9个特质

(ISC)²

网络安全领导者需具备的9个特质

网络安全是企业繁荣的重要因素

现在世界上超过50%的人口都在上网[1]。每天约有100万人加入互联网[2]，而三分之二的人类拥有移动设备[3]。人们熟知的第四次工业革命(4IR)，已经给世界带来了巨大的经济和社会效益。

智能技术在改善人类生活和地球健康方面都有巨大的潜力。然而，许多新的挑战和风险也逐渐浮现。网络攻击已经成为个人和企业的共同危害。第五代(5G)网络、量子计算和人工智能不仅创造了机遇，也带来了新的威胁。

对强大的网络安全的需求显而易见：每14秒[4]就会有一个组织成为勒索软件攻击的受害者 ，而一次成功的攻击可能会迫使企业完全停滞数周，甚至完全关闭。

组织不应该将网络安全仅仅视为防范迫在眉睫的网络安全威胁的另一项IT支出。事实上，网络安全对推动企业发展也能起到至关重要的作用[5]。

图1：长期风险展望。未来10年按可能性和影响分列的十大风险[6]

拥有更强大网络安全战略的组织比那些没有网络安全战略的组织有更强大的竞争优势。随着网络攻击和安全漏洞经常成为新闻头条，消费者对数字服务和产品的安全及隐私变得更加敏锐，无论这些服务和产品是由大企业还是小企业提供。根据沃达丰[7]最近的研究显示，89%的高管们相信，改善企业的网络安全将增强客户的忠诚度和信任度。

然而，各公司仍在努力使网络安全成为与其战略、运营和文化相融和、积极的一部分。尽管网络安全专业人员负责保障企业的安全，但当企业做出重大的战略决策时，网络安全往往是事后的考虑，导致安全和业务风险增加。这意味着企业正在失去网络安全功能所能提供的附加价值。

企业现在需要的是有才华、有经验、有知识的员工，他们既懂得新兴技术的潜力，也明白与之相关的风险。随着技术越来越多地融入到业务流程中，这些专家可以引领企业迎接时代挑战，使网络安全意识和安全成为企业成功的助推器。

成为一名优秀的网络安全专家所需要的技能

企业对人才的需求，对于像您这样的网络安全专业人员来说，是一个很好的机会。但是，未来的安全领导者需要广泛的技能，单凭工作经验并不足以胜任。您需要投入培训来掌握这些技能，以打下坚实的基础，增强自信，并在组织中产生影响力。学习可以让您获得成为真正的领导者所需的技术和软技能。

技术技能组合

对新兴技术的深入了解

新兴技术改变了企业的工作方式，也将在未来创造新的角色。物联网、人工智能、机器学习(ML)、云计算和自动化都被视为支持数字化转型的重要投资。新的安全职位将要求专业人员了解这些新兴技术及其固有的安全挑战。

敏锐的安全专业人员应该今天就掌握这些知识，因为这些新兴技术明天将使工作场所发生变化。如果不了解这种技术是如何影响IT基础设施和业务发展的，一些人可能会发现，随着角色,包括与新兴技术相关的技能的发展，他们会被抛在后面。

对安全最佳实践的深刻认识

网络安全已经成为当今企业的头等大事。安全专业人员的需求量很大，而技能的差距使我们很难找到降低风险所需的帮助。网络安全专业人员必须能够展示出对安全最佳实践的充分了解， 包括：

- 事件检测和响应，以处理组织违反安全政策或标准安全做法所造 成的任何紧迫的威胁。
- SIEM管理，将警报产生的实时分析转化为事件响应计划。
- 分析和威胁情报，以汇总网络和应用数据，防止未来发生攻击。
- 身份和访问管理，以确保安全政策对组织内各种角色和责任显示出可接受的用法。
- 数据管理，以处理、分析、安全地存储各类数据，无论是在内部还是在云端。

全面了解监管环境

GDPR、CCPA、HIPAA、SOX、PIPEDA等法规规定了保护敏感数据和个人数据安全和隐私的要求。如果不遵守这些条例，将受到有关国家监督当局的严厉处罚。这些处罚不仅会影响企业预算，还会损害人们对受影响组织的信任程度。

