CSC

您的商务基石和最佳后盾®

首席信息安全官 (CISO) 2025 年展望

在人工智能兴起和监管日益严格的时代，
应对不断的域名威胁

企业面临的网络安全威胁种类越来越多、强度越来越猛烈，部分原因是人工智能（AI）快速崛起。

如今，不法分子可以使用越来越复杂的方法（DGA）形成威胁，包括深度伪造和域名生成算法，这对企业防御构成日益严峻的挑战。与此同时，首席信息安全官及其团队必须继续防范更具规模的安全威胁，例如分布式拒绝服务（DDoS）攻击。多年来尽管相关人员采取措施并努力遏制此类事件的影响，但公司仍然面临风险。

2025 年第一季度，CSC 委托独立机构对首席信息安全官、首席信息官（CIO）和其他高级 IT 专业人员开展研究，以进一步了解当前的安全忧虑。我们着手了解不断发展的网络威胁、当前的 IT 安全预算状况、网络安全专业人员如何应对日益严格和持续变化的监管水平，以及团队如何通过安全政策和技术来确保企业安全。

研究发现，近四分之三（70%）的受访者认为，未来一年安全威胁将会增加；几乎全部（98%）受访者预测未来三年安全威胁将会增加。近九成（87%）的人认为，人工智能赋能的域名生成算法构成威胁。

> 毫无疑问，首席信息安全官将继续面临安全威胁的挑战。我们的工作是不断寻求更好的方法控制残已有风险和新威胁载体。

我们的专家

Ihab Shraim
CSC 数字品牌服务首席技术官Services

Nina Hrichak
CSC 数字品牌服务部欧洲、中东和非洲地区客户管理副总裁

Mark Flegg
CSC 数字安全产品及服务技术
高级总监

Mark Eggleston
CSC 首席信息安全官

首席信息安全官意见：概览

我们在 2025 年第一季度对 300 名首席信息安全官、首席信息官和 IT 主管开展了调查，发现网络安全威胁是重大风险，而且越来越具有挑战性。

67%

的受访者表示，2024 年的网络安全威胁十分严重或显著。

70%

预计此类威胁在 2025 年将会增加。

98%

受访者认为此类风险在未来三年将会增加。

域名和 DNS 威胁将在有关威胁的整体局面中占主导地位

2024 年三大安全威胁如下：

1. 域名非法抢注 (cybersquatting)
2. 域名和域名系统 (DNS) 劫持
3. DDoS 攻击
4. 勒索软件和恶意软件
5. 社交媒体网络攻击和诽谤
6. 网络钓鱼和社会工程
7. 其他

未来三年预计面临的三大威胁是：

1. 域名非法抢注 (cybersquatting)
2. 域名和 DNS 劫持
3. 勒索软件和恶意软件
4. DDoS 攻击
5. 社交媒体网络攻击和诽谤
6. 网络钓鱼和社会工程
7. 其他

