Doi:10.11835/j.issn.1008-5831.fx.2019.09.002

欢迎按以下格式引用:张敏,马民虎. 企业信息安全法律治理[J]. 重庆大学学报(社会科学版),2020(5):143-155. Doi:10.11835/j.issn.1008-5831.fx. 2019.09.002.

Citation Format: ZHANG Min, MA Minhu. Legal governance of enterprise information security[J]. Journal of Chongqing University(Social Science Edition),2020(5):143-155. Doi:10.11835/ j.issn.1008-5831. fx. 2019.09.002.

企业信息安全法律治理

张 敏,马民虎
(西安交通大学 法学院,陕西 西安 710049)

摘要:企业信息安全法律治理可有效保障国家网络与信息安全,捍卫个人权益,促进产业在"安全"中得以"发展"。我国相关立法中规定的企业安全保护义务多为静态性、措施性的管理性义务,不足以防御多变的安全风险;企业安全法规遵从激励机制缺失,合规动力不足;企业信息安全文化的普及力度欠缺。解决以上难题,应基于"法律治理"思维,将"法人治理"定位为企业信息安全法律治理的重心。在制度设计层面,适当借鉴美国企业信息安全法律治理在立法监管与企业自治中的有益经验,以信息安全法律治理的基本原则为指引,充分发挥立法激励作用,鼓励所有企业建立强制与自愿相结合的信息安全"法人治理"结构,对企业董事、高官人员的信息安全义务之履行予以充分重视,增强企业信息安全文化建设,凸显安全文化的价值。

关键词:法律治理;协同治理;信息安全义务;信息安全法人治理

中图分类号:D922.291.91 **文献标志码**:A **文章编号**:1008-5831(2020)05-0143-13

以云计算、大数据等为驱动的新技术在引领企业向智慧企业转型的同时也打开了安全威胁的潘多拉魔盒:一方面,针对国家关键信息基础设施的持续性大规模网络攻击、企业系统漏洞、数据泄露等安全威胁呈现升级化态势;另一方面,因欧美网络与信息安全立法变革浪潮冲击、跨国IT企业合规僵局、贸易大战与地缘政治安全的复杂结构相交织,进一步加剧了我国信息安全的严峻态势。我国《网络安全法》将网络运营者定位为"协同治理"的中坚力量,并为其量身设定了安全义务体系。在此背景下,我国亟需以《网络安全法》的安全"保障法"定位为指引,在谨慎权衡"安全"与"发展"的基础上,积极探索中国本土化的企业信息安全法律治理之道,以提升《网络安全法》执法和企业合规的有效性,最大

修回日期:2019-09-06

基金项目:国家社会科学基金重大项目"网络社会治理创新研究"(15ZDA047);国家社会科学基金一般项目"我国网络安全立法研究"(15BFX050)

作者简介:张敏(1986—),女,西安交通大学法学院博士研究生,美国印第安纳大学法学院访问学者,主要从事网络与信息安全法、经济法研究,Email:fish_law@163.com;马民虎(1958—),男,教授,博士研究生导师,西安交通大学苏州研究院信息安全法律研究中心主任,主要从事信息安全法、电子商务法研究。

化企业在国家信息安全保障中的能量。

一、企业信息安全法律治理的提出

(一)企业信息安全法律治理之内涵解析:基于"治理"理论视角

"法律治理(Legal Governance)"的理论根基深植于"治理(Governance)"理论。"治理"理论源于西方,流派众多且各具差异,但对"治理"的核心要素即主体多元、平等、协作、共赢等存在共识。全球化趋势使带有工具理性特征的治理理论与法律相结合,在不同国家被重塑与本地化,领域多涉及国家、社会、城市、公司、网络等。新中国成立以来,中国法制建设开启了从管理迈向"法律治理"的革命性变革,对"法律治理"的倚重亦是国家治理能力现代化的标志。"法律治理"是指依据国家权力机关依法律程序制定的法律规则,政府、社会、市场等存在利益分化的多元主体通过合作、协调与互动的方式,实现共同利益与促进社会发展目标。我国学界亦认识到,"与高度复杂性和高度不确定性的时代相适应的社会治理模式应当是一种合作行动模式,只有多元社会治理主体在合作的意愿下共同开展社会治理活动,才能解决已出现的各种各样的社会问题"[1]。

当我国从工业社会迈入网络与数字化社会,安全与发展成为基本的时代诉求。得益于治理理论对网络与信息安全立法的滋养,"协同治理"成为有效应对网络安全威胁的核心理念。"协同治理"是指处于同一治理网络中的多元主体间通过协调合作,形成彼此啮合、相互依存、共同行动、共担风险的局面,产生有序的治理结构,以促进公共利益的实现[2],其强调不同主体间合作的匹配性、动态性、有序性与有效性。我国《网络安全法》将"协同治理"定位为基本原则,其智慧在于:一是强调了安全治理应立足于政府的规范、引导与监督,政府决策应建立在统筹考虑、利益平衡的基础之上;二是强调应发挥政府、企业、社会团体及公民在内的多元主体参与,鼓励多元主体责任分担、协同合力,避免传统"善政"思维对政府责任的无限放大。

企业信息安全法律治理的提出是对"协同治理"理念的践行,其制度内涵包括:一是政府应不断优化网络与信息安全相关立法规范,提升立法技术,发挥"硬法"与"软法"的各自优势,为企业信息安全治理创造良好的外部法治环境;二是立法应引导和激励企业充分发挥"协同治理"的作用,将企业信息安全法人治理作为"重心"。在所有企业中建立自愿与强制相结合的信息安全法人治理结构,明确企业高管之信息安全义务,促进法人治理与安全文化相交融。

