ISSN 2096-2282
CN 10-1421/TP

网络空间安全
Cyberspace Security

CCiD 赛迪出版物　2022年第6期　12月25日出版　总第142期

ISSN 2096-2282
12>
9 772096 228224

国家新闻出版广电总局（原）首批认定学术期刊
中国计算机学会（CCF）审定优秀期刊

本刊已被以下期刊数据库收录：
中国科学引文索引库期刊（CSCI）
中国知识资源总库（CNKI）源期刊
中国学术期刊网络出版总库
中文核心期刊（遴选）数据库
中文科技期刊数据库

目次 Contents

网络空间安全 总第142期 第13卷 第6期 2022年12月

网络安全为人民
网络安全靠人民

密码与应用

系统与网络

可控与防御

人才与教研

保护知识产权
就是保护创新

企业网络安全人才培养的探索与实践

齐丽钰
（中国软件评测中心/工业和信息化部软件与集成电路促进中心，北京100048）

摘 要：

[目的/意义] 近年来，网络技术的更新迭代，使得网络暴露在越来越多的风险因素之中，网络黑客、病毒等使得网络安全逐渐成为企业重视的一项任务。对此，企业构建网络安全体系建设、培养网络安全人才有着十分重要的意义。

[方法/过程] 基于积极响应企业的网络安全需求，通过分析网络人才需求特点网络人才培养面临的问题，找到企业相关部门需要积极探索新型网络安全人才培养模式。

[结果/结论] 以我国企业为主体，对网络安全人才的培养体系及其现状展开研究，明确培养思路、培养方法等，使网络安全人才的培养更加系统化和实践化。

关键词： 网络安全；人才培养；方法实践；复合型人才；人力资源管理；人才梯队建设

中图分类号： C962 **文献标识码：** A

Exploration and practice of enterprise network security personnel training

Qi Liyu
(China Software Testing Center/Research Center for Computer and Microelectronics Industry Development of ministry of Industry and Information Technology, Beijing 100048)

Abstract:

[Purpose/Significance] In recent years, the updating and iteration of network technology has exposed the network to more and more risk factors. Network hackers and viruses have gradually made network security a task that enterprises attach importance to. Therefore, it is of great significance for enterprises to construct network security system and cultivate network security talents.

[Method/Process] Based on the positive response to the network security needs of enterprises, by analyzing the characteristics of network personnel demand and the problems faced by network personnel training, it is found that relevant departments of enterprises need to actively explore new network security personnel training mode.

[Results/Conclusion] Taking Chinese enterprises as the main body, this paper studies the training system and current situation of network security talents, and clarifies the training ideas and methods, so as to make the training of network security talents more systematic and practical.

Keywords: network security; personnel training; method practice; inter-disciplinary talent; human resource management; talent echelon construction

0 引言

网络安全是指对网络系统及其相关各种硬件设备、软件应用等存有的数据信息进行保护，使之不受外界或人为的干扰因素而保持正常稳定运行。但从国家层面看，网络安全因天然属性具有一定的政治属性，是处于“陆、海、空、天”之外的第五大战略空间。正因如此，网络安全也是企业、国家的经济、政治等领域的重要承载工具，与企业、国家的发展息息相关。

根据中国互联网信息中心2022年8月发布的《中国互联网络发展状况统计报告》显示，截止2022年6月，我国网民规模为10.51亿，互联网普及率达到74.4%。虽然网络安全形势持续好转，遭遇安全问题的用户比例有所下降，但是还是有21.8%的网民遭遇着网络安全问题，个人信息遭到泄露。

随着网络安全行业发展逐渐步入成熟期，下属分支也逐渐细分化，这导致该行业对人才的需求逐渐增多。除了军队、公安等部门对高级网络安全人才的需要外，从事网络安全的企业中人员缺口也越来越大。据有关资料统计，截止2014年，我国重要行业网络安全人才需求70余万人，而到2022年达到210余万人。目前，我国网络安全专业人才缺口预估在50万以上，所以，解决网络安全建没问题的关键是解决网络安全人才的匮乏。

