中国首席安全官（CSO）
调研报告

安全内参

360 企业安全研究院

2018 年 9 月

摘　　要

- 本次调研共收集到来自不同行业政企机构的调研问卷129份。从被调研者所属行业来看，IT 和互联网行业占比最高，分别为 25.6%和 13.2%。其次，通信行业占比为 10.9%。
- 从 CSO 岗位的设置情况来看：正式设立 CSO 或相应级别岗位的政企机构约为 30.2%；20.9%的机构正在考虑设置；而近一半的机构，目前完全没有设立 CSO 或相应的岗位。
- 从 CSO 的汇报对象来看：27.2%的 CSO 的汇报对象是公司 CEO 或机构一把手；12.4%的 CSO 汇报对象是技术副总裁；41.1%的 CSO 的汇报对象是分管领导。
- 在大中型企业中，百万级规模网络安全投入是主流。38%的万人以上规模的政企机构投入超过 5000 万；25%的 3000-5000 人规模的政企机构投入超过 5000 万。
- 八成以上的政企机构在过去两年内对网络安全的投入都在增加。其中，明显增加的占比为 42.6%；稍有增加的占比为 41.9%；但是，仍有 15.5%的机构没有增加网络安全的投入。
- CSO 对网络安全团队建设最大挑战的看法：32.6%的 CSO 认为是待遇薪资太低留不住人才，29.5%的 CSO 认为是网络安全人才稀缺；20.9%的 CSO 认为是安全人才的上升通道不畅。
- CSO 评价自身所在机构的网络安全建设水平处于滑动标尺模型的阶段：仅有 0.8%CSO 认为达到了进攻反制阶段；而 41.1%的 CSO 认为仅仅是达到了被动防御的建设阶段。认为自己所在机构能达到主动防御阶段水平的被调研者约占 27.1%。

- CSO 对机构自身的网络安全建设水平的看法：仅有 4.7%的 CSO 认为已经达到了国际先进的水平；认为自己达到了国内领先和行业领先水平的分别占 15.5%和 20.9%。
- CSO 对内部威胁的看法：43.4%的 CSO 认为“内部”威胁过去不是重点，目前重视度在增加；37.2%的 CSO 认为内部威胁已经是目前防护的重点之一；13.2%的 CSO 认为，针对内部威胁缺乏行之有效的措施。
- CSO 对网络安全工作转型的主要聚焦于：29.5%的 CSO 们认为是“需从事后补救式防护转向三同步”；其次，27.9%的 CSO 认为是“需要从安全合规转向安全能力建设”，选“需要从边界防护转向主动立体防护”占比 21.7%。
- CSO 对未来网络安全建设的看法：约七成的 CSO 认为，从购买安全产品逐步转向购买安全服务；40.3%的 CSO 认为未来在网络安全建设时会与安全公司联合运营；还有 29.5%的 CSO 认为，在未来网络安全建设时会采用安全服务外包。
- CSO 关注的网络安全技术创新领域：72.1%的 CSO 选择了“大数据”，排名第一；其次是“人工智能”，65.9%的 CSO 看好这一领域；“用户行为分析”排名第三，看好率为 55.8%。

关键词：首席安全官、首席信息官、CSO、网络安全

目　　录

第一章 CSO 现状与面临的挑战.....3

一、 CSO 岗位的设立.....3

二、 CSO 的行政级别.....4

三、 CSO 的汇报对象.....5

四、 运营与管理中的困难.....6

第二章 网络安全投入与团队建设.....8

一、 网络安全的投入情况.....8

二、 安全团队的建设规模.....10

三、 安全团队的建设难点.....11

第三章 CSO 对机构安全建设的自评.....12

一、 网络安全发展阶段.....12

二、 网络安全建设水平.....14

三、 对内部威胁的看法.....14

第四章 CSO 对网络安全趋势的认知.....16

一、 网络安全工作的转型.....16

二、 网络安全服务的普及.....17

三、 网络安全技术的创新.....18

第五章 总结.....19

附录 1　2018 中国首席安全官调查问卷.....20

附录 2　安全内参.....21

研究背景

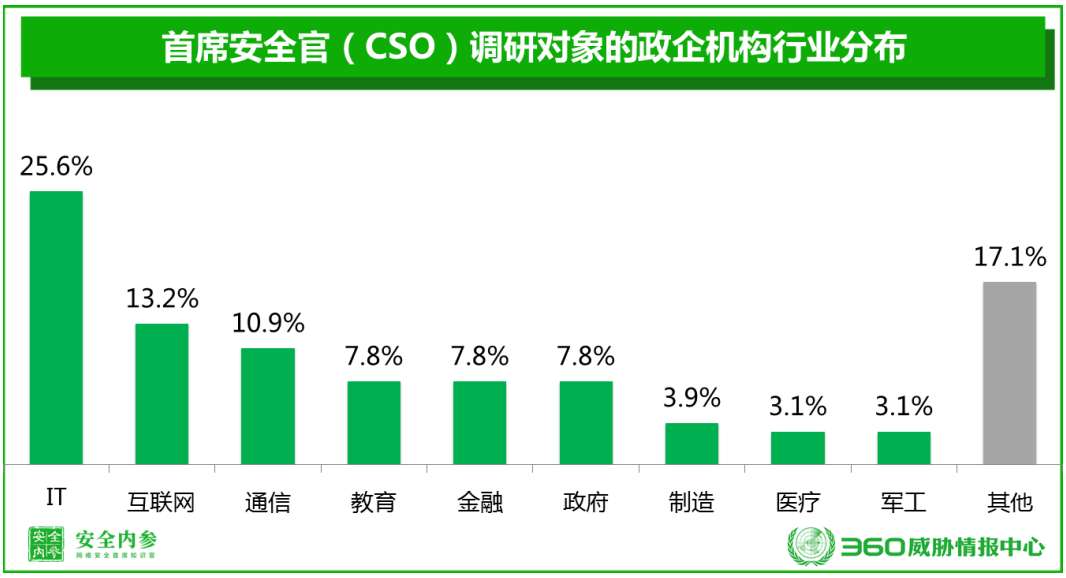
CSO，即 Chief Security Officer，意为首席安全官或首席安全信息官，主管一个机构内部的网络安全事务。这一关键性职务目前在欧美国家的大型政企机构中已经普遍设置，并且具有较高的内部权力。同时，这一职务在国内也正在得到越来越多的认可与重视。

为了深入了解国内大型政企机构网络安全建设现状，了解中国各大政企机构首席安全官的工作环境，国内权威网络安全咨询平台《安全内参》与 360 政企机构安全研究院展开联合研究，对不同行业政企机构的首席安全官或安全负责人进行了一次深入的调研，并形成此份研究报告。

