我国网络安全人才队伍建设现状及思考

中国信息安全测评中心 位华

网络安全已成为事关经济社会发展、国家长治久安和人民群众福祉的重大战略问题，建立一支规模宏大、结构优化、素质优良的网络安全人才队伍已成为维护国家网络安全和建设网络强国的核心需求。近年来，我们欣喜地看到网络安全人才培养的问题得到了前所未有的重视，国家密集出台一系列战略、政策、法规，无不把网络安全人才队伍建设视为必不可少的一项基础工作。各项人才措施全面推进，得到了全社会的热烈响应。实施网络安全人才工程，需要我们以科学的态度深刻把握网络安全领域以及网络安全人才的特殊性，找准当前安全人才队伍建设中的难点问题，从而为国家的网络安全人才大计提出有针对性的对策建议。

中国信息安全测评中心于 2017 年开展“中国信息安全从业人员现状”调研活动，重点评估我国信息安全从业人员的基本构成和分布、人才供需和结构、能力提升方向和途径、职业发展路径以及职业满意度等情况，着重分析从业人员整体态势并同发达国家进行对照。此次调研覆盖了全国各地区、各行业的信息安全从业人员，具有一定的代表性。通过梳理此次调研数据和专家研讨结果，当前我国网络安全人才队伍建设工作中需要重点解决以下几个问题。

一、我国网络安全人才队伍建设中的难点问题

1. 供需严重失衡

信息安全人才需求迅速增长，人才供应的速度赶不上人才需求增长的速度，这是世界各国普遍面临的急迫问题。我国作为后起国家，网络安全人才短缺情况尤其严重。但要精确地评估人才缺口数量是非常困难的，目前普遍认为这个缺口量级至少在百万级。我们也可以通过薪酬水平，从侧面了解信息安全从业人员的供需情况。人才的薪酬待遇水平是由劳动力市场中的供需关系决定的，根据《中国信息安全从业人员现状调研报告（2017 年度）》（以下简称调研报告），国内信息安全从业人员平均薪资水平在 12.2–17.8 万元之间，大幅超出国家专业技术人员的年平均工资 76325 元，也高于信息技术从业人员的年平均工资 120864 元。信息安全从业人员基本属于“卖方市场”，尤其是优秀的信息安全人才受到抢夺，推高了信息安全从业人员的整体薪酬水平。国际上的情况也是如此，信息安全从业人员的薪酬比信息技术从业人员大约高出 9 个百分点。

信息安全从业人员的供需矛盾不仅仅体现在从业人员绝对数量的不足上，更体现在不同类型人才供给和需求之间的错位。当前的信息安全从业人员中从事运营与维护、技术支持、管理、风险评估与测试的人员相对较多，战略规划、架构设计、信息安全法律相关从业人员相对较少；各类人才均存在缺口的前提下，战略规划（49.2%）和架构设计（46.8%）岗位人才的短缺情况最为突出，运营维护（16.1%）和技术支持（14.5%）岗位人才短缺情况相对比较缓和。人才队伍呈现底部过大，顶部过小的结构，“重产品，轻服务，重技术，轻管理”的现象仍很普遍。人的作用没有得到有效发挥，尤其缺乏技术和管理能力兼备的“将才”。42.8% 的信息安全从业人员认为关键信息基础设施运营单位有必要设置专职的信息安全管理岗位，如首席信息安全官（CISO），54.2% 认为所有单位都需要设立这样的岗位。

2. 教育培训不足

信息安全是技术更新迭代最快的行业之一，信息安全从业人员需要不断更新知识储备，学习掌握新的技能，跟进前沿信息安全态势。可以说，持续教育是贯穿信息安全从业人员职业生涯不变的主题。在各项专业技能中，信息安全从业人员最希望提升的技能方向是网络攻防（70.7%），其次分别是安全管理（50.6%）、安全架构（47.1%），以及安全审计（44.8%）。在信息安全领先国家，用人单位能否为员工支付教育培训和资质认定的费用已成为招聘和留住安全人才的重要因素之一。

从人才队伍的入口来看，信息安全从业人员的来源一是各类院校，二是 IT 人员乃至非科班的人员转化而来。加强网络安全从业人员队伍建设，需要学历教育、职业培训、用人单位内训等多种方式共同发力。但当前的现状是，学历教育需要经过大约 4 年的人才培养周期，每年仅能输出 1.5 万名毕业生，而且目前还存在着偏重理论、实践门槛高、与产业脱节等问题，短期之内无法满足各界对网络安全人才的需要。职业培训周期短、针对性强、紧跟业界前沿趋势，是从业人员和准从业人员理想的能力提升方式。然而不少用人单位疏于培养自有人才，不愿投入足够的资源开展内训或进行专业培训。从业人员在所属单位能够得到定期、有计划目标培训的人群仅占 22.8%。国外调研结果显示，44% 的受访者能得到恰当程度的培训，但仍被认为有待加强。

3. 人才评价手段有限

调研报告显示，25.9% 的从业人员在技术职称序列上没有清晰的归属。信息安全从业人员基于兴趣爱好等内在驱动因素进入行业，之后发生职业流动则主要是受薪酬和晋升空间因素影响。优秀人才流失严重，根源在于网络安全作为一个职业来说缺乏能够有效“衡量人才的尺子”，导致人员责、权、利难以对等实现。人员能力的提升难以在所在单位得到认可，一方面是用人单位留住人才越来越困难，另一方面是优秀的人才在资本的驱动下，在职业流动中寻求人才升值的体现。网络安全缺乏考核从业人员专业能力的评价指标体系，就无法形成一个能够囊括全频谱类别角色、覆盖完整职业生命周期，且为业界普遍认可的职业发展路线图。

