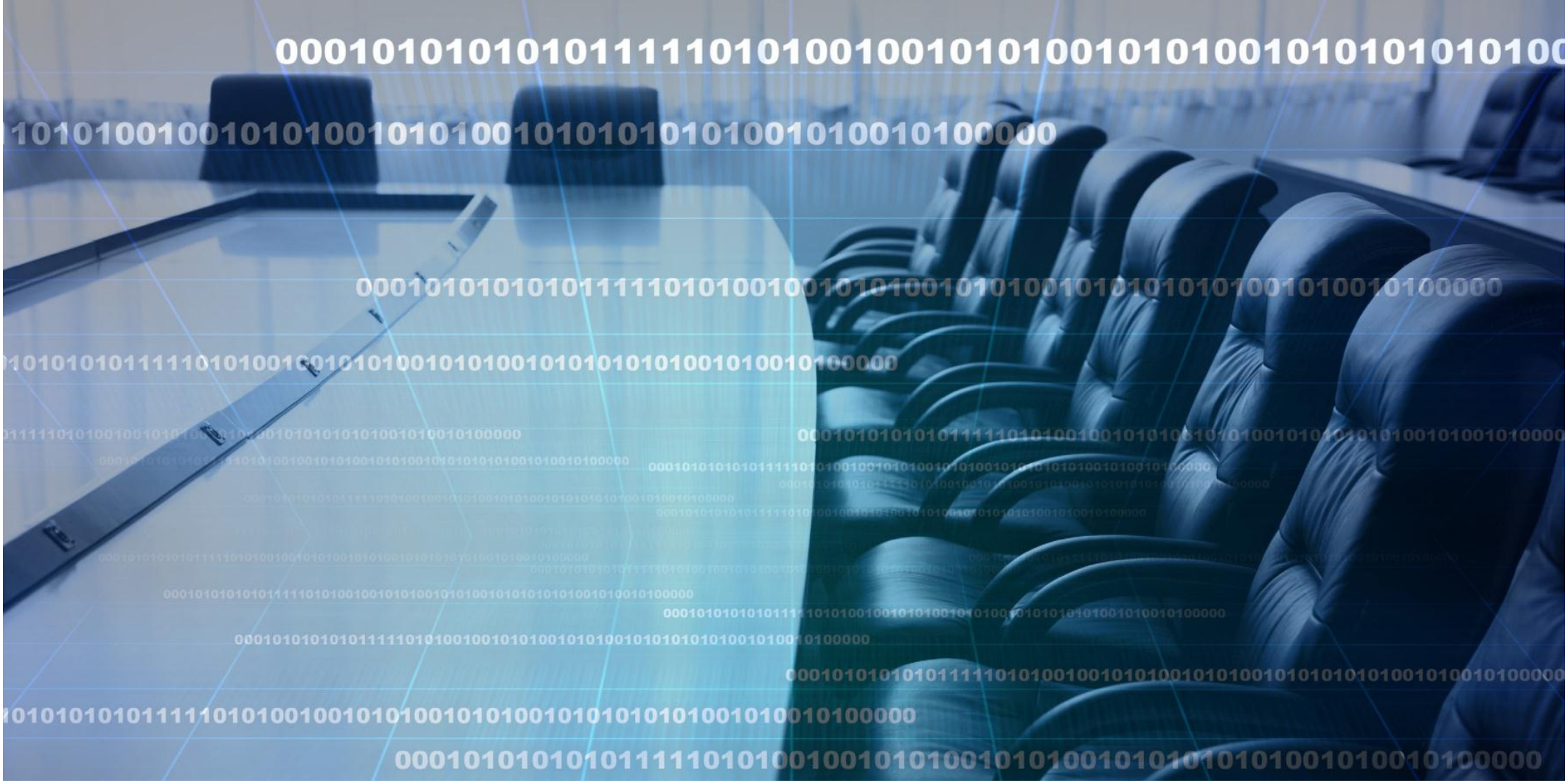


提高最高管理层的安全意识

董事会与最高管理层的网络安全观

IBM 商业价值研究院

执行报告

安全性

IBM 如何提供帮助

网络犯罪这种潜在威胁已然上升至危机水平。尽管很难准确量化，但根据估算，网络犯罪对于全球经济带来的损失很可能介于每年 3750 亿美元到 5750 亿美元之间。[1] 任何地区和行业都无法幸免。经济损失、信誉受损、国家安全问题等等，都是最高管理层需要重点关注的核心风险。从历史角度考量 IT 部门所面对的技术问题，不难发现安全已成为最高管理层亟需解决的核心运营课题，安全问题在董事会层面也不断被提出。

IBM 拥有广泛而集成的安全软件和服务组合，可满足企业预防、检测、响应和纠正安全问题方面的需求，能够帮助他们预测并及早采取行动消除网络安全风险带来的影响。

要了解有关 IBM 如何与企业携手保护数字基础设施的更多信息，请访问：**ibm.com**/security

为什么最高管理层需要关注网络安全

94% 的受访高管认为，未来两年企业有很大可能会经历严重的网络安全事件。虽然 65% 的高管高度自信，认定自己企业的网络安全计划十分完善，但仅有 17% 的受访高管认为自己企业的“网络安全受保护”- 也就是做到了最高水平的安全防范。“网络安全受保护”的企业在制定和实施网络安全战略方面取得了显著的进展。因此，这些企业能够更有效地缓解网络安全风险。从最高管理层的角度而言，“网络安全受保护”的企业更积极地参与威胁管理。他们采取跨职能合作模式，共同解决网络安全问题，他们更有可能任命并授权首席信息安全官 (CISO)，并与外部实体共享事故信息。