企业普遍利用外包服务解决网络安全，但情况各不相同

近一半受访者表示，他们主要使用内部系统、流程并以内部员工为主力，但在有些情况下会把工作外包给专家

只有不到五分之一 (18%) 的人士完全依靠内部资源。

18%

近三分之一 (30%) 的企业将业务外包给专家，同时也利用内部资源。

30%

人工智能将对网络安全产生重大影响

近九成 (87%) 的人认为，由人工智能赋能的域名生成算法构成威胁。

87%

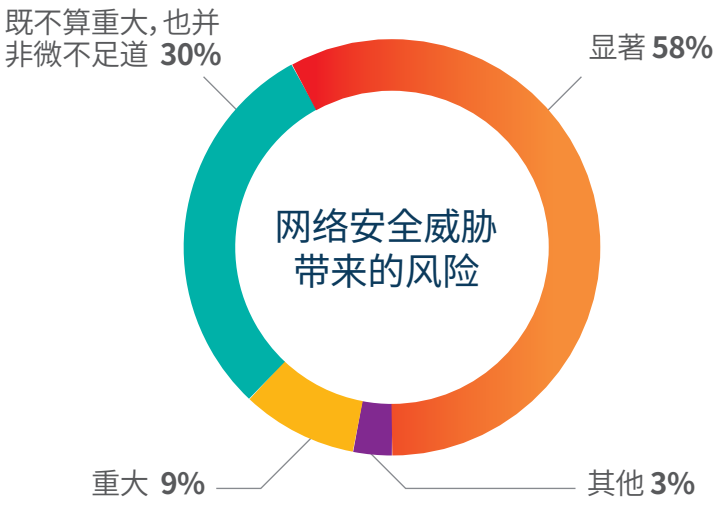
绝大多数人 (97%) 表示对于允许基于人工智能的第三方系统访问公司数据感到忧虑。

97%

网络威胁不断演变，而且只会日益复杂。

首席信息安全官面临日益复杂的网络威胁。 更糟糕的是，他们预测要面临的安全挑战只会日益严峻。

近十分之一 (9%) 的受访者表示， 2024 年网络安全威胁带来“重大”风险。 五分之三 (58%) 的人认为这些风险的影响非常显著，这表示三分之二的人 (67%) 认为风险很大。 另有 30% 的人表示，风险既不算重大，也并非微不足道。



“首席信息安全官需要应对转型的大时代，因此他们感到风险如此严重是可以理解的。”CSC 数字品牌服务部安全产品和服务 高级技术总监 Mark Flegg 表示

“随着企业开始将核心系统从内部、本地基础设施转移到云端，IT 环境也面临新的威胁。 子域名劫持或子域名接管就是很好的例子，这在 20 年前不是什么大问题——当时的公司自行运营数据中心，很少将 IP 地址空间或 DNS 控制权交给第三方。 现在，IT 系统更容易被入侵，不法分子会找寻机会寻找系统漏洞。”

网络威胁带来的风险 将在未来几个月内甚至 数年内恶化。近四分之三（70%）的受访者预计在 2025 年会出现增长，其中 5% 的人士表示增幅“显著”；98% 的人士预计在未来三年会出现增长，其中三分之二（66%）的受访者表示这会变得显著。

强大的人工智能功能涌现，表明有些域相关威胁的影响变得更大。

例如：网络犯罪分子可以使用人工智能进行大规模扫描，搜寻废弃或配置错误的子域名，从而接管子域名。

与此同时，首席信息安全官面临的一大挑战是目前已经在处理的大多数威胁仍然存在，而新的潜在攻击和犯罪手法日益繁多，而且更为复杂。

网络威胁变得越来越复杂，通常结合多种技术来提高成功的机会。 许多人都是从某一形式的社会工程开始的，有时还会结合误植域名（typosquatting）等陷阱，以近似域名的形式来提高可信度。

这些攻击推波助澜，为未来的威胁开辟道路。

其他示例包括：通过 DNS 隧道绕过安全措施，并通过网络传输恶意软件；或破坏第三方供应商的系统，并利用该访问权限窃取企业数据。

“我们看到的是，勒索软件等攻击并不是单独发生的，不法分子可能会通过混合攻击窃取信息，然后造成真正的破坏。”

Mark Eggleston
CSC 首席信息安全官

域名相关威胁
是首席信息安全官最关心的问题。

受访者认为去年的三大安全威胁是：
域名非法抢注、域名和 DNS 劫持，以及 DDoS 攻击。

只有 22% 的人表示他们已经拥有“合适的工具”。显然，首席信息安全官认为他们可以做更多的事情来应对域相关威胁，而且对强化资源的需求变得越来越迫切。

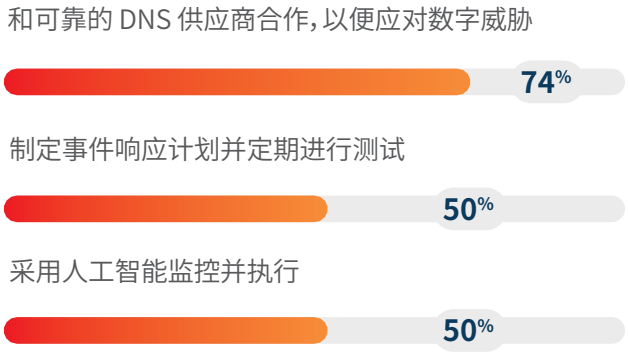
76% 四分之三的人表示，他们对公司缓解域名攻击的能力“有点信心”；只有 7% 的人表示他们“非常有信心”