考虑到国内很多政企机构的网络安全主管人员并不一定会被任命为首席安全官，或相关岗位有其他名称，所以，本次调研所针对的对象并不严格限定为 CSO 或首席安全官，而包括首席安全官、首席信息官（CIO）、网络安全主管、网络安全分管领导、网络安全主要负责人等。被调研人员一定为该机构网络安全工作的主管领导或主要负责人，但不一定是专职领导或负责人。

本次调研共收集到来自不同行业政企机构的调研问卷 129 份。从被调研者所属行业来看，IT 和互联网行业占比最高，分别为 25.6%和 13.2%；IT 和互联网是以网络为基础发展起来的，其对网络安全的认知与感知度相对较高。其次，通信行业占比为

10.9%；教育行业占比为 7.8%。具体分布情况如下图所示。



以这 129 份调研问卷为基准，本次报告在首席安全官的现状与面临的挑战、网络安全投入与团队建设、CSO 对机构安全建设的自评以及 CSO 对网络安全趋势的认知等方面进行了深入的分析与研究。

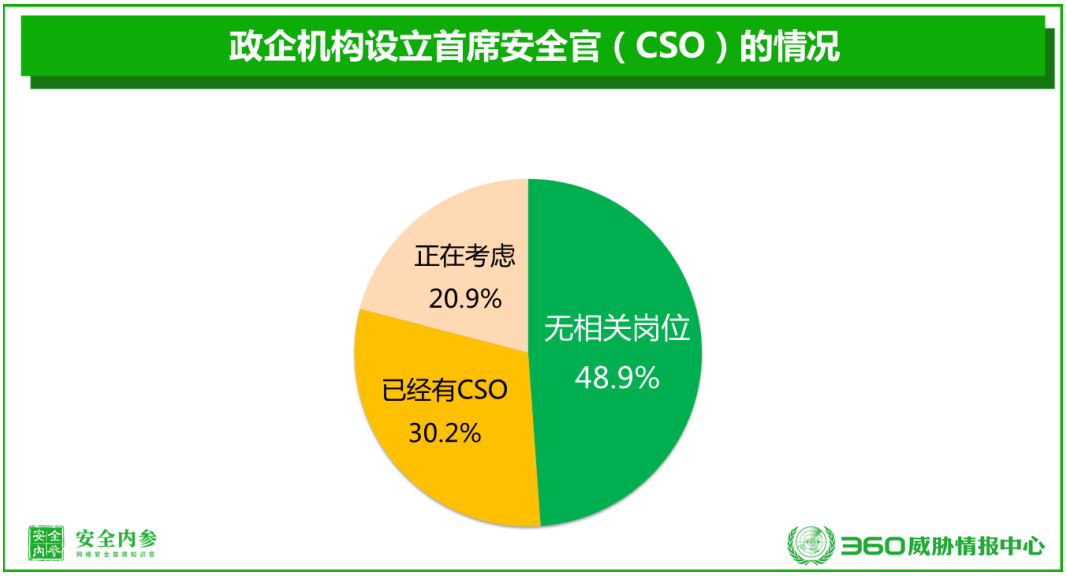
第一章 CSO 现状与面临的挑战

CSO，即 Chief Security Officer，意为首席安全官或首席安全信息官，主管一个机构内部的网络安全事务。这一关键性职务目前在欧美国家的大型政企机构中已经普遍设置，并且具有较高的内部权力。同时，这一职务在国内也正在得到越来越多的认可与重视。

本章主要对政企机构的首席安全官的岗位设置情况、行政级别、汇报对象以及运营与管理中的困难进行分析。

一、 CSO 岗位的设立

政企机构设置 CSO 这个岗位，通常意味着机构高层希望在某种程度上把信息安全工作抓起来、需要有人对此统筹、负责。而此次调研显示，目前正式设立 CSO 或相应级别岗位的政企机构不足三成，约为 30.2%；20.9%的机构正在考虑设置这一岗位；而近一半的机构，目前完全没有设立 CSO 或相应的岗位，也没有考虑短期内设置这一岗位。这一结果在一定程度上反映出网络安全工作仍然普遍没有得到足够的重视，网络安全主管人员或主要负责人，在政企机构内部的地位仍然普遍不高。



特别需要说明的是，由于很多政企机构尚未设立首席安全官（CSO）的岗位，所以本次调研对象中除了正式的 CSO 外，还包括首席信息官（CIO）、网络安全主管、网络安全分管领导、网络安全主要负责人等。但本次报告为了分析和表述方便，如无特殊说明，后文中统一使用 CSO 或首席安全官指代政企机构中的网络安全主管和主要负责人，不论其实际岗位名称或行政级别如何。

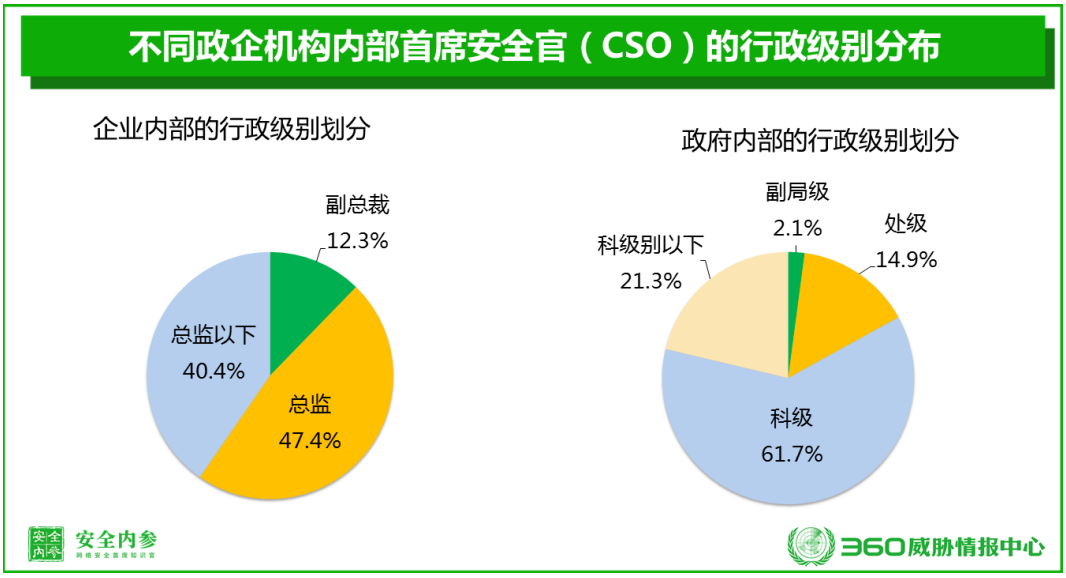
二、 CSO 的行政级别

首席安全官的行政级别在一定程度上代表了该机构对网络安全的重视程度。CSO 的行政级别越高，一般相应的权力也越大、话语权越高，拥有的资源越多，网络安全运维与管理工作也相对更容易开展。