立法监管与企业法人治理是企业信息安全法律治理的有机组成部分,两者相辅相依。企业信息安全法律治理应立足于立法的引导、监督与鼓励,可分别通过设定指引性与禁止性法律规则为企业信息安全自治设定法定"基线"与违法"红线",设定激励性规则鼓励企业守法与合规。企业应以法律原则、规则为治理依据,根据风险变化灵活优化企业法人治理结构,最终在政府与企业"二元"治理的有机互动中保障信息在处理、存储及流转中的完整性、机密性与可用性。

(二)企业信息安全法律治理的制度价值

企业信息安全法律治理凭借蕴含价值理性和道德判断的法律的介入,用法律权威将安全义务归化到企业,从而实现以下制度价值。

1. 有效保障国家网络与信息安全,维护公共利益

网络安全现已对国家安全产生了全面的颠覆性影响,成为国家安全竞争的最前沿领域和国家安全

变革的最难以预测的因素[3]。威胁国家网络安全因素复杂多样,黑客攻击与数据泄露最为典型。大规模、高级可持续性攻击的目标正在从传统的 IT 系统转向石油、天然气、航空运输等关键行业的工业控制系统。关键信息基础设施运营者向社会公众提供的产品及服务具有公共产品属性,其安全防范中的弱项可能成为黑客攻击的"短板",从法律治理的高度去应对企业安全难题则是较为有效的手段。

2. 有效保障个人信息安全,捍卫个人权益

个人信息蕴含财产利益与人格尊严,我国立法将其视为基本民事权利。个人信息泄露常规路径有三种:(1)内部人员非法盗取、转卖;(2)企业在非授权范围内利用与经营用户信息;(3)恶意程序利用网络漏洞非法入侵数据库进而盗取、劫持个人信息。随着电子商务与社交平台迈入鼎盛时期,海量用户数据被企业抓取、整合、分析、画像,严重危及个人权益。很多人将数据泄露的"原罪"归于个人信息立法的不完备,而忽视了立法并未真正映射、内生于企业治理层面是数据泄露有增无减的内因。

3. 促进产业在"安全"中得以"发展"

在信息化时代,很多企业(尤其是发展中国家企业)的信息安全治理水平令人忧虑。只有在解决安全问题的前提下,企业发展才能没有后顾之忧。从合规角度,欧美网络安全及数据保护立法变革给企业亦带来考验,如何进行安全合规、降低战略运营风险已成为大型企业走出国门时应考虑的问题。法规遵从并非结果,而是一个持续渐进的过程。建立内生于企业、业务流程及产品设计相融的安全治理机制才能促进产业在"安全"中得以"发展"。

二、我国企业信息安全法律治理:问题检视及治理"重心"的定位

(一)我国企业信息安全义务的法律渊源

法的渊源是指由不同国家机关制定、认可和变动的,具有不同法的效力或地位的各种法的形式。我国企业信息安全义务来源于三层面:一是《网络安全法》(简称"网安法")及其配套的下位法①;二是网络安全等级保护制度②;三是相关国家标准及行业标准③。网安法及相关配套性制度是我国企业信息安全义务的主要法律渊源,相关国家标准与行业性标准为网安法确立的安全义务提供了更为具体的实施依据。

(二)我国企业信息安全法律治理在立法实践中存在的问题检视:基于网安法"保障法"定位展开

网安法是国家网络与信息安全治理的基础性"保障法"。网安法颁布近 3 年来,国家层面和地方政府机构都开始专项检查和执法行动,从"执法第一案"进入执法常态化。从网安法的"保障法"定位去检视立法制度以及执法效果,仍存在一些问题。

1. 企业安全义务多为静态性、具体措施性的管理性义务,而非内生于企业"治理"层面的义务

网安法明确了网络运营者的安全义务体系,其建构在实体性法律规范的基础上,并附加一些履行

①如 2017 年《关键信息基础设施安全保护条例(草案)》、2019《网络安全审查办法(征求意见稿)》等。

②如 1994 年《中华人民共和国计算机信息系统安全保护条例》、1999 年《计算机信息系统安全保护等级划分准则》、2007 年《信息安全等级保护管理办法》、2018 年《网络安全等级保护条例(草案)》的出台标志着国家网络安全等级保护迈入新时期。

③"国家标准"包括《信息系统安全等级保护基本要求》(GB/T 22239—2008)、《信息安全技术信息系统安全等级保护定级指南》(GB/T22240—2008)、《信息安全技术信息系统安全等级保护实施指南》(GB/T 25058—2010)、《网络安全等级保护测评要求》(GB/T 28448—2019)等;"行业标准"是基于《信息系统安全等级保护基本要求》,电力与银行、证券、海关、铁道、民航等重点行业根据各自行业的特点对上述要求作出的扩展。