合规是一个持续的过程，而不是一次性的工作。网络安全专业人员需要了解这些条例中所述的安全要求，并尽职尽责地实施适当的安全控制。遵守这些规定可以提供竞争优势，对每个组织来说都是一种附加值。

软技能

领导力和沟通

安全专家通过他们的信誉、响应能力和道德操守来展示领导力。此外，沟通技巧可以帮助安全专家赢得高级管理层、同行和下属的信任。安全专业人员应能向领导层提供与业务需求和风险环境相联系的可操作的见解，帮助管理人员做出明智的决定。

对学习的热情

安全专家应不断学习业务环境中的最新趋势、技术和安全挑战。他们必须对学习和专业成长充满热情，才能获得成功。安全是IT行业中节奏最快的领域之一，需要有求知欲和专业知识的人。

决心

网络安全专业人员必须坚持不懈地应对不断变化的威胁环境。坚持是关键。网络安全专家要将解决方案贯穿始终，不解决难题不罢休。

协作

网络安全是整个组织的共同责任。因此，安全专业人员必须在各级相互协作，灌输一种文化，确保安全政策不仅到位，而且要得到遵守。同样重要的是，要获得整个组织对安全倡议的支持。

分析和批判性思维

一个专业的网络安全专家会对事件的发生方式、容易被利用的攻击面以及如何将网络攻击降到最低进行分析。一个有分析力和洞察力的安全专家会预测黑客将如何利用网络及其应用。在某种程度上，网络安全专家应该像攻击者一样思考，提前发现漏洞。

项目管理

最后，作为一名网络安全专家，你需要整合全面的安全解决方案，以防止、检测和应对网络攻击。与其将实施解决方案视为"一劳永逸"，不如从更全面的角度考虑，建立一个与企业所有资源相一致的安全策略。

网络挑战使企业面临风险

威胁格局正在变化和扩大

企业正在数字化，以期提高生产力的同时将总体成本降至最低，并加强员工之间以及与合作伙伴或供应商之间的协作。数字化背后的理念是，不仅要利用技术将现有的服务以数字化的形式复制出来，还要利用技术将这种服务转化为更好的东西。

数据是所有数字化工作的核心。这些数据（通常是个人和敏感数据）的处理和存储方式由众多具有深远影响的隐私法规决定，如GDPR和CCPA。然而，高调的数据泄露事件成为新闻头条，政府行为者滥用个人数据，增加了人们对现行处理和存储敏感数据的政策和战略的不信任感。

伴随着隐私问题的增加，数字化转型的举措扩大了业务威胁的范围，因为通常情况下，安全是事后的考虑。在一个超级互联的世界里，问题不在于企业是否被入侵，而在于何时会遇到安全事故。事实上，2019年被网络攻击影响的组织比例达到了80.7%，高于2018年的78.0%[8]，而两年内遭遇数据泄露的比率从2014年的22.6%上升到2019年的29.6%[9]。

虽然这些新兴技术创造了惊人的新的组织能力，但也造成了新的复杂问题、互联和漏洞点，网络犯罪分子已经很快学会了利用这些漏洞。传统的周边安全和基于规则的网络安全方法不再适用于新的数字组织，因为用户现在正在以远程形式访问组织最敏感的资源，而且超出了传统的边界安全范围。

个人数据、证书是主要攻击目标

现在身份是新的边界安全。企业需要对访问企业数据的用户或设备进行迅速高效的认证，无论这些数据是储存在本地还是云端。数字身份对所有组织来说都是宝贵的资产，但它们也是网络犯罪分子有利可图的目标。犯罪分子喜欢用简单的方式完成工作，这也解释了为什么他们会使用和滥用偷来的凭证。黑客攻击和社交漏洞等攻击类型受益于凭证失窃，这样就不再需要使用恶意软件来保持持久性。因此，账户接管和凭证滥用攻击使其成为各组织最关注的前五大网络威胁[10]。

同时，个人数据被盗刷的情况也比往年更多。2019年58%的泄露事件涉及个人数据，是2018年30%的近两倍[11]。这包括电子邮件地址、姓名、电话号码、物理地址和其他类型的数据，人们可能会发现这些数据隐藏在电子邮件或存储在错误配置的数据库中。一旦掌握了这些珍贵的数据，犯罪分子就会在股价极高的暗网上出售，或者利用这些数据发动其他攻击，比如网络钓鱼。