考虑到政府及事业单位的行政级别与企业内部的行政级别有较大的差异，所以，本次调研进行了分别统计。统计显示，在

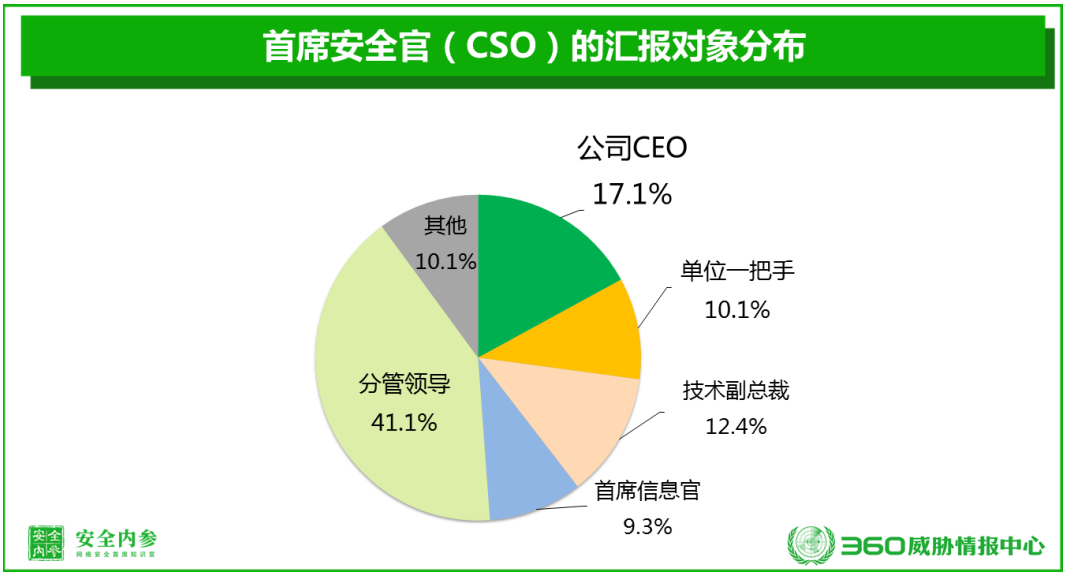
企业中，仅有 12.3%的 CSO 行政级别达到了副总裁级别；47.4%的 CSO 属于总监级别；40.4%的 CSO 级别为总监级别以下。

从政府及事业单位来看，仅有 2.1%的 CSO 行政级别能够达到副局级；14.9%的 CSO 行政级别达到处级；61.7%的 CSO 的行政级别处于科级；21.3%的 CSO 的行政级别处于科级别以下。具体分布情况如下图所示。由此可见，对于绝大多数政企机构来说，CSO 的行政级别极低，很难发挥有效的安全管理作用。



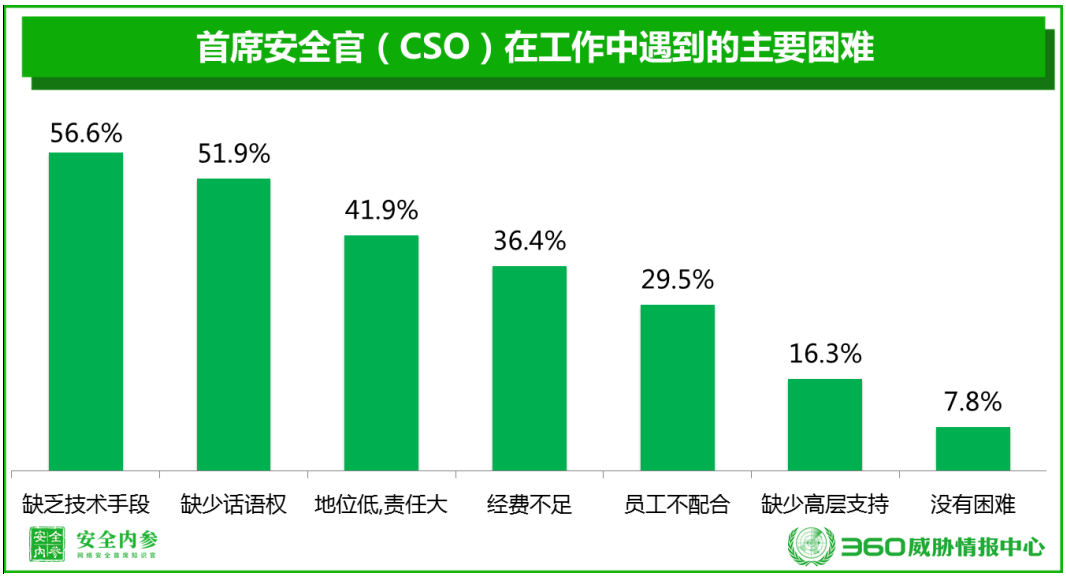
三、 CSO 的汇报对象

我们再来看 CSO 的工作汇报对象。统计显示，27.2%的 CSO 的汇报对象是公司 CEO 或机构一把手；12.4%的 CSO 汇报对象是技术副总裁；41.1%的 CSO 的汇报对象是分管领导。具体分布如下图所示。



四、 运营与管理中的困难

首席安全官在工作中也会遇到各种各样的困难。调研显示，56.6%的 CSO 认为当前缺乏有效的技术手段落实安全管理；51.9%的 CSO 认为相对于业务发展，安全部门缺少话语权；41.9%的 CSO 认为安全人员地位低但责任大。仅有 7.8%的 CSO 认为没有太大的困难。



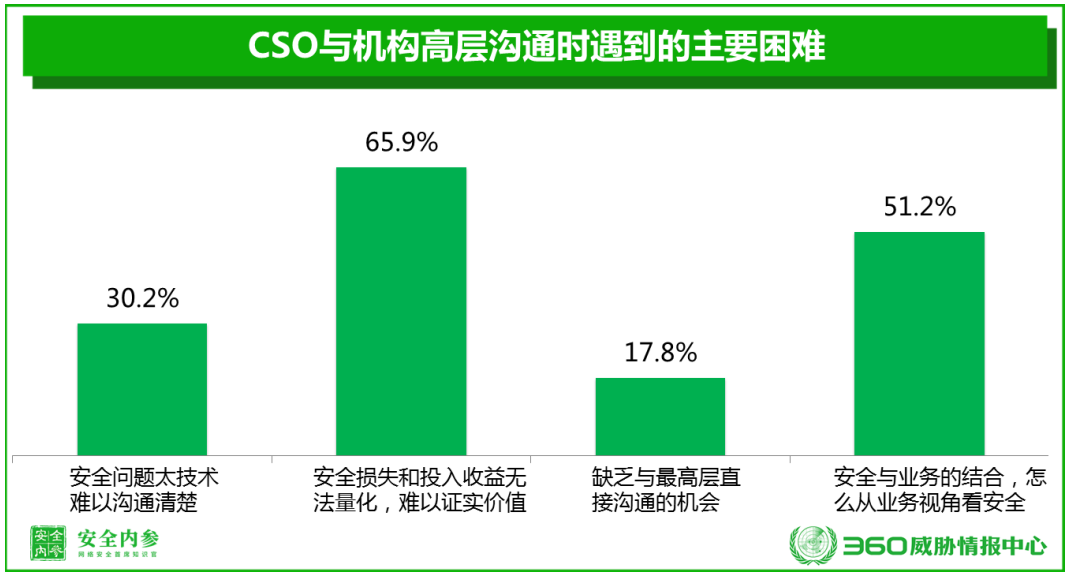
网络安全工作的价值和重要性往往难以得到领导或机构高层的认可，与高层的沟通也存在诸多的困难。这也是本次调研反映出的一个重要问题。这些与机构高层沟通中遇到的困难主要表现在以下四个方面：