为保障网络安全行业的健康、正常、有序发展，网络安全人才队伍的建设与培养，则是企业信息化发展的重要战略之一，企业相关部门应探讨明确企业信息安全保障体系建设的基础和所需资源，并吸纳人才开展建设。对此，决策者既要掌握网络安全人才培养的发展规律，又要制定符合本企业实际需求的人才培养模式，为企业发展贡献合格的、优秀的网络安全人才。

1 网络安全人才需求特点

1.1 具有交叉学科知识的复合型人才

网络安全是以互联网为基础发展起来的学科，并在此基础上发展出其他延伸性学科领域。因此，网络安全涉及计算机科学与技术、通信工程、管理学等多门学科，这些学科分属理科、工科等类别之下。但是，相对于传统的计算机学科，网络空间安全学科涉及的科目更多，复杂性更高，也因此需要具备交叉学科背景的人才，更关注多学科交叉情景下的网络安全实践。

1.2 网络安全实践型人才

网络安全是一门实践性较强的学科，因而对于相关人才的素质也有相应的要求。网络安全人才需要具备较强的动手实践能力或者是有较丰富的实践经验，以便在审计、应急响应、漏洞恢复等方面尽快适应工作内容和工作要求。人才在入职后还要经历培训等阶段，使人才将理论学习与技术实践紧密结合，逐渐在学习与实践中锻炼成为具备专业实践能力、创新能力为一体的网络安全人才。

1.3 多元化发展方向的人才

网络安全人才既要有多学科理论背景，又要有较强的实践能力，且在实践中还要考虑多元化发展方向。从企业经营实际需求来看，企业需要网络安全人才的发展方向，主要集中于系统运维、系统管理等，具体而言，网络安全人才的细分岗位包括系统安全管理、系统安全运营、系统运营维护、系统研发等。可见，多类型、多层次的网络安全人才，有助于企业的网络系统运行更加安全、稳定。

1.4 能够持续性学习的人才

由于网络安全行业的学科背景特殊性、行业要求特殊性，因此网络安全人才也要求具备一定的持续性学习能力，以保证从业人员可以很快跟进和适应行业工作的发展和变化。网络信息技术的更新迭代速度比较快，网络安全人才只有培养持续性学习的习惯，才能迎接快速发展信息技术的挑战。

2 人才培养面临的困难

2.1 人才素质与企业需求不符

考察实际企业招聘与人才求职的不同需求，

可以看出，人才素质与企业需求不匹配的主要原因有5个方面。

第一，企业与高校的教学侧重点不同。

多数企业更注重经验，员工一般都是从工作中积累经验；而高校的教学体系更注重理论方面的教学，学生通常难以由此获得实践经验。

另外，在网络安全行业中，专业技术更迭十分频繁，高校的理论课程仅限于基础性教学，而这些往往与行业发展无太大联系，因而两者出现脱节，学生毕业后进入企业则感到所学非所用。

第二，从事网络安全行业的人员薪资待遇因岗位职能不同而有较大差异。

在大学期间，所学专业为网络安全的学生，在企业中的工作业绩比学历更低的人的表现稍差，收益差距和价值成就感也较大。

另外，从事不同岗位方向人的薪资水平也有差异，系统防护类岗位的薪资水平相对更高，导致不同岗位之间形成了围城效应。

第三，业务需求使企业网络安全建设要求人员能够快速熟悉业务流程。

从事网络安全的人员除了具有专业知识外，还要明确企业的业务需求，并与涉及业务的其他部门互相配合协作，这就要求员工具有一定的沟通能力、业务熟练度等。但是能兼顾技术与业务的网络安全人才往往是少数人，多数人一般擅长其中一种。

第四，网络安全专业在国内成立时间较短，毕业生人数有限，且人才来源渠道单一。

这直接导致人才市场上供需关系失衡，企业招聘渠道狭窄，而毕业生又对行业缺乏足够了解，员工入职一般也都是靠熟人引荐，这就导致企业缺乏可靠、稳定的人才输送机制，企业很难组建素质较好的网络安全队伍。