执行摘要

网络安全不再只是 IT 部门的问题；相反，这些问题会威胁到企业的方方面面，对业务连续性和商业信誉带来严重威胁。这些问题不仅会影响技术环境，还会蔓延至整个业务生态系统。网络安全解决方案不仅要提供技术修复，而且还要应对业务流程、控制、管理和员工行为的变化。

为深入了解高管在网络安全方面的关切和观点，IBM 联合《经济学人》智库 (Economist Intelligence Unit) 对 28 个国家/地区、18 个行业的 700 余最高层主管开展了一次调研。参与调研的高管既包括传统的最高管理层，也包括合规主管和法律顾问。本报告将深入探究高管对风险和挑战的评估意见，并确定如何使这些评估符合实际威胁情况。

网络安全十分重要，但人们往往对敌手不甚了解

2/3 的受访高管将网络安全视为必须解决的首要问题。但是，他们并不清楚哪些安全因素会带来最大的风险。54% 的受访者认为风险来自有组织的犯罪团伙。不过，许多受访者似乎过度强调了投机型“恶棍”带来的风险，而忽视了其他来源的危险，比如产业间谍、外国政府及商业生态系统的人员（员工、供应商及合作伙伴）。了解敌手有助于优化风险管理和安全解决方案投资。

协作是在网络安全斗争中取胜的关键

安全领域普遍认为，以协作方式共享事故信息，是对抗网络坏蛋的有力武器。事实上，众所周知，最成功的网络犯罪分子通过“黑暗网络”(dark web) 开展合作，共享信息。“黑暗网络”是指互联网不良的一面，一些动机险恶的用户匿名在此开展恶意勾当。