99% 此外，几乎所有人（99%）都承认，他们有些担心或非常担心域名注册商没有遵循“了解您的客户（Know Your Customer，KYC）”政策来验证客户和供应商的身份。

59% 近五分之三（59%）的受访者表示，当公司检测到域相关网络威胁时，他们会采用工具和流程来缓解威胁，但消除威胁是一个复杂且耗时的过程。

参与《首席信息安全官 2025 年展望》调查的四分之三受访者与可靠的 DNS 供应商合作，以便应对瞄准攻击面和数字资产的数字威胁。

50% 的企业已经制定事件响应计划并定期进行测试，50% 的企业使用基于人工智能的监控和执行解决方案。



“最严重的安全风险仍然源自人为因素，所有公司最薄弱的环节就是团队内部缺乏教育。有些人现在才意识到 DNS 劫持和子域接管等风险。”

Nina Hrichak
CSC 数字品牌服务部欧洲、中东和非洲地区客户管理副总裁

人工智能在打击网络威胁方面发挥作用

但其普及程度仍然令人担忧

人工智能无疑正在为全球企业创造价值。我们采访过的首席信息安全官和其他高层领导表示，在人工智能集成方面，最大的投资回报（ROI）是流程自动化，其次是内部教育和数据分析

1. 流程自动化
2. 内部教育和员工培训
3. 网络安全
4. 欺诈检测
5. 数据分析
6. 查询响应

然而，在安全领域，人工智能显然被视为一把双刃剑，尤其会涉及在以下方面造成的威胁：员工和供应商将敏感数据上传到 ChatGPT 等大语言模型（LLM），以及网络犯罪分子使用人工智能来强化域生成算法等工具。

“人工智能可以用于有利方面，因为有助于我们更快地开展研究。例如：尽管存在出错的风险，任何人都不应该在未经人工验证的情况下交出生成式人工智能（GenAI）材料，但这仍然是开展背景工作的好方法。”Mark E 解释道，

“然而，同样重要的是，我们要认识到人工智能会带来新的威胁，例如用于网络钓鱼的深度伪造技术。”

对于允许基于人工智能的第三方系统访问公司数据，几乎全部受访者都感到担心。

大多数人（87%）表示，由人工智能赋能的域名生成算法对他们的组织构成威胁。造成威胁的不法分子可以生成大量侵犯知识产权、销售假冒商品或支持网络钓鱼计划的新域。可以在域名中使用的关键词组合可以说是无穷无尽。

Ihab 警告说，人工智能还有助于犯罪分子打造和发起完整的活动（包括有说服力的信息、虚假网站和自动化工具）来攻击企业。

“目前有各种以人工智能构建的平台，可以让不法分子针对特定垂直行业（例如金融服务）发起有针对性的攻击活动。"Ihab 表示，“这些工具包的设计很全面，令攻击更具说服力。我们过去经常见到的拼写错误和语法错误基本已经消失了，因为人工智能可以生成非常准确且文笔优美的信息。”

企业要有明确的治理政策，规定谁可以访问企业内的哪些大语言模型以及他们共享哪些信息。这包括要意识到影子人工智能（Shadow AI）造成的威胁与日俱增——这个概念是指员工或供应商未经批准而使用人工智能工具或应用程序。