不能的法律责任,但仍暴露出一些问题:其一,网安法对网络运营者的诸多义务性规定多由政府主导自上而下施加,并通过国家、行业标准规定非常具体的措施性要求作为义务的主要内容,然后通过行政处罚等手段强制要求管理对象合规[4]。而传统法律理论认为,过多禁止性法律规范会造成"管理型"立法而非"治理型"立法[5],减损执法效果。网安法及其下位法在规则设计时偏重于以技术性措施与管理性手段防控企业安全风险,以行政处罚手段震慑企业逾越法律"红线"的规制思路,易导致企业负责人以"不出事"的"管理"式思维被动合规,影响执法效果。其二,网安法设定的企业安全保护义务多为静态性、具体措施性的义务,缺乏对内生于企业的治理层面的义务的宏观考量,不足以应对多变的网络安全风险。如网安法第10条、第21条、第34条、第42条详细规定了网络运营者在保障网络数据三性、等级保护、个人信息保护方面的具体性规定,该规定多以"技术措施""其他必要措施"及"补救性措施"等静态性、措施性规定为主。但网络的"静态"安全或"形式安全"无法从根本上应对网络安全风险的无界传播与溢出效应。随着技术的发展,移动设备、路由器、可穿戴设备、物联网等已逐步成为顶级攻击者的目标。美国国家安全局技术总监戴夫·霍格(Dave Hogue)称,黑客的速度非常快,只要安全漏洞公开发布,国家资助的攻击者可在不到一天的时间内将其武器化[6]。快速化、新型化的安全威胁使企业的整体安全水平只取决于企业最"弱"的一环,而不是最"强"的地方。静态的企业安全风险管理思维已无法防御严峻的安全风险。正如有学者所言,"挂在墙上的资质证书完全无法应对真刀真枪的战略威胁"[7]。

2. 企业安全法规遵从的激励机制缺失,难以扭转企业信息安全治理的"被动"思维

在全球行政改革浪潮中,命令控制式规制受到广泛批评,激励性监管得到重视,人们发现规则如果能够与被管理者激励相容,会极大降低执法成本,提高合规动力[8]。我国网安法建立起企业安全义务体系框架,并通过设置法律责任予以震慑并督促企业遵从,故企业法规遵从的基本动因仍基于法律的强制力。企业多具有逐利的理性人特征,多会将"安全"投入视为"成本"负担,加之安全意识普遍淡薄和违法不利后果的威慑力有限,易导致企业负责人以"不出事"的"管理"式思维被动合规。尤其是中、小型企业,网络安全资源有限,安全意识更为淡薄,对安全威胁的识别、防御能力低,易成为供应链安全的"短板"而降低整个供应链的安全性。对安全风险的静态与被动防御思维根本无法有效应对日益严重的安全危机。Cybereason联合创始人兼首席执行官所言:"企业在网络安全领域的投入每年都在增加,但新型攻击的发生率以及企业遭遇黑客入侵的情况并没有发生实质性的好转。"

3. 企业信息安全文化的引导与塑造力度欠缺,不利于形成良好的治理生态

网络安全立法属于政治上层建筑,信息安全文化属于意识形态上层建筑,二者具有正相关的交互作用。尽管网安法已颁布并进入实施正轨,国家和各级政府也积极组织举办"网络安全宣传周"等活动,以此形式宣传安全文化,但安全文化仍然难以在企业层面深入人心。企业中的每一个个体都是安全链条中的重要环节,任何缺乏安全意识的基层员工及管理层的疏漏都会引发安全风险乃至整个安全防御链条断裂,引发难以预测的安全危机。

(三)我国企业信息安全法律治理的"重心":法人治理

1. 企业信息安全"法人治理"的内涵

法人治理在公司法学上主要指有关公司机关的权力分配与行使关系的制度体系[9]。企业信息安全法人治理是指企业将信息安全保护义务充分融入企业机关的权力分配与权力行使关系中,以明确董

高监及中基层员工的安全义务为核心,是企业内生的且能不断优化的信息安全治理结构。

2. 企业信息安全“法人治理”的比较优势

其一,与技术治理及管理相比,“法人治理”可以充分发挥技术与法律二元共治,有机互补的优势。技术治理是一种运用确定性和精确性的科学知识,对网络社会中的人们的行为进行一定的管制,以期符合治理者自身利益的活动[10]。然而,没有绝对完美的技术,安全风险总是存在。为了确保安全,技术人员也可能会过度使用验证、加密等技术而无形造成企业发展的壁垒。技术主管或安全监管部门仅是企业整体结构的一个很小的部分,仅从网络技术角度采取安全措施或是在发生安全事故时采取一定的措施,不能从全局的角度出发解决日益严峻的信息安全问题[11]。故,我们需要蕴含价值理性和道德判断的法律的介入,通过自上而下的权力运作,用法律的规范作用将技术与人、部门、组织有机且动态相连,将对信息的“安全”“可控”的治理目标以“责任”的形式传递、归化到企业中的个体。

其二,“法人治理”可充分发挥企业自治的优势,以较少成本控制安全风险。企业是网络安全事件的受害者,同时也是施害者。在安全风险治理中,与政府、个人相比,企业具有天然的优势。企业是安全事件的直接参与者或受害者,对风险和安全隐患具有更强的感知、分析和应对能力。此外,企业具有保障网络安全的软硬件设施、专业的技术人才与资源优势,更易以较少的成本控制安全风险。

其三,企业信息安全法人治理回应了企业履行保障信息安全“社会责任”的时代诉求。施托伊雷尔认为,现代多中心主义的治理方式与企业社会责任是一体两面。它们以相似的路径重塑着国家与私人之间的关系。参与政府治理既是企业和个人享有的一项权利,也是其承担的一项社会责任[12]。企业内部安全事件常导致社会及国家层面的较大负外部效应,作为国家网络安全保障的核心力量,企业应时刻意识到信息安全治理的社会责任往往蕴含着人权、社会稳定及国家整体安全的内容。

三、美国企业信息安全法律治理:立法监管、企业自治及启示

(一)立法渊源广泛,重视保障数据的“机密性”“可用性”与“完整性”

