专栏

为网络安全职业发展保驾护航

技能差距

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Cq2x23

虚位以待！急需数百万的安全专业人士来填补关键职位，保护世界上的基础设施、数据和人员 — 立即申请吧！

虽然对安全专业人士的需求量巨大，但问题在于没有足够的合格员工来填补企业所需职位。如需确认核实，请查看信息系统审计与控制协会 (ISACA) 发布的报告*《2018 年网络安全局势》*。[1] 该报告第 1 部分概述了安全领域的人力资源情况，并提到 59% 的受访者都表示仍有安全职位空缺。多年以来代价高昂的安全事件和安全漏洞让首席执行官们 (CEO) 对安全威胁忧心忡忡。普华永道 2018 年的报告*《让首席执行官们夜不能寐的威胁因地区而异》*[2] 强调，高管们十分担心网络安全威胁 — 这一问题在 2017 年排名第 10，但在 2018 年就跃升至了第 4 位。网络安全现在已成为高管们的一个头等话题，也成为董事会密切关注的话题。

虽然企业对安全问题的担忧似乎没有尽头，但是无法保证员工将拥有永久的工作保障，也无法保证员工的工作不会受到破坏人力资本的行业变化的影响。因为技术和自动化将是安全领域领导人追赶对手的重中之重，所以安全专业人士需要发展和提升自身到更高的职位，好为自己的工作保驾护航。

无论是不是安全领域的新手，也无论有没有一定的经验，应征者绝对不能不思进取，而是应该不断地获取雇主所寻求的职业技能。

技术技能 — 积极主动、学习新事物

安全从业者会有很多学习新技能的机会，并且大多数成本很低，甚至不需花费一分钱。雇主可能会分配一些预算来发展新技能，但是无论如何，从业者必须自我投资，不要指望雇主的投入。技术发展太快，没时间让人坐下来舒服一会。

员工应广泛涉猎，至少要了解新技术的基础知识。多年前，建立一个实验室所需的硬件和许可证耗资不菲。如今，以极低的成本在云端构建实验室的机会多如牛毛。这是构建、打破、重构、然后与他人分享经验的一种绝妙的方式。这是一个精彩的故事。在技术面试中或者作为一名有经验的雇员，谈谈您对这一点的理解将大有裨益，可向潜在团队展现您言行一致的能力。在许多情况下，这可能足以助您获取下一个内部或外部职位。

Mike Saurbaugh，CRISC、CISM、CISSP、MSIA
担任企业客户的技术联盟主管，负责业务开发解决方案集成。在此之前，他在金融服务业从事网络安全和技术工作近二十载，并且担任网络安全负责人一职已有 12 年。Saurbaugh 是 IANS Research 的员工，为列名财富杂志 (Fortune) 的客户提供网络安全方面的战略建议。Saurbaugh 自 Security Current 创办起便参与其中，担任研究总监一职，领导了许多针对全球安全供应商和首席信息安全官 (CISO) 的战略项目。Saurbaugh 还是 MACH37 和 Queen City Fintech 网络安全加速器项目的导师，并且他拥有一家安全咨询公司，开展独立咨询和风险评估工作。Saurbaugh 曾在各种高等教育课程咨询委员会中任职。

尽管新技术层出不穷，但是从短期来说，很少有新技术能脱颖而出。以下是一些成长的领域，从业者可以并且应该花一些时间来帮助自身确定优势地位，获取下一个职位：

- Python
- PowerShell
- Amazon Web Services (AWS)
- Microsoft Azure
- Docker
- 分析和事故响应
- 应用安全
- Kubernetes
- 威胁情报
- 威胁狩猎
- 取证
- 恶意软件分析
- 渗透测试
- 数据科学基础

> “从业者的好奇心和尝试新事物的兴趣，尤其是在安全领域，应该是种期望和雇主寻求的品质。”

开始学习一门知识后，或许很快就会发现这不是正确的路径。即便很快就失败了也没什么大不了。从业者的好奇心和尝试新事物的兴趣，尤其是在安全领域，应该是种期望和雇主寻求的品质。若是对某项技术提不起兴趣或者难以掌握它的基础知识，那也没有关系。重要的是继续前进并尝试其他的东西而不是舒服地待着不动。