CSC 数字品牌服务部首席技术官 IHAB SHRAIM 的专家观点

域相关威胁成为日益严峻的挑战的原因

“DNS 和域相关基础设施是网络犯罪分子的软目标，他们使用特定的威胁载体（如 DNS 劫持或域欺骗）来利用暴露的系统。

不法分子会广泛侦察，扫描从社交媒体到招聘网站的所有内容，以找到潜在的漏洞，包括对公司有所不满的内部人员，这些人可能容易成为网络钓鱼攻击的目标。

他们特别关注企业必须让公众访问的资产，如 DNS、网站或电子邮件网关，从而更容易发起域名非法占用或 DNS 缓存中毒等精确攻击。

我们已经看到大量的此类攻击，随着更多现成工具和用于攻击的工具包被广泛使用，我们预计到 2025 年，此类攻击将急剧增加。”

Ihab Shraim 提出的五大措施，旨在制定人工智能治理政策

1. **制定明确的人工智能政策。**
对于采用人工智能的企业来说，首要任务是制定一项在整个企业内传达的正式政策 。

2. **制定明确的数据共享规则。**
明确定义员工可以和不可以输入大语言模型的数据类型，以最大限度地降低暴露风险。

3. **在隔离环境中进行测试。**
使用人工智能模型进行测试时，请在企业管理的安全、私密环境（而不是云端）中运行，以保持控制权并降低风险 。

4. **定义具体的用例。**
构建人工智能模型时应有明确的目标，例如实现某个特定功能自动化，以防止意外的数据污染。

5. **验证人工智能输出的成果。**
使用人工智能的人士都不应假设由人工智能生成的数据是一直准确的——人工审计仍然至关重要。

Ihab 表示：“随着信息在互联的人工智能模型中不断被重复传播和强化，虚假数据可能会污染互联网的整个细分领域。展望未来，技术人员对所用数据进行基本检查将变得更具挑战性。”

Ihab Shraim
CSC 数字品牌服务部首席技术官

注重
影子人工智能

当最终用户绕过 IT 治理时，首席信息安全官面临一系列安全威胁，从某种程度上来说，影子人工智能可以被视为当中的最新类型，类似于员工首次采用 Dropbox 等工具，或将自己的移动设备带入工作场所而不受监督的情况。

从另一个角度来看，这要复杂得多，也更为阴险。由于许多人工智能工具都是基于云端并在外部托管的，因此不法分子可以用于发现漏洞或滥用员工无意中使用的数据。如果公司或客户的敏感信息因未经授权被使用而泄露，则风险包括数据泄露及未能达到合规标准。

Mark E. 表示，解决影子人工智能相关问题的方法是使用软件代理来跟踪在整个企业范围内使用的所有大语言模型。“这意味着我们可以看到谁在通过人工智能工具上传和下载信息，并且我们可以阻止那些风险很高的行为。然后，您可以采用零信任体系，验证用户并加以控制，以确保每个人都遵守企业的人工智能治理政策。”

IT 安全预算

可能无法跟上网络威胁日益严峻的形势。

尽管大型企业将网络安全视为首要业务重点，但仍然可能很难获得所需的预算来防范日益增多的威胁，以及保护企业必须管理的庞大数据集。

“问题在于，网络安全方面的投资并不会带来丰厚的回报。”Mark F 说，

“这就像购买保险——每个人都不愿意支付保费，但当需要提出索赔时，保单就是有史以来最好的保障。注重预算的企业仍然质疑用于保护的成本是否真的合理。”

“我们必须每年都计划增加预算。”Mark F 补充说，“因为已经在处理的威胁不会就此消失，所以仍然需要资金来应对这些威胁以及出现的新问题。首席信息安全官花费了大量时间构建防火墙、拉起通往城堡的吊桥，现在他们发现有人在壕沟下修建隧道。”

由董事会确定的网络安全优先事项与资金安排不相符的原因之一是，决策者不一定是最了解域名安全风险潜在影响的人员。

首席信息安全官正在采取措施，通过讨论域名相关威胁可能产生的现实影响来解决这种差异，而且许多人正在与高层同事沟通合作，以确保其他人更好地理解这些威胁。

网络安全及相关信息安全与管理的总体预算。

仅有 7% 的受访者表示，在 2024 年至 2025 年间，其公司的网络安全及相关信息安全与管理的总体预算大幅增加，而大多数（80%）受访者表示，其预算略有增加。