美国企业的信息安全义务的立法渊源广泛,主要包括联邦、州层面的法律法规、普通法、侵权法、合同承诺、商业标准、政府规章、国际法律法规及执法行动等。联邦及州层面的成文法律、法规是最主要的立法渊源,在立法措辞上多使用“安全(security)”与“保障(safeguards)”。企业的信息安全义务多以保护信息安全的三性为目的,在措辞上多使用“认证(authenticate)”、保护数据的“完整性(integrity)”“机密性(confidentiality)”及“数据可用性(availability of data)”等予以体现。如,联邦层面的立法包括1996年《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act,HIPAA)、1999年《统一电子商务法案》(Uniform Electronic Transaction Act,UETA)、1999年《金融服务现代化法案》(Gramm-Leach-Bliley Act,GLBA)、2000年《全球及国内商务电子签名法案》(Electronic Signatures in Global and National Commerce Act,E-SIGN)、2002年《萨班斯-奥克斯利法案》(Sarbanes-Oxley Act,SOA)、2003年《保护网络空间的国家战略》(National Strategy to Secure Cyberspace)、2015年《网络安全法》(Cyber Security Act)等。以上立法涉及医疗健康、电子商务、金融、企业内控等方面,涵盖企业保障信息安全“三性”的一般义务性规定。

(二)企业信息安全义务主体为所有企业,义务客体涵盖“所有数据”

美国企业信息安全治理义务主体涵盖所有行业部门的所有企业。尽管早期的个别成文法将企业

的信息安全义务限定于某一行业内的企业,但随着美国网络与信息安全立法数量的增多,实际上所有企业承担了立法赋予的信息安全义务。在司法实践中,美国企业信息安全义务的法律演进始于联邦贸易委员会(FTC)反公平贸易的实践,随后众多的州立法持续跟进,法院通过一系列司法判例将企业信息安全义务扩展至所有企业。2002年起,借助于一系列的执法行动及同意令,美国FTC根据《联邦贸易委员会法》(FTC Act)关于反公平贸易的规定扩大了其执法行动的范围,认为企业即使未对信息安全状况作出虚假陈述,但怠于履行个人信息安全保障义务本身就是一种不公平的贸易行为。2004年,加州颁布了一项立法,规定所有企业应采取合理的安全措施与实践,保护加州居民的个人信息免受未经授权的访问、破坏、使用、修改或披露。随后,其他州也纷纷效仿,加入立法行列。此外,通过典型案例的审判,法院也开始意识到所有企业都有保障个人信息安全的普通法义务,未能履行该义务即构成侵权[13]。

值得一提的是,近年来美国政府意识到小企业在美国制造业供应链中占据重要地位,但在国防工业基础方面存在弱点,尤其在网络安全威胁和数据泄露方面也存在脆弱性及安全漏洞。2018年,美国总统特朗普正式签署《NIST小企业网络安全法案》(NIST Small Business Cybersecurity Act),将小企业的网络安全风险防御与治理纳入美国联邦法律。此外,美国企业信息安全义务的客体为所有的公司数据,主要包括个人数据、其他公司数据、电子记录。个人数据保护与美国源远流长的隐私保护制度密切相关,众多联邦立法及州层面的立法都有明确规定。其他公司数据包括公司财务数据、交易记录、税收记录。

(三)更具弹性的"合理安全(reasonable security)"标准是衡量企业信息安全治理成熟度的法定基线,"合理安全"以"程序导向(process-oriented)"为评判标准

美国著名密码学家Bruce Schneier经典名言,"安全是一个过程而并非结果(Security is a process, not a product)[14]。美国人早已意识到信息技术快速更迭必然带来新的安全风险,法律的稳定性难以应对新的安全危机,企业的信息安全义务的衡量标准应更具弹性与张力。美国立法并未明文规定企业应采取什么样的具体安全措施以确保企业获得足够的安全保障,而是要求企业满足更具弹性的"合理安全(reasonable security)"标准,与之类似的还有"适当安全(appropriate security)""合适安全(suitable security)"。"合理安全"标准并非特指具体的安全措施,而是在实践中可发展、可改进且能有效应对安全风险的动态标准。企业是否履行信息安全义务以"程序导向(process-oriented)"为主要评价标准。企业信息安全的法律标准要求公司实施综合性的及书面性的信息安全程序,包括:(1)识别被保护的信息及其系统资产;(2)进行周期性的风险评估以识别公司所面临的资产威胁、脆弱性评估及其威胁发生后造成的损失;(3)选择并实施适当的安全控制措施以控制风险的识别;(4)监控与测试项目以确保其有效性;(5)根据项目的变化进行不断的审查与调试,包括进行常规性的独立审计并在必要时进行报告;(6)监督第三方服务提供者的协议。实际,以上的过程并非一成不变,还可被不断地审查、修订及升级[13]。在美国的司法实践中,"程序导向型"的公司信息安全法律标准是基于GLBA的规定,首先应用于一些关于金融行业的企业信息安全规制中。随后,HIPAA也有类似的规定。

除上述成文法规定外,美国FTC认为企业应将"程序导向型(process-oriented)"标准作为企业最佳实践(best practice)应用于所有企业,未能履行该标准的企业将被FTC裁定为未履行"合理的"信息安全义务。在一些典型案例中,"程序导向型"成为司法实践中法官认定被告是否违反"合理安全"义

务的主要审查标准。

(四)优化的“法人治理结构”是企业信息安全治理的重心

美国政府认为建立自律且持续完善的企业信息安全治理结构是应对企业信息安全难题的有力手段。早在2003年8月,美国商业软件联盟(BSA)信息安全特别工作组在华盛顿召开的商业软件联盟年度CEO论坛上提交了名为“信息安全治理:从框架迈向行动”的白皮书[15]。白皮书认为,尽管政府已经制定了众多的法律规制企业IT安全,但企业建立有效的、可持续的信息安全治理框架仍不可替代。2004年12月,美国国土安全部(DHS)在加州圣克拉拉市主办的“国家网络安全峰会”成立“法人治理工作组”[16]并发布了“信息安全治理行动倡议(call for action)”报告[17]。该报告将企业理想的企业信息安全治理结构以企业规模为分类标准,归纳为大型企业、中型企业、小型企业及公共机构几种类型(见图1—图4),为企业信息安全治理结构的建立与完善提供了指引。