钓鱼攻击是攻击者在企业网络中获得存在感的第一步。

大多数安全报告都认为，网络钓鱼是安全漏洞中出现的第一个初始感染载体[12]。钓鱼是社会工程攻击最喜欢的行动路线，在96%的场合下通过电子邮件到达。虽然凭证是目前网络钓鱼漏洞中最常见的泄露属性，但个人数据也受到追捧[13]。

对攻击者来说，网络钓鱼一直是而且仍然是一种卓有成效的方法。这也是为什么它是企业最关注的网络威胁[14]。令人担忧的是，越来越多的攻击者通过商务电子邮件妥协(BEC)使用网络钓鱼策略，也就是所谓的CEO欺诈，加剧了这种担忧。这种攻击是出于经济动机，并且已经被证明是非常有效的：受影响的公司每次损失高达44,000美元[15]。

云计算安全问题备受关注

将企业数据转移到云端是企业进行数字化转型的一部分。随着公司向云端转移，犯罪分子也是。2019年约有24%的泄露事件涉及云资产，73%的情况下涉及电子邮件或Web应用服务器。此外，77%的云端泄露事件还涉及凭证违规[16]。这与其说是对云安全的控诉，不如说是说明了网络犯罪分子寻找最快捷、最简单的途径来对付受害者的趋势。

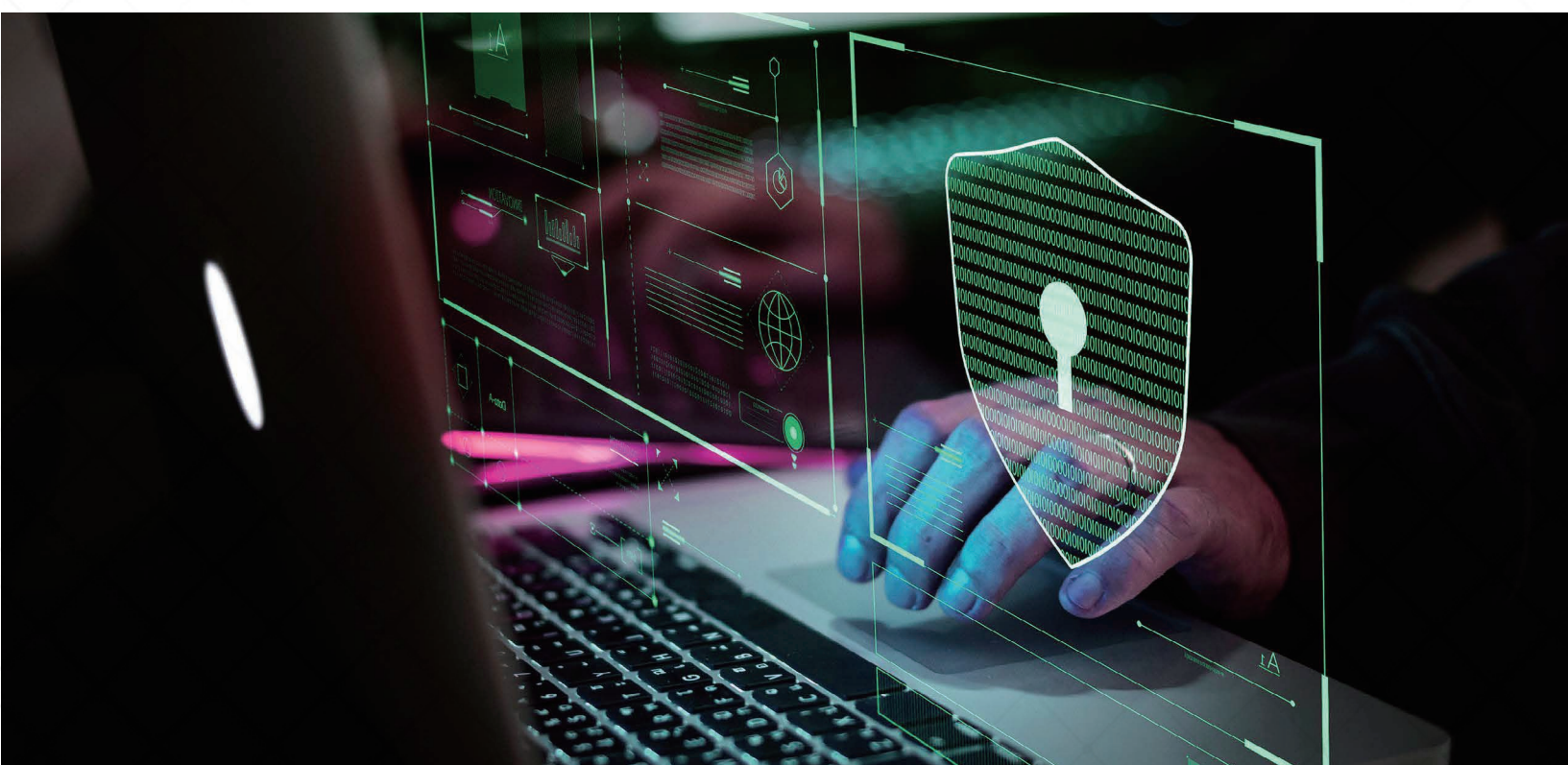
这些统计数字使人们对云资产的安全态势信心下降[17]。事实上，在850万条被泄露的数据记录中，有86%的数据记录是由于服务器配置错误造成的，要么是面向公众的云资产，要么是云中未加密的数据[18]。这些组织未能理解云提供商的共同责任模式，在这种模型中，云数据的安全是所有者的绝对责任。