谁负责决定分配用于网络安全的资金？

资金分配的决策者最有可能是首席风险官（CRO）或风险管理团队（23%）、首席财务官或财务团队（21%）或首席信息安全官或 IT 团队（18%）。

首席信息安全官与其他部门讨论的与数字风险相关的五大主题排名如下：

1. 商誉和经济损失
2. 网络安全与数据保护
3. 战略规划和业务目标
4. 预算和资源分配
5. 合规与风险管理

“很高兴看到首席信息安全官关注商誉和财务风险，而不是合规，合规通常是网络安全战略中最简单的部分。” **Mark E.** 表示，“大多数首席信息安全官都知道如何处理合规问题，但声誉受损才是让我们夜不能寐的事情。”

域名安全预算有时会被忽视的原因

“许多公司仍然将域名纯粹视为商标预算项目，这种思路需要转变，应从安全性角度衡量。”Nina 表示。

“谈到公司的域组合时，有两件事需要牢记。”她指出，“首先，注册域名相对便宜。其次，在许多司法管辖区，与注册相关的规则很少甚至完全没有。因此，通过域注册来保护品牌极为重要，不仅在核心市场，而且在高风险域扩展范围中。

所以，应该为域名安全留出更大比例的安全预算。有些公司的首席信息安全官对数字资产管理方式缺乏了解，且责任落在不太关注安全性的人员身上，注册表锁定等具有成本效益的关键措施可能会被忽视。

不存在万能法则。公司可以采取广泛注册的防御战略，或者采取更精简的方式，监控侵权行为并在必要时采取行动。”

NIS2 合规 **对于许多企业来说仍是一项正在进行 的工作**

监管合规对于首席信息安全官来说是一个持续的挑战。不遵守《网络和信息安全指令 2》(The Network and Information Security Directive 2，NIS2)和《通用数据保护条例》(General Data Protection Regulation，GDPR)等法规，将面临巨额罚款和声誉受损的风险。

尽管如此，企业可能对 NIS2 视若无睹，因为领导层认为该法律不适用于自己的公司，或者因为不同的欧盟国家在推出新法律的当地版本方面进展缓慢。

这种延迟可以解释为什么受访者根据解决特定网络安全和信息安全风险的难度，对监管体系进行排名的情况如下：

1. NIS2 **(欧洲)**

2. GDPR **(欧洲)**

3. 网络安全成熟度模型认证 **(美国)**

4. 国际标准化组织、国际电工委员会 **(ISO/IEC) 27001/2 (全球)**

5. 支付卡行业数据安全标准 **(美国)**

6. 关键基础设施保护 **(CIP)** 标准 **(美国)**

7. 《数字运营弹性法案》**(DORA) (欧洲)**

“有些国家会完全照搬该指令，而其他国家则会根据自己的情况进行调整。" **Mark F.** 说，“目前，我们所能做的就是找出迄今为止，各国实施 NIS2 的不同方式之间存在的共同点。”

只有 9% 的人表示他们的企业完全符合 NIS2。最大的挑战是确保外部合作伙伴遵守规定（73%），以及难以正确理解和执行复杂的法规（64%）。

这与本报告前面列出的调查结果相呼应：受访者担心合作伙伴未能与供应商和其他第三方完成 KYC 检查，这种做法可能会影响企业供应链的安全。

“我们认为，NIS2 之所以排在第一位，因为这是目前最紧迫的任务。”Nina 说，“我们正在经历与处理 GDPR 类似的过程，每个人都知道他们需要做某事，但不太确定从哪里开始着手。同时，ISO/IEC 27001/2 已经存在很长时间了，获得认证的过程非常紧张。”

您是否预计，公司在未来三年内面临的安全审计数量以及监管和合规要求会增加？

为增加安全审计做好准备

Mark E. 指出，公司现在面临的监管要求增加，部分原因是各司法管辖区对人工智能监管表现出与之前对数据隐私法相同的趋势，这有利于开发自己的体系。

“相应的管理方法是将所有与监管相关的数据（无论是隐私、人工智能还是其他）置于一个

控制体系中。”**Mark E.** 表示，这意味着当首席信息安全官去审核某些内容时，他们可以根据所有标准进行认证；如果他们能做到‘审核一次，认证多项’，那么确实可以减少所需的工作量。