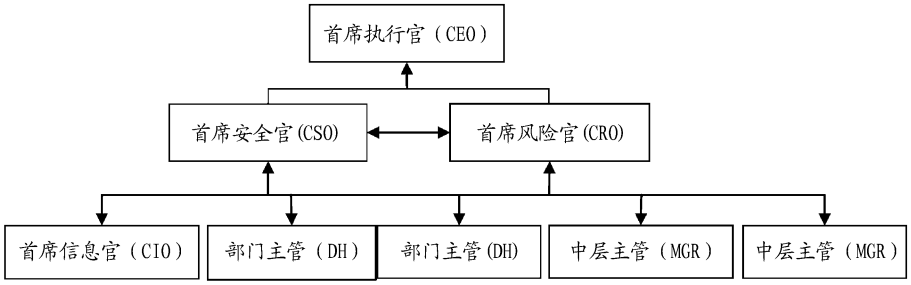

图1　大型企业

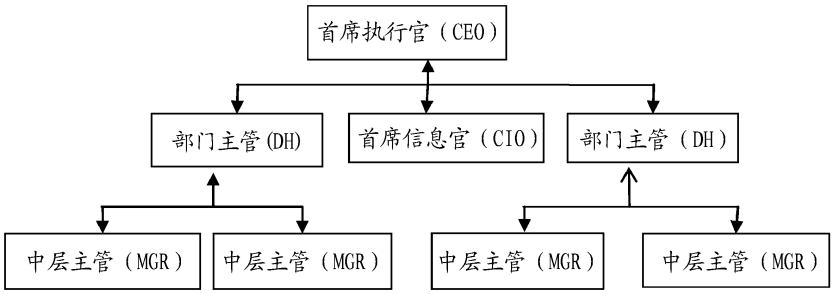

图2　中型企业

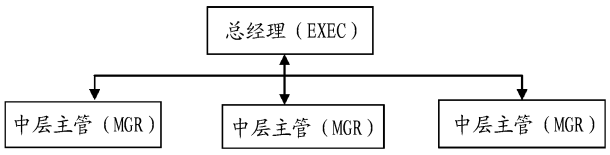

图3　小型企业

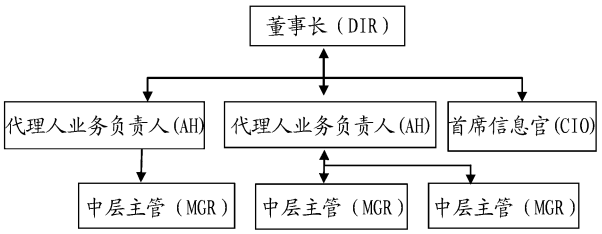

图4　公共机构

(五)明晰CEO及高级管理人员信息安全责任是企业信息安全治理的关键

美国企业CEO及其高管人员的信息安全趋于明晰,如2004年美国“信息安全治理行动倡议”的报告从职能主体层面明确了大型、中型、小型及公共机构在总裁、首席安全官、首席信息官、首席风险官、部门负责人、中层主管,以及雇佣员工层面的信息安全职责,为企业信息安全治理义务的明确提供了指引(见表1)。

表1 美国企业信息安全职责

主体	责任	大型企业						中型企业				小型企业			公共机构			
		CCEO	CCSO	CCRO	CCCIO	DDDH	MMGR	CCEO	CCIO	DDH	MMGR	EEXEC	MMGR	EEXPL	DDIR	AAH	CCIO	MMGR
高级管理层 Senior Exeutive 特别是对于公司董事会直接负责的首席执行官应该监督企业的整体信息安全计划	1. 对组织内的不同的功能主体分派责任、义务及权力	••						••				••			••			
	2. 监督组织对于文件要求的安全需求的遵从,包括因遵从而产生的授权行为及执行责任	••						••				••			••			
	3. 向董事会、受托人或其他类似的治理实体报告对于本文件的组织遵从情况,包括:总结评估结果,明确对于残余风险的接受程度;信息安全政策的显著缺陷及应对此缺陷的补救措施	••						••				••			••			
	4. 指派具有专业资质的高级信息安全官的人选,以执行文件要求的信息安全计划	••						••				••						••
总经理 Executive 管理团队的具体成员,向高级管理层直接汇报,应监督组织的安全政策与实践	1. 监督信息安全政策、原则、标准、指南的发展与实施,并与公认的安全实践保持一致,例如 ISO/IEC 17799		••									••			••	••		
	2. 确保信息安全管理流程与企业战略及运营规划流程相融合		••									••						
	3. 使信息安全政策与程序同相关的信息资源管理政策与程序相协调		••					••	••			••			••			
	4. 对于由企业使用或运营的信息遭受未经授权的使用、披露、破坏、篡改或损毁时应提供与风险或损害相匹配的信息安全保护措施			••					••			••				••		
	5. 确保企业内部独立职能部门制定并维持一个信息安全计划		••										••				••	
	6. 确保企业的高级信息安全官与部门主管相协作,阶段性向高级管理层报告包括补救措施在内的信息安全计划的有效性		••						••			••						••
	7. 确保高级信息安全官协助企业部门经理履行信息安全责任		••									•	••				••	
中层管理者 Mid-level manager 各职能部门的管理人员,其应该确保上级主管针对本部门的信息及信息系统制定的安全计划的执行	1. 评估因对信息或信息系统进行未经授权的使用、披露、中断、篡改或毁坏而致的风险与损失			••					••				••						••
	2. 在风险评估和成本最小化的基础上执行政策和程序,将信息安全风险降到合理水平			••					••	••			••						••
	3. 确定与保护企业信息和信息系统相匹配的信息安全保护水平			••			••				••		••						••
	4. 阶段性测试评估信息安全控制项及技术,确保其有效实施						••				••		••						••
	5. 确保公司所培训人员能够协助公司达到文件和相关的政策、规则、标准的要求						••				••		••						••
	6. 确保所有的雇员、契约人和其他的信息系统用户能够意识到他们在公司信息安全政策中的角色和所承担的责任																	
员工与用户理解、遵从政策与实施	1. 按照他们在公司中的角色,知悉相应的信息安全政策	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••
	2. 遵守与其所使用的信息和信息系统相关的信息安全政策程序	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••
	3. 按照正确的途径报告安全政策的弱点或突发事件的影响	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••	••