65%

的受访高管非常自信，认为自己的网络安全计划十分完善，但仅有 17% 的受访者表现出最高水平的准备工作和实施能力。

68%

的 CEO 不愿意对外共享安全事故信息，但外部协作却是抵御网络犯罪的有力武器。

60%

的 CFO、CHRO 和 CMO 在网络安全威胁管理活动方面的参与度最低，但却掌管着最令黑客垂涎的数据。

不过，“好人”对于协作却更为谨慎。在我们的调研中，超过 2/3 的 CEO 表示不愿意对外共享企业的网络安全事故信息。同样值得注意的是，企业内部职能部门之间的协作也很薄弱，首席人力资源官 (CHRO)、首席市场官 (CMO) 和首席财务官 (CFO) 这三大高管角色之间的协作尤为不畅，而他们却掌管着最令黑客垂涎的数据（分别是员工信息、客户信息和财务信息）。同样，也是这三类高管对企业网络安全计划的信心最低，他们往往认为这样的计划不够完善或者无法正确实施。

组织可以向做好完备防御的企业学习，并从中受益

“网络安全受保护”的企业实施全方位的网络安全计划，检测违规，防止事故，缓解风险。最能说明问题的是，这些企业设立了信息安全办公室，任命首席信息安全官 (CISO) 并实施跨职能治理模式，使董事会、管理层和员工都能参与进来。另外，他们也更愿意开展协作，和外界共享安全事故情报。

高管关心的问题

准备提升网络安全能力的企业可以效仿网络安全精英。首先，要弄清楚哪类群体带来的风险最大，并评估企业在风险防范方面的努力程度。接下来，提升整个企业的安全意识，推动建立风险文化。创立网络安全治理、持续监控、事故报告和应对准备制度。最后，通过内外协作管控威胁，保护企业最宝贵的数字资产。在 IT 基础结构和业务流程中强制实施安全标准。

高管的网络安全观点

重要观点

IBM 在 2015 年的全球最高管理层调研中，对 5,600 多位高管进行了采访，内容涵盖众多战略问题和新兴趋势。[2] 68% 的受访者将 IT 安全列为最关注的问题，认为技术很可能会在未来三至五年对业务带来彻底变革（见图 1）。提高对新兴技术中 IT 安全风险的关注度十分重要；但是，现有的旧基础架构以及与供应商、客户、合作伙伴的集成点同样存在安全隐患。

出于这个原因，了解可靠的网络安全计划应当包含哪些要素至关重要。在我们的调研中，绝大多数高管强烈赞同 IT 安全防御包含四个重要组成部分：

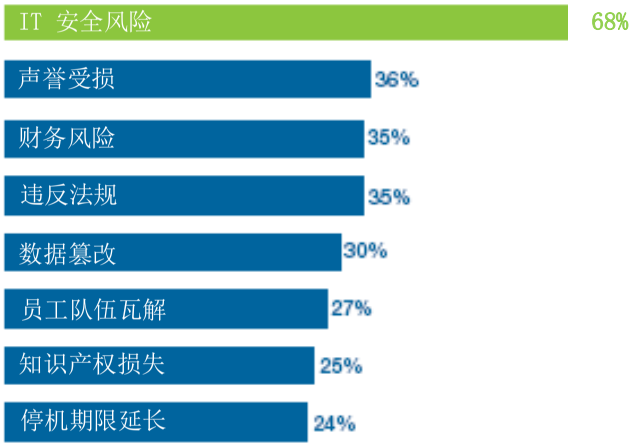
- 预防（77%）：缓解潜在威胁的战略、计划、培训和技术；
- 检测（76%）：监控和检测违规行为的实时系统和流程，以及执行根本原因分析的取证分析能力；
- 响应（74%）：取证分析、沟通、负责人、预先编写的声明、根据分析结果采取的行动；
- 补救（78%）：落实计划，快速解决安全问题，消除安全短板（技术、流程、培训等）。

.....但这对我有什么影响？

51% 的受访高管认为，发生违规时，有 1/4 的可能会对企业产生严重影响。他们对于风险有着深刻的认识，据近期的一项调研表明，他们“估计在未来 24 个月内，发生数据违规的可能性达到 22%，至少涉及 10,000 条记录。”[3]