首席信息安全官要确保他们的治理、风险和合规计划有效，并将上述所有要求置于一个共同的

体系，并且他们可以在审计和保持控制方面实现自动化

战略性外包 有助于首席信息安全官大规模管理复杂问题

大多数首席信息安全官及其所在的企业都认识到在检测、管理和预防网络攻击方面将工作外包的价值。

48%

说他们主要依靠内部系统、流程和员工

30%

主要外包给专家

在公司内部处理所有事情

18%

将所有事情外包

4%

现实情况是，大多数 IT 和网络安全团队不可能专注于所有领域。外包有助于填补关键空白，特别是在需要持续监控、深厚专业知识或超出内部团队能力的规模的领域。

外部合作伙伴可以提供真正价值的一个例子是检测和响应第三方域名注册。新域名不断被注册，而且注册相对容易，所以光凭内部团队，几乎不可能跟上节奏。注册量激增通常是由现实世界

的事件、产品发布或公开声明而导致的，跟踪这些模式可以揭示在传统品牌监控之外的新兴威胁或市场信号。经验丰富的供应商可以提供自动化监控，以大规模扫描并识别可提供更广泛的商业情报的趋势，而不仅仅是潜在的侵权行为。

然而，实现监控自动化只是开始。最重要的是由专家解释结果和指导决策，例如是否防御性地注册域名或删除。并非每个企业都拥有对域活动或相关背景具有深入了解的员工，因此，一个能够掌握最新动态的合作伙伴，可以带来关键见解和敏捷性。

> “经验丰富的合作伙伴可以帮助您应对不同网络安全风险的演变。我们今天所看到的情况，并不意味着几个月后我们还会看到同样的趋势。可能会有一些新的事物到来，您必须领先一步。”

Nina Hrichak
CSC 数字品牌服务部欧洲、
中东和非洲地区客户管理副总裁

们专家提供的更多信息

为简化而合作：
一站式管理域和 DNS 安全事务

“针对域和 DNS 安全问题，在考虑与外包合作伙伴并肩作战时，重点是根据企业相关行业、其数字资产组合的构成方式、预算和风险承受能力来制定战略。”**Nina** 表示，

“这包括选择正确的单一供应商，而不是多个供应商，因为拥有许多不同的联系点可能会带来风险。 企业应该简化他们的战略，以确保在出现问题的时候，他们知道向谁求助，而不是同时拥有 10 个不同的供应商——尤其是在紧急情况下。

此外，还需要建立可靠的合作伙伴关系，并确保供应商采用与公司内部相同的方法。

回顾行业的发展和新兴的威胁载体，公司必须不断重新思考战略，因为没有任何企业能够停滞不前，域和商标组合不会发生变化。

与此同时，公司必须跟上行业的发展，而这正是可靠的供应商能够真正提供帮助的另一个领域。”

多层次、合规的安全计划是什么样的？

CSC 能够在域名安全生态系统方面很好地帮助企业。 这是因为我们提供多层安全保障——一种在不同层次（包括域名）采用多种安全措施的网络安全方法。 我们防范包括 DDoS 攻击、域欺骗、在线品牌滥用和网络钓鱼在内的威胁。

“如果没有域名安全，您的安全部署就不完整。”**Ihab** 解释说， “监测很重要，但不能单独存在。” 如果没有全球打击机制，您只是通知企业存在问题，但却没有能力去解决该问题。”

当域名被盗用时，犯罪分子可以将网站访问者重定向到钓鱼网站，冒充品牌，销售假冒商品，并关闭网站和关键业务操作，从而损害客户信任和公司声誉。

Mark F. 强调，域名和 DNS 是企业在线形象的基础。 “把您的企业想象成一座用扑克牌搭建的房子。 底行代表您的域和 DNS，支持您在线进行的所有操作。 如果我把最底层的卡片拿出来，您在其上建造的一切都会倒塌。 您的网站、电子邮件都会受到影响，如果您使用 IP 语音，您的电话也会受到影响。 首席信息安全官需要问自己，如果发生这种情况，我们的后备计划是什么？”