1） 网络安全损失和投入收益无法量化，难以证实安全的价值。这也是网络安全负责人与机构高层沟通中遇到的最为普遍困难，65.9%的 CSO 遇到了这样的困难。

2） 网络安全该怎样与业务的结合，怎么从业务视角看安全也是一个重要的沟通难题。有超过半数（51.2%）的 CSO 遇到了这样的困难。

3） 安全问题太技术，难以沟通清楚。30.2%的 CSO 遭遇这样的沟通困难。

4） 缺乏与最高层直接沟通的机会。17.8%的 CSO 认为存在此类沟通问题。



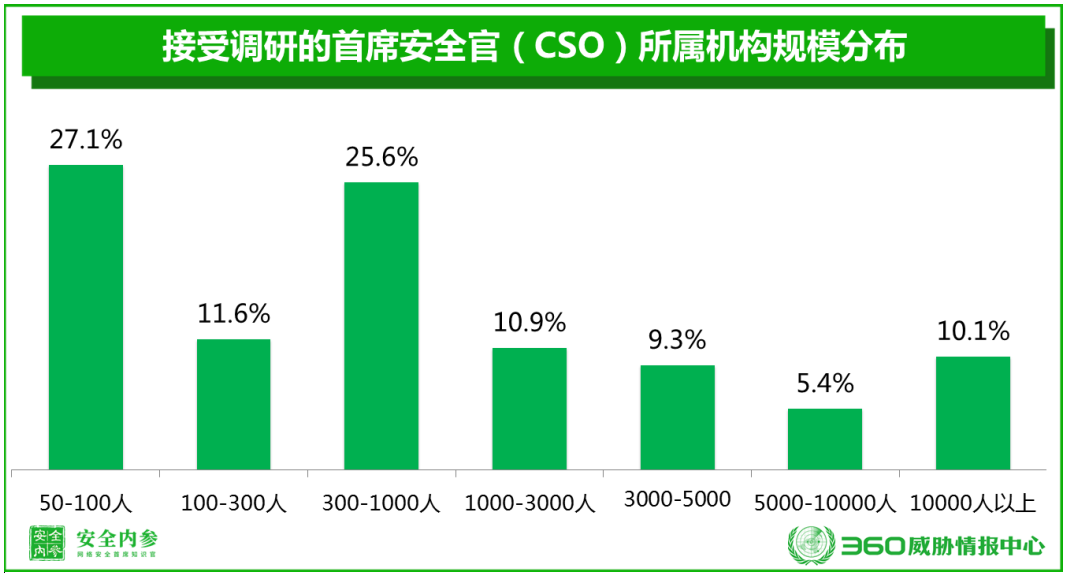
第二章 网络安全投入与团队建设

政企机构对网络安全的资金投入，在一定程度上也能反应出该机构对网络安全工作的重视程度。在机构规模和业务相近的情况下，重视程度越高，一般投入也越大。本章主要对不同行业，不同规模的政企机构的网络安全投入情况、安全团队的建设规模和难点等问题进行分析。