工业攻击正在增加

攻击者并不仅仅出于财务目的而关注企业。他们还急于破坏国家关键基础设施的可用性和可靠性以造成严重破坏。与2018年相比，2019年威胁行为者针对工业控制系统(ICS)和类似运营技术(OT)资产的事件增加了2000%以上[19]。大多数观察到的攻击都围绕着使用SCADA和ICS硬件组件内的已知漏洞组合。

还有很多情况，攻击者利用了IT和OT基础设施的融合。这种重叠使得IT漏洞可以针对控制物理资产的OT设备，从而大大增加恢复成本。各行业对物联网设备的爆炸性使用扩大了攻击面，威胁行为者利用了这一点。具有网络接入的受损设备可以被攻击者用作潜在的枢纽点，试图在组织中建立立足点。

减轻当今的网络威胁风险，需要的不仅是投资于正确的技术。你必须确保这些技术得到最佳的部署、正确地配置和充分地监控，使你的组织尽力避免成为头版新闻。一个经验丰富、受过良好教育的网络安全专业人员可以将所有的拼图组合在一起，帮助任何组织建立一个强大的安全态势。



成功的网络安全专家的9个特点

网络安全专家要确保将网络风险管控在可接受的水平，从而支持其组织的任务。由于没有任何企业能够免受网络威胁，因此当发生泄露事件时，企业需要做好准备。每个组织的最终目标都应该是弹性力，即识别和最大限度地减少事件影响的能力，以便尽可能有效地保持业务连续性。

根据世界经济论坛报告《数字世界领导者网络安全指南》[20]"，网络安全专业人员应坚持"基本"信条："一个组织必须执行这些信条，才能将网络安全嵌入企业DNA，并作为全面网络安全计划的一部分，对网络弹性进行尽职调查。"

1. **像企业领导者一样思考**，将网络安全从一个支持功能转变为提升企业声誉、收入、品牌资产和客户关系的业务推动者。领导力的一部分是促进内部和外部的合作伙伴关系，确保始终满足业务需求，同时以更有效的方式管理相关的网络风险。

2. **建立和实践强有力的网络卫生**，因为有效和持续地实施强有力的网络卫生可能会降低过去十年中大多数的网络攻击。

3. 根据"最低特权"原则保**护对任务关键资产的访问**，同时，建立强大的身份和访问管理系统。

4. **保护电子邮件，防止网络钓鱼**。电子邮件是最有价值、使用最广泛的企业通信手段之一，但是根据Verizon的DBIR 2020报告[20]，它是最常见的网络攻击载体。

5. **采用零信任的方法来确保供应链安全**，不要以为公司可以在其"安全"的企业网络周边内安然无恙。无边界零信任的方法将控制权置于数据资产周围，并提高了数据资产在整个数字商业生态系统中使用的可视性。