图 1

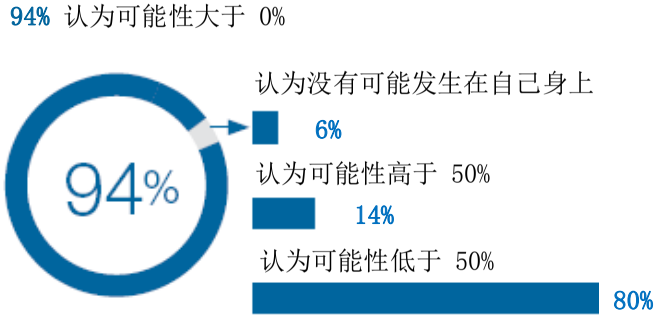
最高管理层对于未来 3 至 5 年技术风险的看法



来源：IBM 商业价值研究院。

图 2

最高管理层对于重大违规可能性的看法



来源：IBM 商业价值研究院。

另外 49% 的高管对于违规可能性的看法大相径庭。13% 的高管已然经历过重大违规，或者认为重大违规不可避免（分别占到 5% 和 8%）。出人意料的是，6% 的受访者表示，他们认为不可能发生会对企业产生严重影响的违规。（见图 2）。

虽然就总体而言，高管对于违规可能性的观点各不相同，但 CISO 处于网络安全前线，因此对此更为重视。事实上，很多 CISO 认为威胁形势十分严峻，甚至感觉会输掉这场“战争”。据 2014 年 IBM CISO 调研发现：

- 83% 的 CISO 表示，过去三年外部威胁带来的挑战不断攀升(42% 表示外部威胁显著增加)；
- 59% 的 CISO 强烈赞同，攻击者的水平超过了企业的防御水平；
- 40% 的 CISO 表示，复杂的外部威胁是面临的首要挑战[4]。

无可否认，评估安全违规对企业带来严重不利影响的可能性大小既是科学也是艺术；鉴于威胁发动者、攻击动机、行业和地理差别以及特定企业中现有安全缺陷特性的多样性，这种评估就显得尤为重要。或许人们最担心的是，可能经过数月乃至数年才会发现事故。到那时，往往已经为时过晚，因为损失很可能已经酿成。

哪些方面存在 IT 风险？

当问及他们对于 IT 基础架构特定风险的看法时，57% 的高管认为员工移动设备，也就是员工自带设备 (BYOD) 所带来的风险最大，54% 的高管将票投给社交媒体/渠道系统（如网上冲浪以及在工作时回复电子邮件）（见图 3）。企业移动、云和业务生态系统集成点（合作伙伴/供应商集成点）同样也被视为存在高风险。不过，旧基础架构也会带来很多安全风险，不容忽视。相较于其他旧漏洞，移动设备所产生的事故数目依然很少，因此高管很可能是将远虑当成了近忧。

过去几年发生的重大违规表明，一些旧基础架构组件存在较高的风险隐患，尤其是：

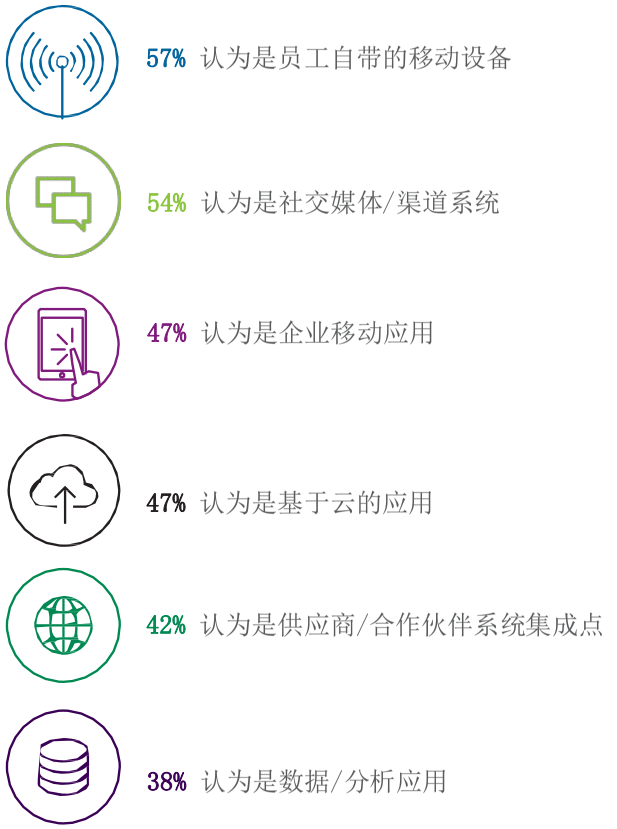
- 员工和管理层缺乏安全意识；
- 尚未修复一些常见漏洞（例如，未及时更新软件补丁）；
- 未定期实施或更新基础保护，如防病毒程序和恶意软件检测。