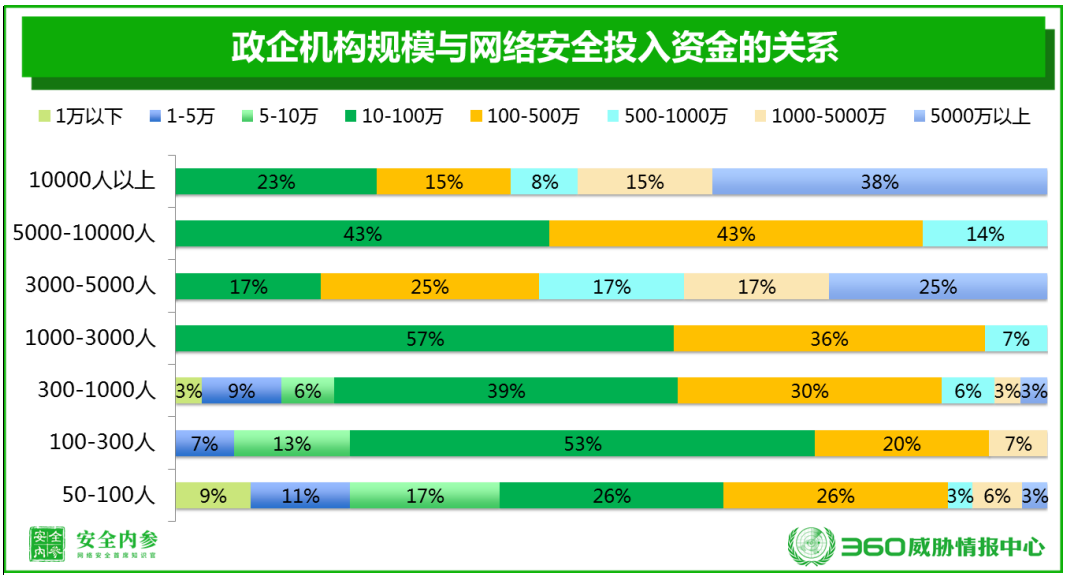
一、 网络安全的投入情况

影响政企机构网络安全投入水平的第一因素是机构的规模。通常来说，政企机构规模越大，IT 化程度越高，所需在网络安全方面投入的资金也越多。

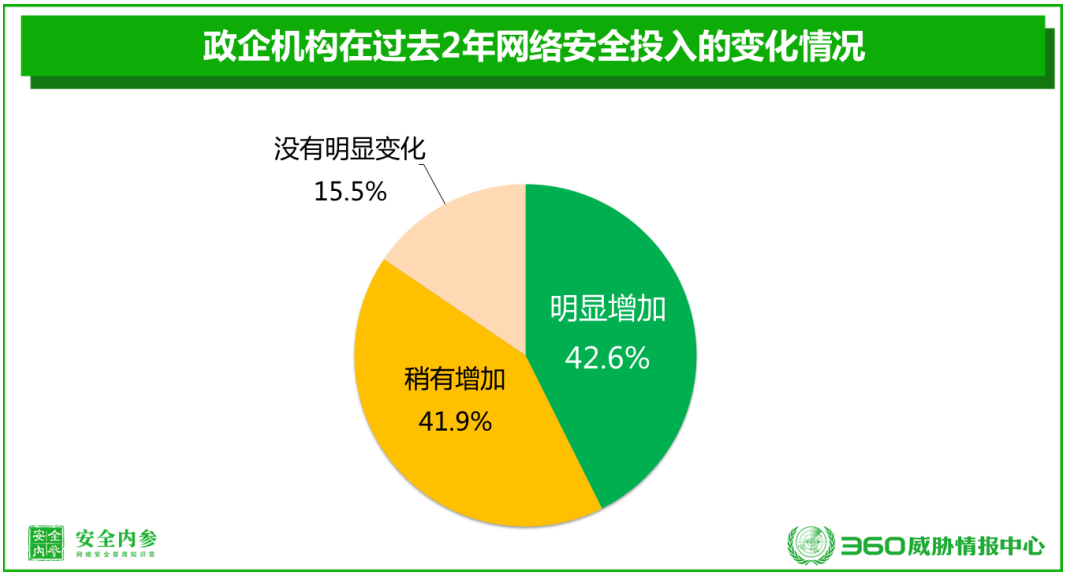
在本次调研的 129 位受访者所属的机构中，约六成的机构规模在 1000 人以下。其中，100 人以下的政企机构，占 27.1%；100-300 人的机构，占 11.6%；300 人至 1000 人的机构规模占到了 25.6%。具体分布如下图所示。



从政企机构规模与网络安全投入之间的关系来看，规模越大的机构在网络安全上的投入资金往往更多。但总体来看在大中型企业中，百万级规模的网络安全投入是主流，主要集中在 100 万以下和 100 万-500 万这两个层次间。38%的万人以上规模的政企机构在网络安全上的资金投入超过 5000 万；25%的 3000-5000 人规模的政企机构在网络安全上的投入超过 5000 万。具体分布如下图所示。

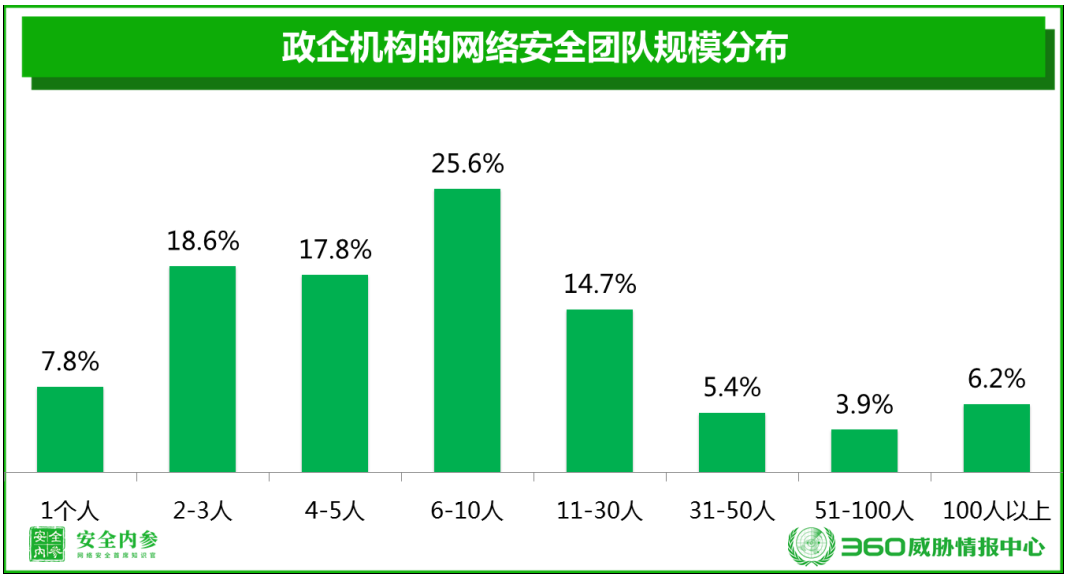


本次研究还特别对网络安全投入的增长情况进行了分析。统计显示，八成以上的政企机构在过去两年内对网络安全的投入都在增加。其中，明显增加的占比为 42.6%；稍有增加的占比为 41.9%，可见，网络安全工作受重视的程度整体上还是在不断提高。但是，仍有 15.5%的政企机构在过去两年内无动于衷，没有增加网络安全的投入。具体分布情况如下图所示。



二、 安全团队的建设规模

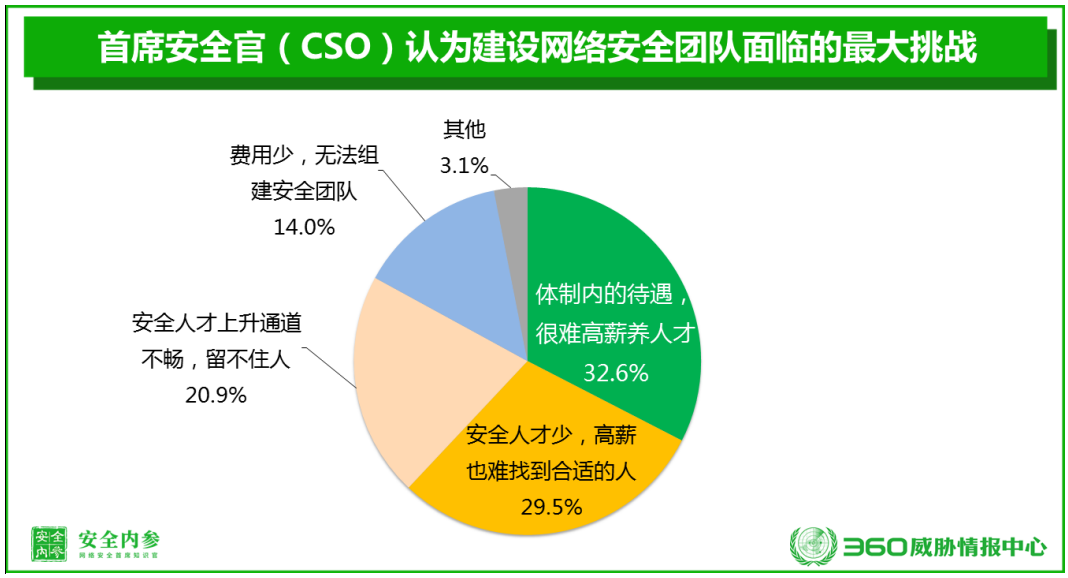
网络安全团队是保护政企机构的核心基础资源的重要力量，网络安全团队的人数可以在一定程度上反映出机构自身网络安全运维与管理的能力。统计显示，44.2%的政企机构只有 5 人以下的小型团队来保护网络安全。拥有 11-50 人的中型网络安全团队的机构约占 20.1%；拥有 50 人以上较大规模网络安全团队的机构约占 10.1%。具体分布情况如下图。