国内出现实质上的信息安全从业人员只有二十余年的历史，作为一个相对年轻、新兴的职业，网络安全还没有被收录入国家职业资格大典。信息安全从业人员的职称评审多依附于信息技术等类别之下，大量政府部门、事业单位，以及关键信息基础设施运营单位信息安全从业人员在评审职称或进行其他评价时存在困难，特别是寻求向高级别、专家型人才进阶时常常无路可循。而企业中即使设立了相应的人才评价标准和级别，也往往是各行其是、互不兼容。这样的状况既不利于国家对信息安全人才队伍建设的整体规划和引导，也不利于从业人员依照职业路线图寻求职业发展。

二、关于网络安全人才队伍建设难点问题的思考

网络安全人才事业已迎来最好的发展机遇，人才队伍建设工作多点发力，成效初现。中国信息安全测评中心承担信息安全人员资质测评的重要职责，十五年来通过注册信息安全专业人员（CISP）培训体系为党政军、重要行业、关键信息基础设施培养了数万名信息安全专业骨干人才。在当前网络安全人才发展的关键历史时期，我们将担当起时代使命，继续投身网安人才培养实践和探索性工作。

1. 加强主力建设，从业人员和储备人员的教育培训是关键

落实国家网络安全人才战略，需要综合提升各类人群的网络安全意识和能力，包括各级领导干部、关键信息基础设施运营者、安全从业人员、高校和中小学学生，以及普通公众等。其中尤为关键的是信息安全从业人员以及准备进入行业的储备人员，因为他们是实施各项网络安全保障措施的主力

军，也是有望在网络安全核心技术取得突破的先锋力量。对于从业人员，要满足他们在网络安全细分领域和前沿领域能力提升的需要。CISP 职业培训体系及时掌握人员培训需求，2018 年知识体系已全面升级，细分领域培训全线铺开，完整覆盖渗透测试、安全审计、安全开发、工控安全，及互联网等人才紧缺的方向，成为我国重要行业、关键信息基础设施运营单位以及大中型企业首先的人员培训品牌。对于网络安全相关专业的学生，要创新人才培养模式，解决传统教育与产业脱节的痛点问题。由测评中心主办的信息安全铁人三项赛打造常态化的训练营，把网安对抗融入教学各个环节，以比赛驱动学习和提升，为探索产教融合的网络安全教育改革提供了有重要参考价值的范本。学历教育和职业培训双管齐下，通过规模化培养解决最为突出的信息安全人才供需矛盾，通过专业化培养填补信息安全细分领域人才缺口。

2. 做好人才量尺，研究编制人才评价标准至关重要

同传统行业不同，信息安全的历史不长，本身又具有更新快、跨领域、碎片化的特点，从业人员评价手段不足导致的问题已日益凸显。要落实国家网络安全战略，做好人才的“选、育、用、留”，加强队伍稳定性，必须尽快研究制定从业人员评价标准，完善人才评价手段。目前人才评价最大的难点在于，传统的人才评价方式不完全适用于网络安全从业人员，尤其不适用于掌握特殊技能的人才。习总书记指出，对于特殊的网络安全人才“不要都用一把尺子衡量”。国外的做法更倾向于使用人员资质的方式，如美国国防部所有信息安全保障岗位都需要达到相应的人员基线资质要求。我国的 CISP 注册资质证书也已成为信息安全领域人才识别和能力评价的重要依据，以及不少单位招聘时的必备要求。如何编制更全面、更系统，能够满足全社会需要的网络安全从业人员评价指标体系是我们下一步的重点工作任务。

3. 强化统筹协调，统一推进确保工作成效

网络安全人才培养是一项战略性、基础性、范围广、领域多的工作，需要提前谋篇布局，需要政产学研用多方力量参与。要加强主管领导部门的统筹协调职责，强化各职能部门的工作权限和职责范围，动员全社会相关企业、行业组织和院校协作配合，共同建立适应网络安全人才特点的队伍建设工作体系。可以参考网络安全先进国家的做法，如美国于 2008 年谋划、2010 年开始实施的“国家网络安全教育计划（NICE）”，在全美范围内掀起一场网络安全教育革命。NICE 计划下设工作组和跨部门协调委员会，能够协调国防部、国土安全部、教育部、商务部、人事管理办公室等十几个政府部门和大量产业界、学术界组织。英国也将制定专门的网络安全技能战略，不仅要将网络安全纳入教育体系，还准备建立由政府、用人单位、专业团体、技能团体、教育机构和学术界组成的技能咨询组织。

三、结语

我国网络安全人才队伍现状最大的特点就是发展不充分、不平衡。当前国内网络安全市场规模仅为三、四百亿元，但黑色灰色产业已达千亿元规模。安全投入明显不足，安全责任不到位，包括人才在内的网络安全市场需求尚未得到有效释放。过去一年里，层出不穷的信息泄露、勒索病毒、DDoS，以及工控安全事件促使政府和各企事业单位不得不重视、应对网络安全风险，网络安全人才成为各单位生存和发展的刚需型人才。随着《网络安全法》、《关键信息基础设施安全保护条例》的出台，网络安全相关需求已成为法律强制要求。网络安全人才不到位，就无法满足相关法规实施提出的要求。在业务刚需和法律强制要求的牵引下，对网络安全从业人员的需求将出现跨越式增长。剖析人才工作难点，把握网络安全特点，找准着力点，探索创新点，加快网络安全人才队伍建设时不我待。