Coursera[3]、edX[4]、LinkedIn[5]、Udacity[6] 和 Udemy[7] 等提供各种免费或低价的技术课程。此外，微软提供 Azure[8] 培训，亚马逊提供 AWS[9] 培训。

最终，技术技能很有可能为求职者赢得工作机会。这可能很难，对于那些一步步晋升到管理层的经验丰富的求职者而言尤为如此。也正因为如此，不用从事日常基础工作的管理者们更应该竭尽所能地保持技能更新。

软技能很重要

反之，经验较少但渴望更高职位的员工应该专注于能让他们脱颖而出的特质。软技能确实很重要。在安全和技术领域，软技能常被忽视。

软技能是支持我们与他人互动的个人特质。它与技术工作以及长时间面对屏幕和键盘进行双向通信的计算机工作所带来的独处有很大不同。

众所周知，企业依赖技术，这使得网络安全成为注重系统和数据保护的企业所关注的重点领域。拥有软技能，才能获得企业的认同。许多技术人员擅长实现系统安全、正常运行时间和功能等所要求的技术，但可能不具备必要的软技能。

哪些软技能和个人特质能够给职业发展带来积极影响呢？许多答案众所周知，但给予的关注确远远不够：

- 沟通（书面、口头）
- 团队导向
- 组织
- 项目管理技能
- 服务导向
- 理解商务相关的财务
- 商业头脑
- 情商

Enjoying this article?

- Read *State of Cybersecurity 2018–Part 1: Workforce Development* *www.isaca.org/state-of-cybersecurity-2018*

- 同理心
- 倾听
- 个性
- 谈判

软技能也能转化为专业水平。换句话说，职业发展往往取决于专业方面的成长和摈弃拖人后腿的坏习惯。成为一个他人愿意共事的人也是一大职业优势。技能可以培训，但是让员工摆脱错误的态度的确是一个完全不同的挑战，也是多数管理者不愿意长期斡旋的一个挑战。在信息安全领域这一点不言而喻。更全面地说，真实、诚恳和高度诚信在这一领域至关重要。

职业网络的重要性

建立强大的职业网络至关重要。那些与行业中的其他人长时间隔离的员工可能会发现，当他们想要做出改变时，已经很难融入另一个组织。这并不是说对组织的忠诚和奉献是一件坏事，而是说我们必须要花时间社交。

有些人很能看清这一点，因此能够很好地建立一个强大的职业网络。但令人惊讶的是，有些人很容易停留在他们的舒适区，不愿与他人交往。问题在于，当这些人在寻求新职位时，他们可能很难获得自己满意的职位。许多职位并不对外发布，并且有时候在职位发布之前，同行就已经知道了这些新出现的机会。那些有关系的人更有可能抢占先机来证明自身是最佳人选。

显然，社交网络是一个入门的好地方。专业人士不一定是 Twitter 或 LinkedIn 达人，但建议他们一定要取得某种存在感（至少在 LinkedIn 上）。此外，会议是结识新朋友、建立新关系的好地方。这样做对于那些不热衷社交的人来说可能会感到不自在，但是一步步地开始建立关系网络非常有必要。不花钱或只花一点钱参加会议，结识本地的新朋友没有丝毫坏处。现在，许多全球性活动都可网上参加。[10]

会议需要发言人。征文 (CFP) 投稿不失为一个选择。在会议上发言是提高个人魅力的一个好方法。做得好，将为您成为特定学科的领导者奠定基石。但是，发言者必须要小心应对，因为安全行业人员会仔细审查您的发言内容，因此发言人需要做好充分准备，提供内容丰富的演示文稿。

花点时间帮助他人

学有所长的人应该分享自己的知识。这对职业发展有什么用呢？首先，它有助于提升个人魅力和获取行业认可。此外，它还帮助技术和非技术人员对该主题获得教育。这在会议讨论和个人博客文章中是常见的现象。当从业者和管理者在日常活动中分享自己所学（无论好坏）时，必将促进安全行业蓬勃发展。

将安全知识传达给技术受众无疑令之受益，但对于非技术人员呢？在办公室工作和社交媒体方面，拥有智能手机和/或计算机的普通人所用的大多数应用程序与世界上其他人所用的并无不同。花一些时间，自愿帮助非技术人员了解如何更好地保护他们的数据和系统，大大有助于扩大一个人的技术贡献。它还有助于从业者提高沟通技巧。外行或门外汉对缩略语可以说是一无所知。这是一个提高沟通技巧、让他人理解自己的观点的磨练机会。