第五，国内网络安全认证体系不健全。

这种不健全导致行业缺乏持续认证、缺失专业教育、缺少较为完善的人才标准，直接造成招聘的人才素质良莠不齐、专业水平和业务能力差距较大。

2.2 人才的整体工作能力普遍偏低

造成这种现象的原因不止在员工自身，行业发展阶段和自身特征也占较大比重。

首先，企业内部从事网络安全工作的老员工因忙于业务，剩余时间精力难以支持老员工学习新技能，导致老员工技能更新跟不上行业技术变化。

其次，绝大多数从事网络安全行业的企业，并没有为员工设置专门的网络安全技能实验和训练环境，员工自身也难以找到可以学习提升的教学资源和机会。虽然少数企业有提供相关技能培训的机会和资源，但是由于员工与企业的认知度不足，导致这部分培训往往只是应付任务，达不到预期效果，也因此很难具备持续性。

再者，网络安全从业人员在企业部门分配中，只是一个负责日常设备调试的小部门，部门业务、发展规划没有得到上级决策者的重视，员工价值、团队价值没有得到锻炼和体现的机会。

2.3 网络安全人才的职场稳定性较差

从事网络安全行业的企业既有央企、国企，也有民企、中外合资企业、外企等多种所有制形式。但是，从福利待遇和发展平台来看，央企和国企的发展明显要好于多数民企，很多从业人员考虑到职业的心智水平、职场环境、工作强度等因素，往往也会选择央企、国企这类体制内的工作。因此，除了这两类企业以外的其他企业的薪酬福利、晋升通道、资源投入程度等，都很难与之竞争，从而导致行业人才流失较多，最终大概率地会流向发展和平台更好的企业。

3 人才培养存在问题的主要原因

3.1 培训体系不完善

网络安全行业往往需要具有跨学科背景的人才，同时对于相关人才的实践能力也有着严格要求。然而现状却时行业标准与人才水平不相称。因此很多企业需要对员工进行大量的岗前培训，或是由老员工一对一指导。培养方式十分单一，培训体系也不够健全，部分中小企业甚至是让员工自主学习。

由此可见，网络安全行业的员工培养还有很大的完善空间，各个企业应当基于自身业务流

程、发展现状有针对性的制定培养方案，例如在培训网络安全工作人员时可以有侧重点地介绍公司的核心业务，同时强化对风险意识、责任意识的培训，尤其是在涉及知识产权、公司商业秘密的情况下，提高员工对网络安全工作任务的重视程度。

3.2 管理体系不科学

我国网络安全行业起步较晚，发展十分不完善。行业领袖较少，企业缺乏发展的参考对象。在管理网络安全人员时重视行业门槛，对从业经验、学习背景有着严格要求，但忽视实际的应用能力与培养空间。企业不应当将发展压力留给员工本身，而应当承担起管理职责，从招聘、培训、绩效考核等多方面着手，打造契合企业发展的团队。

首先，在招聘时对应聘者多加了解，例如金融投资公司可以选择具有经济背景的人才。

其次，对入职员工展开系统的培训，帮助员工了解公司的组架构，明确自身职责。

最后，根据职位要求与个人能力制定合理的绩效考核目标，利用薪资激励等方法调动网络安全人员的工作积极性。

总之，企业需要在人才管理方面探索出完整、系统、灵活且高效的体系，才能更迅速的突破瓶颈，实现长远地发展。

4 人才培养的新策略

4.1 企业应制定激励政策留住人才

目前，我国网络安全行业正处于发展期，很多方面的建设与发展都需要人才来铺路，因而行业处于严重的人才紧缺阶段。

对此，各大高校、研究所、科研单位等应采取不同形式、不同途径的人才培养方案，为企业与科研单位的发展提供充足的人力资源。

但这只是开始，最关键的是要能够留住培养出来的人才，关注人才的去留，以防优秀人才的大量流失。这也是很多企业和科研单位的老大难问题，很多企业都想招聘高层次人才，但又苦于企业资源、平台对人才缺乏足够的吸引力，企业给出的人才福利政策也不见成效。因此，人才去留问题始终是各企业高层管理者和人力资源管理部门所面对的关键性、决定性问题。

美国对于稳住人才、构建高稳定性的网络安全队伍已经初具完善措施，这一方面对于我国是一个很好的参考案例。面对网络安全人才这一特殊岗位群体，企业应适当提高对人才的激励措施，并在制度上有所体现，从制度层体现网络安全人才的重要性与特殊性。