安全团队规模与公司规模有一定的相关性。通常来说，公司规模越大，其相对应的网络安全团队人数也就越多。根据数据统计显示：公司规模在 100 人以下的网络安全团队，主要以 3-10 人为主；公司规模在 100 人和 1000 人之间的网络安全团队，主要以 5-10 人为主；公司规模在 1000 人和 5000 人之间的网络安全团队，主要以 10-30 人为主；而万人以上的公司，其网络安全团队一般在 100 人以上。

三、 安全团队的建设难点

薪资待遇、职业发展、人才供给等因素都是目前政企机构组建网络安全团队面临的。在被问及网络安全团队建设“最大”的挑战是什么时，32.6%的 CSO 认为是待遇薪资太低留不住人才，29.5%的 CSO 认为是网络安全人才稀缺；20.9%的 CSO 认为是安全人才的上升通道不畅。具体分布情况如下图。



第三章 CSO 对机构安全建设的自评

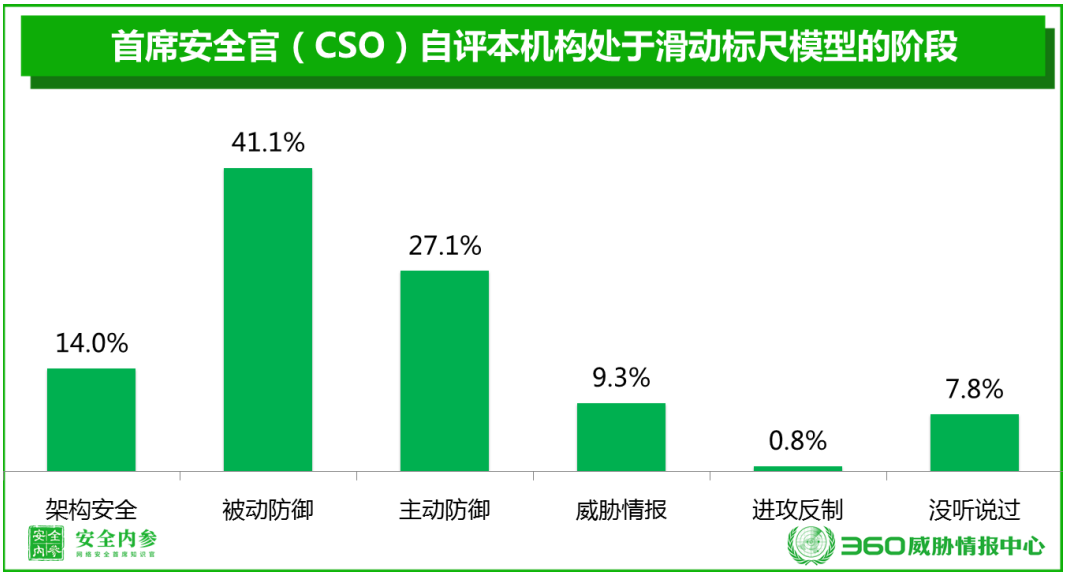
首席安全官对机构内部的网络安全建设水平与发展状况最为了解，首席安全官对自身机构的评价具有一定的意义。

本章主要从首席安全官对其自身所在机构的网络安全发展阶段和建设水平的自我评价，来分析当前国内政企机构的网络安全建设的整体水平。

一、 网络安全发展阶段

SANS 研究所的 Robert M. Lee 提出了一个动态安全模型——网络安全滑动标尺模型。该标尺模型把机构的网络安全建设水平分为五大阶段，分别为架构安全（Architecture）、被动防御（Passive Defense）、积极防御、威胁情报（Intelligence）和进攻（反制 Offense）。这五大类别之间具有连续性关系，并有效展示了防御逐步提升的理念。

本次调研要求被调研者评价自身所在机构的网络安全建设水平处于滑动标尺模型的哪个阶段。统计显示，仅有 0.8%被 CSO 认为，自己所在机构的网络安全建设达到了进攻反制阶段；而 41.1%的 CSO 认为，自己所在机构仅仅是达到了被动防御的建设阶段。认为自己所在机构能达到主动防御阶段水平的 CSO 约占 27.1%。具体分布情况如下图所示。



下面对滑动标尺模型给出的网络安全建设水平分五大阶段进行简要说明。

1）架构安全：在系统规划、建立和维护的过程中充分考虑安全防护。

2）被动防御：在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统。

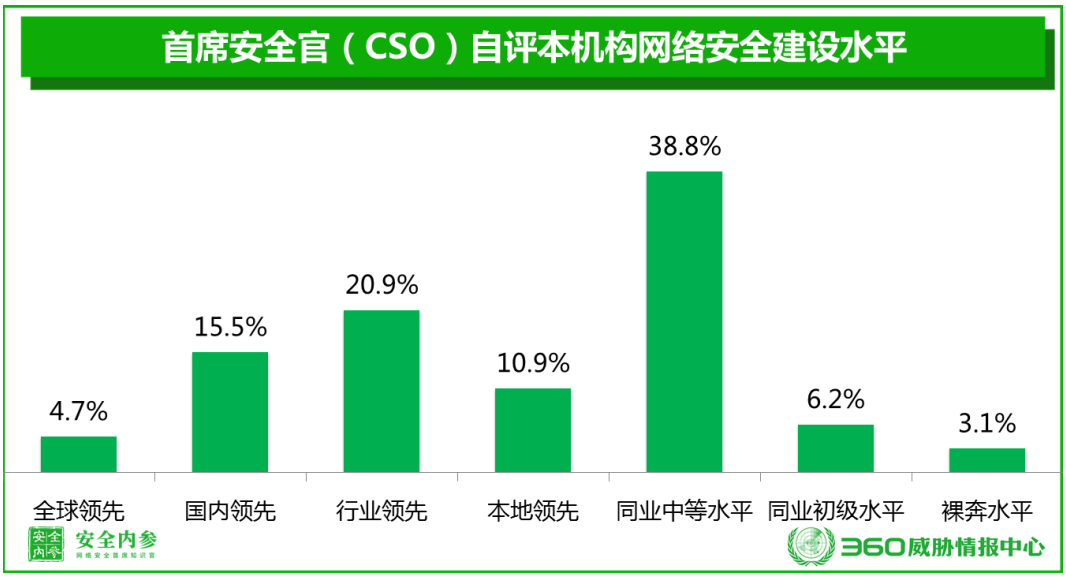
3）积极防御：分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程。

4）威胁情报：收集数据，将数据转换为信息，并将信息生产加工为评估结果以填补已知知识缺口的过程。

5）进攻反制：在友好网络之外对攻击者采取的直接行动（按照国内网络安全法要求，对于政企机构来说主要是通过法律手段对攻击者进行反击）。

二、 网络安全建设水平

对于机构自身的网络安全建设水平，不同机构的 CSO 有不同的看法。统计显示，仅有 4.7%的 CSO 认为自己所在的机构网络安全建设水平已经达到了国际先进的水平；认为自己达到了国内领先和行业领先水平的分别占 15.5%和 20.9%；认为自己只是达到了本地区内领先水平的约占 10.9%。约 38.8%的 CSO 认为，自身机构的网络安全建设水平属于行业中等水平。认为自身机构的网络安全建设只是达到了初级水平，甚至是处于裸奔水平的机构，约占 3.1%。具体分布情况如下图所示。