注:引用美国“信息安全治理行动倡议”报告中大、中、小型企业不同层级安全责任分配的主要内容。

(六)启示

从以上内容综合分析来看,美国企业信息安全治理具有如下鲜明的特征。第一,美国企业信息安全法律治理呈现出立法监管与企业自治有机结合与互补的特色。在国家立法监管层面,美国没有单一立法明确规定企业应采取什么样的具体的安全措施以确保信息安全“三性”,而是为企业设定了一个更具弹性的“合理安全”的法定基线,企业是否履行义务在司法实践中以“程序导向”为评判标准。由此可见,国家立法监管在企业信息安全治理中仅起到宏观引导与规范的作用,而不同类型的企业在如何合规中倚重“程序正义”的指引,两者各有其作用发挥的空间。第二,企业信息安全治理的定位明确合理,即企业信息安全治理是“法人治理”问题而非技术问题或管理问题。立法鼓励不同规模的企业根据自身实际量身定做最优化的法人治理结构,从而将信息安全治理深度融入企业机关的权力分配与行使关系中,最终将信息安全融入企业的文化基因。企业自治在信息安全治理中更为核心,是有效实现信息安全“合理安全”的关键。第三,美国企业的信息安全治理义务覆盖大、中、小型企业。近年来,美国开始意识到小企业是供应链安全中不容忽视的一环,将对小企业的安全风险防控提升到立法层面,这表明美国意识到网络安全风险严峻,网络安全的“短板效应”需要“整体安全”的防御思维予以消解。第四,企业信息安全法人治理的关键环节在于明晰大、中、小型企业,以及公共机构的高、中级管理人员的信息安全责任,清晰的责任分配机制有利于企业内部不同部门的协作与追责,实现企业信息安全法人治理效用的最大化。

四、企业信息安全法律治理的中国进路

企业信息安全法律治理成熟度是衡量国家网络安全强弱与否的重要标尺。中国企业信息安全法律治理应在借鉴发达国家有益经验的基础上立足于本国国情,妥善处理好安全与发展、立法监管与企业自治的关系。在立法层面应明确企业信息安全法律治理的基本原则,充分发挥立法对于企业信息安全治理的指引、监督与激励作用,激励企业从被动“合规”迈向主动“治理”,将信息安全文化融入不断优化的企业治理结构中,以助力网络强国建设。

(一)企业信息安全法律治理应谨慎权衡“安全”与“发展”的关系

尽管网安法标题贯以安全,但安全与发展天平却不能失衡。立法对于“安全”的过分倚重将制约发展,难以确保整体国家安全。发展是化解安全危机的前提,发展意味着我们将掌控、利用更为先进的技术、产业,培养出成千上万的安全顶级人才去促进安全。发展思维将使我们扭转任何封闭与停滞的观念,例如辩证地将漏洞攻击与信息泄露视为安全防御能力的提升和治理手段的完善会为我们提供丰富的实践案例和经验教训。反之,网络安全立法对“发展”的过分倚重将导致社会机体对安全风险抵抗力的降低或丧失。

我国信息与数字化的水平与发达国家相比较低,产业低端重复、创新乏力是痼疾。谨慎权衡安全发展需要我们不忽视具体国情,充分发挥“治理”型立法的引导、激励作用。一方面,企业信息安全法人治理应立足于国家“整体安全”防御思维,即重视关键基础设施运营企业,也兼顾小型企业网络安全,以消弭安全“短板”;另一方面,企业信息安全法人治理结构应“量体裁衣”,重视规范个体责

任和企业安全文化的普及。

(二)优化我国企业信息安全法律治理的基本路径

1. 立法应明确企业信息安全法律治理的基本原则

(1)依法治理原则。一方面,企业信息安全治理应基于国家引导与立法规范,以相关法律原则、规则为治理依据;另一方面,企业应以法律为遵从基线,依法确立法人治理的组织架构、安全管理与技术标准、产品设计、研发流程等。依法治理原则既要求企业有法可依,亦要求企业有法必依。企业有法可依需要网络安全法制体系的建立与完善,为企业遵从营造一个法制化的环境,而企业有法必依则考验企业高管对于法规遵从的智慧。

(2)CEO参与原则。企业信息安全是企业法人治理层面的问题,应该引起CEO的高度重视与参与。一是企业CEO应参与企业信息安全的战略规划与政策制定;二是CEO应参与、监督、协调企业信息安全政策的执行;三是CEO应对企业信息安全义务的履行不能,承担相应的责任。