4.2 完善企业的人才管理体系

针对网络安全人才的培养，企业可以在制度上做出两项调整。

第一，构建人才培养整体规划。企业管理者可以根据本企业的人才需求情况，从组织层面出发，补充新的规章制度、更新原有的企业内部运营体系，并与人力资源部门配合，构建健全的、贯穿培训全程的人才管理体系。

第二，创新人才选拔模式。在与企业高层管理者沟通过后，人力资源部门应根据企业的人员选拔要求，完善选拔任用程序，采用“目标+能力素质+理论素养+岗位适应性”的选人模式，应企业要求为企业设计符合业务需求的网络安全队伍。

完善的网络安全人才培养体系应在完善一系列人才培养措施的背景下实现。具体而言，企业应做到4点。

其一，设计完善的人才引进机制。企业应明确并规划高层次人才引进的相关工作内容，如例引进目标、保障激励、考核评价、管理监督等。

其二，设计符合人才成长规律的培养体系。一般来说，企业都是通过制定建设网络安全人才队伍的制度来配套现有制度，在人才培养、评价、选拔任用、引进、激励保障等方面形成系统完备、科学规范、有效管用、简便易行的制度体系。

其三，创新合理的人才考核评价指标体系。企业对于人员学历等背景的评价与看法依然局限于过去的刻板印象，往往理想化地认为学历越高的人才和资历越多的人才能够更适合企业的发展需求，为企业带来更多利益，而能力与业绩则是靠积累工作经验，不像学历和资历更有分量。但是，人才并不

够的吸引力，企业
效。因此，人才去
者和人力资源管理
问题。

高稳定性的网络安
一方面对于我国是
络安全人才这一特
高对人才的激励措
制度层体现网络安

系

企业可以在制度上

划。企业管理者可
从组织层面出发，
的企业内部运营体
建健全的、贯穿培

在与企业高层管理
据企业的人员选拔
“目标+能力素质
人模式，应企业要
络安全队伍。
系应在完善一系列
体而言，企业应做

机制。企业应明确
作内容，如例引进
理监督等。
津的培养体系。一
网络安全人才队伍
培养、评价、选拔
系统完备、科学
度体系。
评价指标体系。企
看法依然局限于过
为学历越高的人才
业的发展需求，为
绩则是靠积累工作
但是，人才并不

单纯指高学历、高资历的群体，擅长跑业务、搞业绩也是一项本事，企业人力资源管理者应改掉对人才“重学历、资历而轻能力、业绩”的印象，改进考核方法手段，实行业绩评价考核方式，使考核结果更加客观、真实、具有说服力，同时还能反映员工能力、工作业绩等。

其四，健全合理的人才激励机制。归根结底，企业要想真正激励员工自我提升，就要将这一点与员工的切身利益直接联系起来，为员工提供各种福利和发展机会，完善对人才的各种福利待遇，并补充到制度当中严格执行，例如职务晋升规则、带薪休假等福利待遇的制度建设。

4.3 开辟多元化人才招聘渠道

由于网络安全行业人才招聘始终以内部员工推荐为主，招聘渠道和招聘方式缺乏规范化，为企业网络安全人才队伍的构建带来了较大困扰和阻碍。因此，为了提高员工素质、改善人员结构，规范招聘流程并使之运行有效，企业人力资源部门以及高层管理者，应开辟更多新渠道吸纳人才。具体可以采取4项策略。

4.3.1 扩大所需人才的限制范围

在筛选人才的专业背景时，企业不应只将目光聚焦于理工类专业，还应适当招收语言学类专业、管理学等其他专业的人才，以充实企业的人才库，并未以后的业务扩张积累人才资源。另外，企业还可以通过设立有利于人才发展的项目吸引人才，如在职培训计划等。

4.3.2 扩大招聘人才的方式和渠道

企业除了常见的几种招聘方式，如招聘平台、企业官网、内部员工推荐等，还可以寻求其他新型招聘方式。与政府机关等单位有合作的企业可以考虑与政府部门联合招聘并发布公告，搭建点对点的网络安全人才招聘平台。或者还可以尝试开通针对网络安全人才的绿色通道来引进相关高层次人才，并在招聘信息中明确标注绿色通道的招聘方式和简历投递途径。