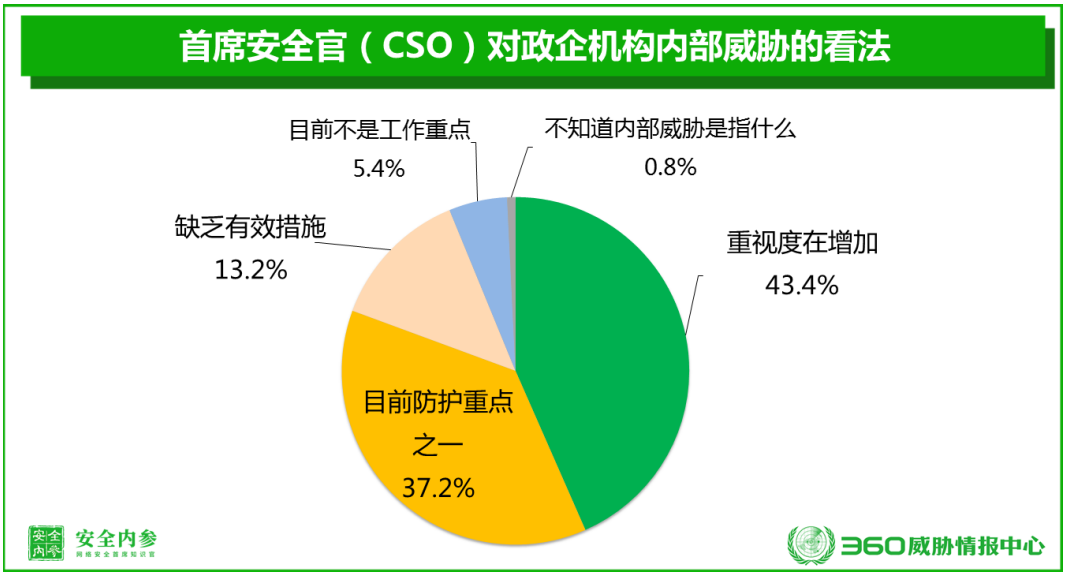


三、 对内部威胁的看法

内部威胁一般是指来自机构内部的网络安全威胁，通常是由机构内部员工（包括离职员工）的违规或内鬼行为导致的。传统的网络安全工作主要防范的是来自外部的网络安全威胁，而对内部威胁重视不够。但近年来，监测和防范内部威胁正在受到政企

机构和网络安全人员越来越多的关注。本次报告也特别就这一问题对 CSO 进行了调研。

统计显示：43.4%的 CSO 认为“内部”威胁过去不是重点，目前重视度在增加；37.2%的 CSO 认为内部威胁已经是目前防护的重点之一；13.2%的 CSO 认为，针对内部威胁缺乏行之有效的措施。具体分布情况如下图所示。



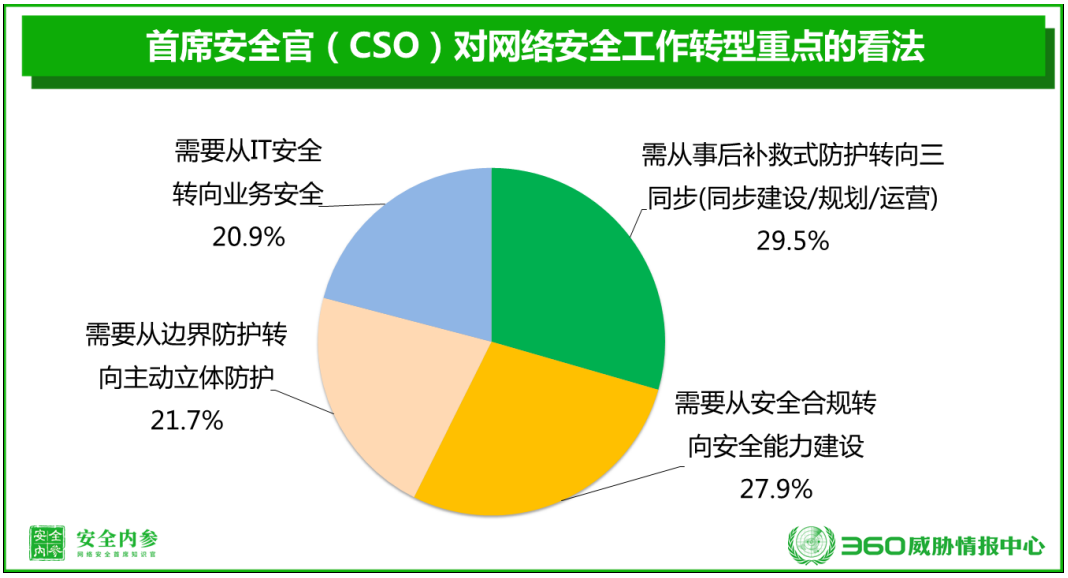
第四章 CSO 对网络安全趋势的认知

网络安全已经上升为国家战略，并且成为网络强国建设的关键核心。习近平总书记在 2014 年指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”之后，在 2018 年全国网络安全和信息化工作会议上，他又再次强调：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”

网络安全也正在发生着前所未有的转变。本章主要通过对 CSO 的调研，从网络安全工作的转型，网络安全服务的转变，以及网络安全技术的创新领域等方向展开分析。

一、 网络安全工作的转型

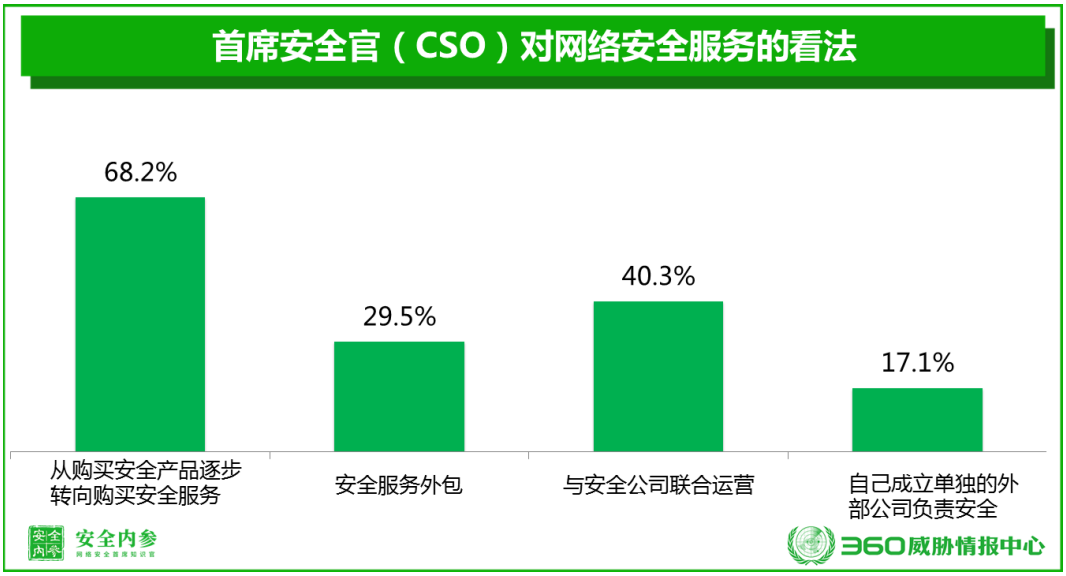
信息化的全面转型必然带动网络安全工作的全面转型。对于网络安全工作转型的重点，CSO 们首选的是“需从事后补救式防护转向三同步（同步建设、规划、运营）”，选择这一选项的 CSO 占比为 29.5%；其次是“需要从安全合规转向安全能力建设”，选择这一选项的 CSO 占比为 27.9%；此外，选“需要从边界防护转向主动立体防护”占比 21.7%；选“需要从 IT 安全转向业务安全”的占比 20.9%。



