyber space and effectively manage and regulate the risk of cyber security incidents, it is practical necessity to construct the effective information disclosure mechanism of cyber security event .

Key words: cyber security; risks and threats; information disclosure; system

(责任编辑 胡志平)