4.3.3 精简人才招聘流程

一般来说，企业的招聘流程需要经历笔试、人力资源部门面试、应聘岗位所在部门的负责人面试等多轮考核流程，这样的流程往往耗费时间和精力，招聘人员最终能否被录取也是个未知数，面试者的信心会因预期的不确定性而大大削减。为向网络安全人才释放更多的确定性和职位可得性，企业应有针对性地简化人才的招聘流程，将最重要最关键的环节保留，使受邀参加面试的人才感受到企业对其的重视程度及其未来工作的发展情况。

4.3.4 人才招聘的多样性

网络安全行业中也有很多行业细分职位和发展方向，为保证企业核心业务的发展足够顺利，企业应招聘多样性发展方向的人才、多元化发展背景的人才，综合管理并合理分配工作职位，分析这些人才各自的擅长之处并尽可能最大化其优势，为企业应对专业性难题和开发新的业务方向打好人力资源基础。不能只关注行业中对行业发展最有利的少数类型人才，也要适当放宽招聘标准，不仅考虑刚步入社会的高学历人群、已经积累一定从业经验的人群，还可以考虑精通某一项专业技能但在学历和工作经验方面有欠缺的人群等，让人才的自身发展经历为企业的未来发展添加助力。

4.4 规范科学的工作评价与业绩考核体系

科学而规范的网络安全工作评价标准与业绩考核体系，是员工工作的指导手册。对于新入职的新员工，这个体系提供了指导工作与适应企业职位需求的良好模板。对于老员工，这个体系提供了规范工作流程与自我管理的工具。可见，该体系在企业各类职工的工作中都发挥其价值职能，为职工的任职要求与任职资格提供了一般性与指导性的规范。

“科学”与“规范”意味着该体系是针对不同职位来制定相应的职位规范，这也是企业人才培养与人才招聘的重要依据之一。国外已有相关案例供国内企业参考，而我国尚无网络安全相关职位

作分析的统一官方标准，企业只能根据自身需求，摸索着构建相关评价体系，用于加速自身的行业发展和巩固行业地位。但是，这显然不利于我国企业网络安全人才培养模式的完善与成熟，也不利于就业市场中网络安全职位招聘与网络安全人才求职，因此应尽快制定、完善网络安全相关职位标准。

5 结束语

网络安全人才的短缺，不仅是我国国内企业发展的瓶颈，也是国际性的问题。随着我国国际地位的日益提高，我国政府与国内企业对于网络安全行业人才的重视程度日益攀升，对于网络安全行业人才的需求数量在增多和需求质量也在逐渐提高。我国企业的网络安全人才仍有缺口，因此，要想建立一支成熟的安全网络人才队伍，首先要从组织、管理和技术各种层面，加强并支撑人才培养，保持企业核心竞争力，其次就是中国企业还要多借鉴国内外成功企业的经验，不断探索走出一条符合自身特点的网络安全人才队伍建设之路。

参考文献：

[1] 王国军,邹卫国.网络安全技能人才培养探索与实践[J].中国信息界,2021(5):4.

[2] 肖利芳,段梅,王海晖,等.以培养人才为中心的网络空间安全专业模式探索[J].当代教育实践与教学研究,2020(04):90-91.

[3] 王国军,邹卫国.网络安全技能人才培养探索与实践[J].中国信息界, 2021(5):82-85.

[4] 王甲生,付钰,徐建桥,吴晓平.对网络空间安全创新人才军民融合培养问题的思考[J].网络空间安全,2020(06).

[5] 杨惜爱,蒋兰军.网络安全和信息化专业职称评价改革探讨[J].网络空间安全,2021(Z1).

[6] 鲁辉,王乐,何陆潇涵,金成杰,田志宏.网络空间安全人才培养的个体引导和激励策略研究[J].网络空间安全,2019(10).

[7] 闫晓丽.加强我国网络安全人才建设的建议[J].网络空间安全,2018(07).

[8] 陶琳,李小勇.高校培养“五育”网络安全人才的路径研究[J].网络空间安全,2018(07).

作者简介：

齐丽钰（1988-），女，汉族，北京人，北京师范大学，硕士；中国软件评测中心/工业和信息化部软件与集成电路促进中心，助理工程师；主要研究方向和关注领域：网络信息技术人才培养、人力资源管理和人才梯队建设。