6. 通过根据组织的业务环境制定一个强而有力的基于风险的方法，**预防、监控和应对新出现的网络威胁**。所实施的安全服务必须符合目的，并适合组织在人员、流程和技术方面的需求。

7. **制定和实施全面的危机管理计划**。在当今世界，危机管理是任何安全计划的重要组成部分。及时沟通安全事件，与透明化、简单化一样重要，才能与客户形成稳固的信任关系。

8. **建立一个强大的、量身定制的灾难恢复计划**，以保护组织免受潜在的网络攻击，并指导如何应对数据泄露的情况，同时减少识别泄露和恢复关键服务所需的时间。

9. **倡导网络安全文化**，将用户置于第一道防线，并认可所有员工在组织安全中的关键作用。保证组织的安全是每个员工的责任。

CISSP如何帮助您为实时事故做好准备？

应聘网络安全专业职位时，您需要证明自己就是他们正在寻找的领导者。安全认证就是您专业技能和知识的证明。

在市场上所有的认证中，(ISC)²的注册信息系统安全专家(CISSP)认证可以为您提供有效执行这些任务所需的知识，并将您的知识与业务需求联系起来。CISSP可以帮助您成为下一代网络安全领导者。

CISSP通用知识体系(CBK)提供了跨学科的信息安全意识，涵盖了以下八个知识域：

安全和风险管理

需要对信息安全的基本安全概念和原则有良好的了解，才能履行安全和风险管理的职能，包括制定和执行政策，支持治理，并在发生网络安全事件时确保业务连续性。

资产安全

对必须保护的内容、应该限制的访问权限、可用的控制机制以及这些机制可能怎样被滥用等问题有可见性和扎实的理解，这是所有安全控制的基础。专业人员应该能够针对这些信息资产运用保密性、完整性、可用性和隐私性的原则。

安全架构和工程

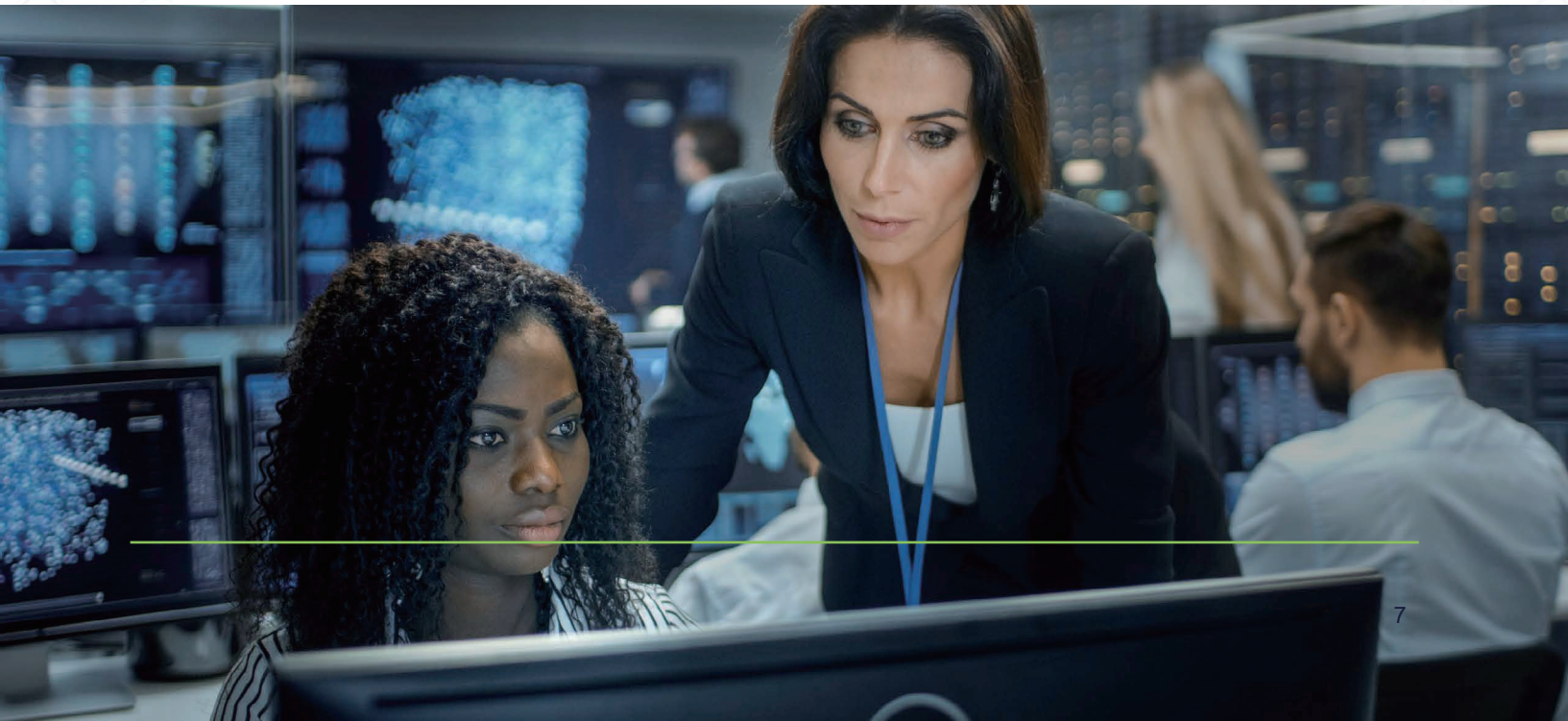
必须要在系统生命周期的设计、实施和持续交付中考虑安全问题。设计和建立一个安全和有弹性的信息系统架构，可以尽力减少恶意行为者、人为错误或系统故障所造成的威胁。最重要的是要了解安全设计原则，并能将安全模型应用于各种分布式和不同的系统，并保护承载这些系统的设施。