换句话说，企业必须将域名安全视为其整体安全战略的不可或缺的基本组成部分，因为当该部分出现故障时，整个结构就会面临风险。

Conclusion

首席信息安全官负责企业中最艰巨的工作之一——确保其企业的数据安全并遵守日益复杂的法规。网络威胁的数量和复杂程度都在增加，包括域和 DNS 攻击。

人工智能在安全领域发挥重要作用，但也会催生新一波复杂的手段，从而对缺乏足够保护的企业造成严重破坏。

尽管面临这些挑战，我们的第一份《首席信息安全官展望》报告发现，对于大多数首席信息安全官来说，IT 安全预算逐年仅呈现小幅增长。这可能反映出高层管理人员对于当今最重大的企业威胁的真正问题存在理解上的差距。

Nina 说，确保员工和合作伙伴始终遵守治理计划尤为重要。

“团队中只要有一个人点击错误的电子邮件并给出错误的数据，就会有问题，合作伙伴也会遇到同样的情况。” Nina 说，“只要有一个合作伙伴在某些事情上失误，就可能会导致非常大的问题。”

在快速变化的威胁形势下保持敏捷同样重要，尤其是当涉及到与域名和数字基础设施相关的不断演变的风险时。

在此背景下，我们鼓励首席信息安全官：

- 采用结构良好、多层次的安全战略，将工具、流程和技能知识以正确的方式融合在一起
- 建立 GRC 计划，注重 用户监控、员工教育和供应商数据安全实践
- 与可靠且具有前瞻性的供应商合作，减轻内部团队的负担并增强整体适应力

如想CSC 如何帮助您的企业在域管理和网络安全方面保持领先一步，请访问 cscdbs.com/cn/.

“我们被迫频繁更改密码是有原因的，因为密码长期不变，被破解的可能性就越大。” **Mark F.** 总结说，“任何入侵或劫持事件或者任何虚假网站都是如此。置之不理越久，影响就越大。这种事不好处理，但还是得迎难而上。”

参与调查的受访者
概况

行业细分领域

- 19% 金融机构
- 18% 医疗保健和保险
- 17% 零售业和消费品
- 16% 技术、媒体和电信
- 11% 工业品、能源和公用事业
- 20% 其他

受访者的职位

- 首席信息安全官 60%
- 首席信息官 13%
- 高级网络安全总监和网络安全主管 11%
- 首席技术官 8%
- IT 主管（或同等职位） 8%

按地区划分的公司总部

33%
欧洲

33%
北美

33%
亚太地区

沟通交流

1 800 927 9800 | cscdbs.com/cn

CSC 简介

CSC 是值得信赖的优选安全和威胁防范提供商，深受福布斯全球企业 2000 强和全球最佳品牌 100 强 (Interbrand®) 企业的青睐，专注于域名安全和管理以及数字品牌和欺诈防护业务。随着全球越来越多的公司加大投资力度完善安全状况，我们的 DomainSec℠ 平台可以一展身手，帮助这些公司了解他们存在的网络安全漏洞并且保护其在线数字资产和品牌。企业可凭借 CSC 的专有技术来增强自身的安全状况，防范针对在线资产和品牌声誉的网络威胁，从而避免遭受严重的收入损失。

CSC 还提供在线品牌保护（将在线品牌监控和维权活动相结合），多维度审视防火墙外针对特定域名的各类网络威胁。欺诈防护服务可在攻击的早期阶段打击网络钓鱼，使我们的解决方案更加完善。

CSC 成立于 1899 年，总部位于美国特拉华州威尔明顿市，在美国、加拿大、欧洲和亚太地区设有办事处。CSC 是一家全球性公司，我们聘用所服务行业的业内专家，为世界各地的客户提供服务。

DBS09102025