开展这项活动有助于我们与现在或未来潜在的雇主进行对话。这糅合了许多雇主寻求的有益特征：技术实力、软技能、对专业的贡献和主动性等等，不一而足。此外，员工积极参加志愿者项目、做出专业贡献并帮助提高相关人员的知识、技能和能力的情况并不少见。

对于更有经验的专业人士而言，辅导级别较低的员工也是一项十分有益的体验。当然，很多此类辅导都是在组织内部进行的，但这并不表示不能在企业之外开展此类活动。如果有人主动且诚恳地表示非常想要向您学习经验，这就是您伸出援助之手的好时机。与此同时，辅导不应过度消耗您的精力，因此时间管理和分配十分重要。

其他方案和资源

行业从业者多年以来一直孜孜不倦地热衷考证，现在情况也是如此。通常，证书的价值因企业招聘而异。如果组织需要证书，那么持有一个或多个证书是很有价值的。有些组织不看重证书，它们更看重的是应征者的工作技能，而不是求职简历上罗列的证书。但是，一般而言，有证还是有好处的。

对于该领域的新员工来说，证书当然值得他们研究和考取。CompTIA、ISACA®、(ISC)² 和 SANS 的证书以及供应商特定认证可以在一定程度上向雇主表明应聘者的水平。此外，这也适用于有经验的员工，可以表明他们对这个领域和职业的奉献。毕竟，除非雇主要求应聘者提供证书，否则很多人都是主动考证的，这也表明了一个人对其职业生涯的奉献和激情。

无论员工职业发展关注的重点是什么，StrengthsFinder 都是一项重要的个人发展资源[11]，它可以帮助员工发现自身的优点，警示自身的缺点。其理念在于不断积累优势、取得更大成功。很多时候，我们关注的是弱点，这可能会拖累我们。然而，我们越是利用优势，表现就越出色，并且越快乐。

那些想要时刻了解本行业人才市场动向的人应好好利用 CyberSeek[12]，它可向雇主、员工、教育工作者和学生提供职业发展信息。

由美国国家标准与技术研究所 (NIST) 提供的国家网络安全教育计划 (NICE)[13] 侧重于教育、培训和人力资源发展。该计划所依据的框架[14] 概述了各个角色执行任务所需的知识、技能和能力。

总结

职业发展是“种瓜得瓜，种豆得豆”。它没有任何保证。持续发展自身能力而不是坐等好运降临，才是符合最佳利益的做法。安全领域需要背景各异、经历不同的各种人士。如前所述，技术技能往往最受关注，但社会需要全面发展的人才。面临选择的时候，掌握更多的安全技术知识始终为上策，同时尽可能抽出时间提高软技能。人才市场看似在很长一段时间内大有前景，但不太可能永盛不衰。付出额外的努力学习新技术、提升软技能、建立专业网络，在这个过程中您会得到诸如“您被录用了！”一类的回馈。

> “安全领域需要背景各异、经历不同的各种人士。”

尾注

1 ISACA®，*2018 年网络安全局势*，*https://cybersecurity.isaca.org/state-of-cybersecurity*
2 普华永道，*让首席执行官们夜不能寐的威胁因地区而异*，2018 年，*www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx/business-threats.html*
3 Coursera, *www.coursera.org/*
4 edX, *www.edx.org/*
5 LinkedIn, *www.linkedin.com/*
6 Udacity, *www.udacity.com/*
7 Udemy, *www.udemy.com/*
8 微软，“从微软获得云技术一手经验”，*https://www.microsoft.com/handsonlabs*
9 AWS，“欢迎加入 AWS 培训和认证”，*https://aws.amazon.com/training/*
10 InfoSec Conferences，“2018 年官方网络安全会议目录”，*https://infosec-conferences.com/*
11 Rath, T.，*发现您的克里夫顿优势*，盖洛普出版社，美国，2007 年
12 Cyber Seek, *www.cyberseek.org/*
13 美国国家标准与技术研究所，“国家网络安全教育计划 (NICE)”，美国，*https://www.nist.gov/itl/applied-cybersecurity/nice*
14 美国国家标准与技术研究所，“NICE 网络安全劳动力框架”，美国，*https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*