通信和网络安全

作为一个安全领导者，您应该能够理解安全网络的组成部分、安全设计以及安全网络运行的模式。此外，您还应该了解分层防御、安全网络技术和管理技术，以防止一些网络拓扑和融合网络中的威胁。

身份和访问管理

身份和访问管理(IAM)是管理数字身份的机制，专业人员应了解管理这些身份的政策和流程，以及支持身份管理所需的技术和协议。



安全评估和测试

涉及安全评估和测试的活动，以持续验证安全控制正在最佳地、有效地执行，以保护信息资产。漏洞评估和渗透测试是网络安全专业人员进行安全评估活动的一部分。

安全运营

安全运营应在任何集中或分布式的环境中运行，以保护和控制信息处理资产，并执行确保安全服务可靠和有效运行所需的日常任务。安全运营包括监控安全、执行事件响应、实施灾难恢复策略、管理物理安全和人员安全的活动。

软件开发安全

应用和数据是信息系统的基础。了解围绕软件的控制、其开发生命周期以及系统和应用程序中固有的漏洞，对于确保软件可靠和安全的开发和维护至关重要。

广泛安全知识的重要性

一个拥有广泛安全知识的专业技术人员可以成为组织最宝贵的资产。对安全事件有了更广泛的了解，安全从业人员就可以根据不断变化的威胁和技术环境，做出准确、及时的影响评估，协助执行委员会分配所需资源以实施相应的缓解措施，确保组织的网络弹性。实施与整体业务目标相一致的安全控制，安全专业人员可以帮助将安全风险降至最低，在很多方面使组织受益，并帮助建立与客户和合作伙伴的信任。

获取CISSP认证有什么好处？

获得CISSP证明您有能力有效地设计、实施和管理一流的网络安全计划。如果您问持有CISSP认证的网络安全专业人员，他们是如何从中获益的，他们会告诉您以下几点：

- **职业机会和发展。** 提高您在改善企业安全方面的知识和专长的可信度，可以促进您的职业发展，并创造新的机会。
- **广泛而基础的网络安全知识。** 掌握可应用于不同技术和方法的通用的、与供应商无关的技能，以了解安全如何协同工作，从而为您的组织建立深度防御。
- **信誉。** 掌握广泛的知识可以帮助您打下坚实的基础，以便更好地减轻和应对网络攻击。
- **自信。** 培养对网络安全挑战和解决方案有更深、更好和更广泛理解的技能。
- **认可。** 让自己在同行中脱颖而出，获得安全专家群体的尊重和认可。
- **更广泛地理解企业与网络安全之间的联系。** 建立对所有现有和新兴的安全技术之间的相互联系和透彻理解，以实现更高生产力和更好成果的业务目标。
- **与您的商业伙伴建立信任和信心。** 能够胜任当前市场上的安全趋势和风险，以及这些安全问题如何直接影响业务、合作伙伴或客户。
- **工资较高。**拥有认证资格的安全专业人员比非认证人员的薪资高35%。
- **成为强大的同行网络中的一员。** 成为(ISC)²会员，可获得大量的独家资源、教育工具和同行交流机会。