(3)透明度原则。企业信息安全法人治理结构应当是企业法人治理的一个子集并确保其透明化。企业对安全事故的披露也应当透明化。企业在安全事故发生后,依法以特定的方式及时将该安全事故信息、潜在的风险、采取的措施通知监管部门和利益相关者。尽管信息安全的披露在短期内会增加企业利益减损,但从长远看有益于增强相关行业和整个产业抵御安全风险的能力。

2. 充分发挥立法的引导与激励作用,鼓励企业从"被动"合规迈向"主动"治理

法律的激励功能、惩戒功能同组织管理功能一并作为法律的三大基本功能,激励功能的社会认同感最强。激励法律的制定是基于人们对不同利益的需求,通过给予利益,激发人们的积极性,从而实施法律所希望的行为,不仅给行为人带来利益,也能达成立法者预期的某种效果[18]。与美国相比,我国网络安全立法起步较晚,企业网安法合规欠账多,法规遵从需要企业投入更多的资金与人力成本,故一些企业存在畏难、抵触情绪。我们需要思考如何在发挥立法惩戒功能的同时发挥其激励功能,调动企业守法能动性,使企业从"安全是成本"转变为"安全是投资"[19],进而从"被动"合规迈向"主动"治理。完善网安法的激励功能,鼓励行业自律与企业自治,根据企业信息安全法人治理的成熟度给予物质性、精神性及责任豁免性奖励,具体激励方式可包括并不限于财政补贴、税收激励、政府项目优先(如资源申请优先)、精神性表彰或奖励及责任豁免。

3. 立法引导和激励企业建立"强制与自愿相结合"的信息安全"法人治理"结构,消弭安全"短板"

企业信息安全法人治理结构的建立和优化应当成为我国企业信息安全法律治理的重心。立法应当鼓励所有企业根据其实际情况构建"强制与自愿相结合"的法人治理结构。建议延续网安法的制度设计思路,对国家网络安全保障中具有"关键性"及"战略性"的关键信息基础设施(CII)运营者进行强制性法人信息安全治理,对于非CII运营者则以立法激励与企业自愿为主。强制性的制度内容包括:第一,对于大、中型CII运营者构建层级清晰、权责分明的信息安全法人治理结构,并将其作为法人治理结构的一个子集予以重视。企业董事会(或董事长)、高层主管应从战略上重视对安全风险的"感知—抵御—应对",将防控安全风险融入企业战略规划、资金预算、业务拓展、产品研发与

销售等关键环节,最终将安全融入企业文化。

企业信息安全法人治理的关键在于明确企业的董事会(或董事长)、CEO(或总裁)、高层主管(包括首席安全官、首席信息官、首席风险官及部门主管)、中层主管及普通员工的信息安全职责:(1)企业董事会(或董事长)应当从战略上充分认识信息及信息安全的重要价值,确定企业重要资产,统一部署企业综合性、全局性的信息安全计划(如企业级漏洞响应计划或综合性风险评估计划),监督企业高管定期汇报信息安全计划执行的适当性和有效性。(2)CEO(或总裁)是企业信息安全的直接负责人。应当确保知悉企业的战略计划、风险偏好及运营策略,在此基础上制定、升级企业的信息安全政策,监督企业对国家法律法规的全面遵从;对企业其他中高层主管、员工分派信息安全责任、义务及权力,明确不同层级人员因法规遵从或企业信息安全计划产生的授权行为与执行责任,监督、协调企业信息安全政策的执行;向董事会报告企业信息安全政策的执行,包括关键风险识别、风险评估结果、企业风险耐受水平及风险防控计划;选任专业资质的信息安全官执行企业信息安全政策;确保企业有充足的人力、财力及技术资源以执行安全政策。(3)企业高层主管应确保企业的安全政策与企业战略、业务的一致性,与公司内外的利益相关方沟通协调;检查企业信息安全政策的进展和执行,确保安全法规的遵从;确保企业的信息安全保护措施与企业可能承受的信息安全风险相匹配;与各部门负责人协调一致,定期向 CEO(或总裁)汇报信息安全计划的执行情况;确保企业员工接受有效的信息安全培训并知悉企业的安全政策。(4)企业中层主管在风险评估和成本最小化的基础上执行企业的信息安全计划;定期测试、评估企业的信息安全控制技术、措施,确保其有效运行;确保雇员、合同相对人和用户对企业信息安全责任的履行。(5)企业员工应知悉、遵守企业的信息安全政策,及时报告政策的弱点及突发性信息安全事件的影响。

第二,对于资金有限、安全保护措施不够完善的小型 CII 运营者,可考虑给予一些资源支持与协调,确保其构建与自身实际相符的安全治理结构。充分重视企业总经理或中层主管信息安全责任之履行,包括总经理应当确保公司战略、运营流程与企业信息安全治理需求相融合;识别企业重要资产、评估信息系统安全风险、制定应急计划等;确保企业对于安全的资金投入;中层主管应当负责执行企业的信息安全政策,阶段性地测试评估信息安全控制项,确保有效实施;确保对企业雇员的信息安全培训

4. 重视企业董事、高级管理人员信息安全义务的履行,将其作为《公司法》董事、高级管理人员“忠实与勤勉义务”的适当延伸

忠实与勤勉义务是现代治理结构下企业董事会成员对于公司的法定义务。我国公司法第 148 条对董事及高级管理人员的忠实与勤勉义务作出了明确规定。实践中,董事及高管义务有扩大趋势,这源于法律从“股东至上”到对企业社会责任及利益相关者权益保护之重视。目前,严峻的信息安全风险正威胁着我国国家安全、社会稳定及个人权益,企业应勇于承担保障信息安全的社会责任,这也依赖于企业董事及高管对于信息安全义务的积极履行。企业董事及高管的信息安全义务可作为公司法层面“忠实与勤勉”义务的有机组成部分,包括:(1)基本的信息安全义务,即确保企业对国家网络与信息安全立法制度(如 CII 保护,网络安全审查、数据出境评估等)的全面遵从,配合、