二、 网络安全服务的普及

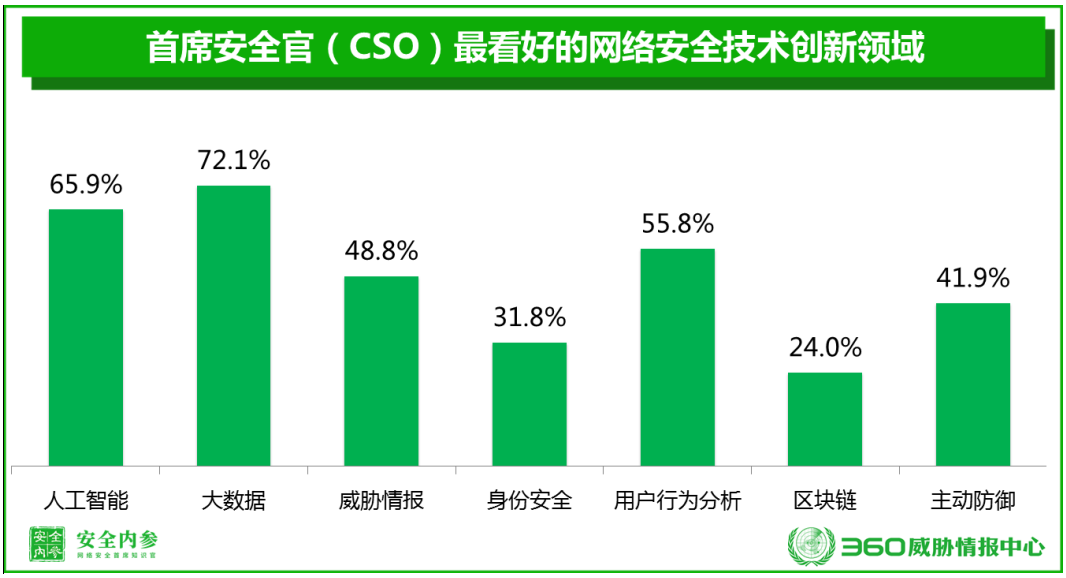
政企机构传统的网络安全建设比较注重网络安全类软硬件产品的采购。但近两年来，越来越多的政企机构开始重视网络安全服务，并将采购的重心从产品转向服务。

对于安全服务的问题，约七成的 CSO 认为，从购买安全产品逐步转向购买安全服务是未来网络安全建设的趋势；40.3%的 CSO 认为未来在网络安全建设时会与安全公司联合运营；还有 29.5%的 CSO 认为，在未来网络安全建设时会采用安全服务外包。另外，也有 17.1%的机构愿意自己成立单独的外部公司负责网络安全工作。



三、 网络安全技术的创新

时下正处于网络安全技术创新有史以来最为活跃的时期。本次研究也特别对 CSO 们关注哪些网络安全技术创新进行了调研。在被问及比较看好哪些领域的网络安全技术创新时，72.1%的 CSO 选择了“大数据”，排名第一；其次是“人工智能”，65.9%的 CSO 看好这一领域；“用户行为分析”排名第三，看好率为 55.8%。



第五章 总结

现阶段，网络安全负责人在政企机构内部的地位仍然普遍不高，行政级别低、缺少话语权是普遍存在的问题。而且近一半的政企机构目前完全没有设立 CSO 或相应的岗位，也没有考虑短期内设置这一岗位的计划。

资金投入与团队规模是政企机构网络安全能力的重要体现。八成以上的政企机构在过去两年内对网络安全的投入都有所增加。大中型政企机构的网络安全资金投入规模一般集中在 100 万元以下和 100 万-500 万元这两个层次间。在万人以上规模的政企机构中，近四成机构的网络安全团队超过 100 人。

薪资待遇、职业发展、人才供给等因素都是目前政企机构组建网络安全团队面临的“最大”的挑战。

政企机构传统的网络安全建设比较注重网络安全类软硬件产品的采购。但近两年来，越来越多的政企机构开始重视网络安全服务，并将采购的重心从产品转向服务。

对于网络安全技术的发展，CSO 们普遍最看好的三个领域是：大数据、人工智能和和用户行为分析。

附录 1　2018 中国首席安全官调查问卷

为了更加深入了解国内大型政企机构网络安全建设现状，了解中国各大政企机构首席安全官/网络安全主管的工作环境，国内权威网络安全咨询平台《安全内参》与 360 企业安全研究院联合展开此次针对中国首席安全官/网络安全主管的网络调研活动，并最终形成调研报告。

作为 ISC2018 第六届中国互联网安全大会官方合作媒体，《安全内参》获得 ISC 组委会特别授权，向每一位参与调研的首席安全官/网络安全主管赠送《走进安全》一书。

调研问卷链接：https://www.wjx.cn/jq/27296338.aspx

附录 2　安全内参

《安全内参》是专注于网络安全产业发展和行业应用的高端智库平台，依托于专业的安全团队和数千位国内外顶级的产业和行业智库和专家团队，为网络安全相关政府主管、行业、企业和机构的管理者、决策者和从业者提供全球视野、高价值的安全知识和安全智慧，致力于成为网络安全首席知识官。

做网络安全管理和决策的知识罗盘

这里有，

来自 2000 位智库和专家的智慧洞见

来自 1000 位顶级机构 CSO 的实践和经验

来自全球最前沿的产业趋势和方向

来自全球 100 家安全媒体和社区的知识精华

来自 200 家主管和研究咨询机构的决策研究

在这里，

与 10000 位政策专家、战略专家、产业专家、技术专家、行业专家和 CSO 们一起学习和分享。

安全内参
网络安全首席知识官

马上扫码，马上读懂！
关注公众号
下载APP
https://www.secrss.com