(ISC)²如何助力

网络安全专业一直在变化，即使是最杰出的人，也会从通向成功之路的指导中受益。

CISSP被公认为是网络安全专业人员的金牌标准。CISSP是有经验的安全从业者、经理和高管的理想选择，能够证明自己在广泛的安全实践和原则方面的知识，包括首席信息安全官(CISO)、首席信息官(CIO)、安全总监、安全系统工程师、安全分析师、安全经理和安全顾问等职位。

CISSP通用知识体系(CBK)提供了对这里介绍的所有八个安全领域的深入认识和专业知识，有助于建立和展示坚实的网络安全基础、强大而多样的技能，这将成为任何寻求在网络安全领域发展的人的宝贵财富。

(ISC)²是安全认证领域的领导者，得到了全球企业的认可。(ISC)²可以帮助您发现正确路径，制定个人计划，并在职业生涯中蓬勃发展。要了解更多信息，请访问https://www.isc2china.org/?page_id=432

关于(ISC)²

(ISC)²（国际信息系统安全认证联盟）是一个国际非营利会员组织，专注于启迪构建一个安全可靠的网络世界。因其广受好评的信息系统安全认证专家(CISSP®)认证而最为人熟知，(ISC)²提供全方位、程序化的安全解决方案认证组合。我们的全球会员人数已经超过150,000，由经过认证的网络、信息、软件和基础设施安全专家组成，志在为行业发展带来改变并协助其进步。我们以慈善基金——网络安全和教育中心™对教育和普及大众的承诺而践行我们的愿景。

更多详情请见(ISC)²中文官网：https://www.isc2china.org； (ISC)²全球官网：https://www.isc2.org/

参考文献

[1] 国际电信联盟 (ITU)，“Measuring Digital Development, Facts and figures 2019”，见https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf。

[2] Datareportal，"Digital 2019:Global Digital Overview”，见https://datareportal.com/reports/digital-2019-global-digital-overview。

[3] Bank My Cell，“How Many Smartphones Are In The World?”，见https://www.bankmycell.com/blog/how-many-phones-are-in-the-world。

[4] 美通社，Ransomware Attack Every 14 Seconds”，见https://www.prnewswire.com/news-releases/ransomware-attack-every-14-seconds---prilock-announces-3-99-for-1-click-protection-300986165.html。

[5] Netwrix，“How Can Cybersecurity Help in Business Growth?”，见https://blog.netwrix.com/2019/10/22/how-can-cybersecurity-help-in-business-growth/。

[6] 沃达丰，“Cyber Security:The Innovation Accelerator”，见https://www.vodafone.com/business/white-paper/cyber-security-research-the-innovation-accelerator。

[7] 2020年CyberEdge网络威胁防御报告，见https://cyber-edge.com/cdr/。

[8] IBM，2019年数据泄露成本报告，见https://www.ibm.com/security/data-breach。

[9] 2020年CyberEdge网络威胁防御报告，见https://cyber-edge.com/cdr/。

[10] 2020年Verizon数据泄露调查报告(DBIR)，见https://enterprise.verizon.com/resources/reports/dbir/。

[11] IBM 2020年X-Force威胁情报指数，见https://www.ibm.com/security/data-breach/threat-intelligence。

[12] 2020年Verizon数据泄露调查报告(DBIR)。

[13] 2020年CyberEdge网络威胁防御报告。

[14] 2020年Verizon数据泄露调查报告(DBIR)。

[15] 2020年Verizon数据泄露调查报告(DBIR)。

[16] 2020年CyberEdge网络威胁防御报告。

[17] IBM 2020年X-Force威胁情报指数。

[18] IBM 2020年X-Force威胁情报指数。

[19] 世界经济论坛"当今数字世界领导人网络安全指南"，见https://www.weforum.org/reports/the-cybersecurity-guide-for-leaders-in-today-s-digital-world。

[20] 2020年Verizon数据泄露调查报告(DBIR)。