协助执法检查。(2)履行其在企业信息安全法人治理中的核心义务,包括被保护的信息与资产的识别;制定、升级企业的信息安全政策;安全风险评估;确保企业员工接受有效的信息安全培训;确保企业有充足的人力、财力及资源实现公司的安全政策。此外,还可鼓励公司章程中增加董事、高管对于保障企业信息安全的注意义务,接受公司股东与公众的监督。

5.引导和促进企业信息安全文化建设,深度融入企业法人治理中,以凸显安全文化的价值

法律对于安全风险的防控需要借助文化的力量,通过主流文化的传播使法律价值得到普遍认同,从而有效提升法律的实施效果。企业信息安全文化建设可助力于修复不同社会主体的安全认知"漏洞",提升企业在网络安全保障中的效用。企业信息安全文化建设不可忽视两个层面:一是重视企业信息安全文化在法人治理层面的融合。企业信息安全文化不只局限于员工安全培训等常规活动,还应当在企业的总体战略、理念、形象识别、业务规划、生产过程控制及监督反馈等各个方面融合安全文化的内容,最终将安全文化融入企业法人治理结构中;二是重视从企业高管到基层员工的"个体"信息安全意识的提升,将安全意识与个体责任挂钩,使"人"成为企业安全风险防御的最强大资产。安全文化的普及与人的安全意识的提升是对抗攻击的最有效的武器。

参考文献:

[1]张康之.论主体多元化条件下的社会治理[J]中国人民大学学报2014,28(2):1-13.

[2]李辉,任晓春.善治视野下的协同治理研究[J].科学与管理,2010,30(6):55-58.

[3]倪良.论网络安全对国家安全的颠覆性影响[J].中国信息安全,2016(9):26-27.

[4]洪延青."以管理为基础的规制":对网络运营者安全保护义务的重构[J].环球法律评论,2016,38(4):20-40.

[5]周汉华.探索激励相容的个人数据治理之道:中国个人信息保护法的立法方向[J].法学研究,2018,40(2):3-23.

[6]安全内参.美国国家安全局:黑客可在24小时内将已知漏洞武器化[EB/OL].(2018-05-04)[2019-05-10]. https://www.secrss.com/articles/2432.

[7]沈逸.专家解读网络安全法草案:为建设网络强国提供制度保障[EB/OL].(2015-07-16)[2019-05-12]. http://www.thepaper.cn/newsDetail_forward_1353139.

[8]弗里曼.合作治理与新行政法[M].毕洪海,译.北京:商务印书,2010:24-25.

[9]朱伯玉,冯向辉.司法人治理结构的法理学分析[J].江苏社会科学,2002(3):171-175.

[10]郑智航.网络社会法律治理与技术治理的二元共治[J].中国法学,2018(2):108-130.

[11]马民虎.美国公司信息安全治理研究动态(上)[J].信息网络安全,2006(9):60-61.

[12]STEURER R. Disentangling governance: A synoptic view of regulation by government, business and civil society[J]. Policy Sciences,2013,46:387-410.

[13]SMEDINGHOFF T J. Information security law: The emerging standard for corporate compliance[M]. IT Governance Publishing Ltd,2008:24-26.

[14]SCHNEIER B. The process of security[J]. Information Security,2000(4):1-4.

[15]BSA information security framework for CEO governance[EB/OL]. (2003-10-23)[2019-06-12]. http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/118100/.pdf.

[16]IT GOVERNANCE INSTITUTE. Information security governance: Guidance for boards of directors and executive management[M]. 2nd Edition. Printed in the United states of America,2006:43-44.

[17]CONNER F W. Information security governance: A call to action[EB/OL]. (2004-06-10)[2019-06-12]. https://www.dhs.gov/sites/default/files/publications/csd-informationsecuritygovernance-acalltoaction-2004.

[18]付子堂,孟甜甜.激励型法的学理探讨:以美国《拜杜法案》为切入点[J].河南财经政法大学学报,2014(3):60-66.

[19]ROUX Y. Blending corporate governance with information security[EB/OL]. (2006-07-05)[2019-06-15]. http://www.isticom.it/documenti/evidenza/08_Yves_Le_Roux_2.pdf.

Legal governance of enterprise information security

ZHANG Min, MA Minhu

(*School of Law, Xi'an Jiaotong University, Xi'an 710049, P. R. China*)

Abstract: Legal governance of enterprise information security is an effective way to ensure national network and information security, defend personal information rights and interests, and promote the industry to "develop" in "security". The enterprise information security obligations in China's Law are mostly in static and tactical state, which can not protect against the changeable security risks. The incentive mechanism of compliance with the laws and regulations of enterprises is lacking, and the motivation to compliance is insufficient. The popularization of information security culture is lacking. In order to solve the above problems, we should base on the thinking of legal governance and position "corporate governance" as the focus of legal governance of enterprise information security. In the level of system design, we should draw lessons from the beneficial experience of American enterprise information security legal governance in legislation supervision and enterprise autonomy, take the basic principles of information security legal governance as the guide, give full play to the role of legislative incentive, encourage all enterprises to establish a mandatory and voluntary information security "corporate governance" structure, attach importance to the implementation of information security obligations of the directors and senior executives, promote the construction of enterprise information security culture, and highlight the value of security culture.

Key words: governance of law; collaborative governance; information security obligations; information security corporate governance

(责任编辑　胡志平)