敌人是谁？

知己知彼，百战不殆。因此必须了解不同的威胁发动者、他们的攻击方式以及攻击复杂度，所有这些信息均可用于评估风险级别。安全专家可根据事故监控和分析有效了解威胁发动者的一系列活动。动机和目标各异的攻击发动者不断寻找各种漏洞。他们当中，有些是“过失攻击者”，完全不存在发动“高级持续性威胁”(ATP) 的恶意目的，而 ATP 则阴险得多，而且具有资金和资源支持，会带来更高的风险、更严重的影响。

图 3

最高管理层对于*风险最高的 IT 基础架构领域的看法*



来源：IBM 商业价值研究院。

我们要求受访者指出哪三类攻击者是企业面临的最主要风险威胁来源。70% 的高管将流氓攻击者选为最高风险来源，38% 的高管将其选为最有威胁的攻击者。有组织犯罪集团紧随其后，这表明高管对这些攻击者所带来的风险看法一致。知识产权保护显然是担心的问题，因此行业竞争对手被视为第三大最主要的威胁来源。

高管眼中的威胁可能与各种威胁来源的潜在影响并不相符。由于攻击意图、攻击手法的老练程度以及承担的事故责任不同，攻击者的威胁特征也各不相同。流氓个人攻击者的进攻手段比较粗浅、资金有限而且攻击的往往是一些易于防护的熟知漏洞，因此他们造成的威胁相对较低。相较于消除更老练的威胁来源（如国家政府、产业间谍及有组织的犯罪团伙），过于专注流氓个人攻击者群体很可能使安全投资无法得到应有的回报，恶意的内部人员及其他外部代理商（员工、供应商、合作伙伴）所带来的风险可能会更大。

IBM 2015 年“网络安全情报指数”报告提供的事故分析数据发人深省：31.5% 的数据违规由恶意内部人员造成，23.5 % 因内部人员出差错或未遵循流程和政策而无意中产生数据违规或信息披露导致。[5] 在本次调研中，仅有 32% 的高管将目前/前雇员选入最主要的三大威胁，只有 8% 将目前/前供应商选入最主要的三大威胁。事故数据分析可以深入洞察各种威胁来源，从而提高风险意识，帮助高管更明智地确定安全战略重点。

治理与协作

公开透明地在企业内外部开展协作和分享事故信息，是应对网络犯罪的有效之策。违规取证分析可揭示入侵方法、手段及来源。在企业的各职能部门之间以及与企业外部共享相关信息，有助于汇集集体智慧，深入洞悉威胁来源及其攻击方法，从而形成有效的解决方案。

高管应积极参与企业内部的网络安全合作，企业应当在必要时和业务生态系统中的其他成员（比如供应商、合作伙伴甚至行业竞争对手）开展相关合作。最成功的网络犯罪分子积极开展合作，在黑暗网络上分享他们发现的漏洞信息。而由于协作不畅，企业在抵御网络犯罪方面始终处于被动挨打地位；网络犯罪分子却通过合作，到处兴风作浪，无孔不入。

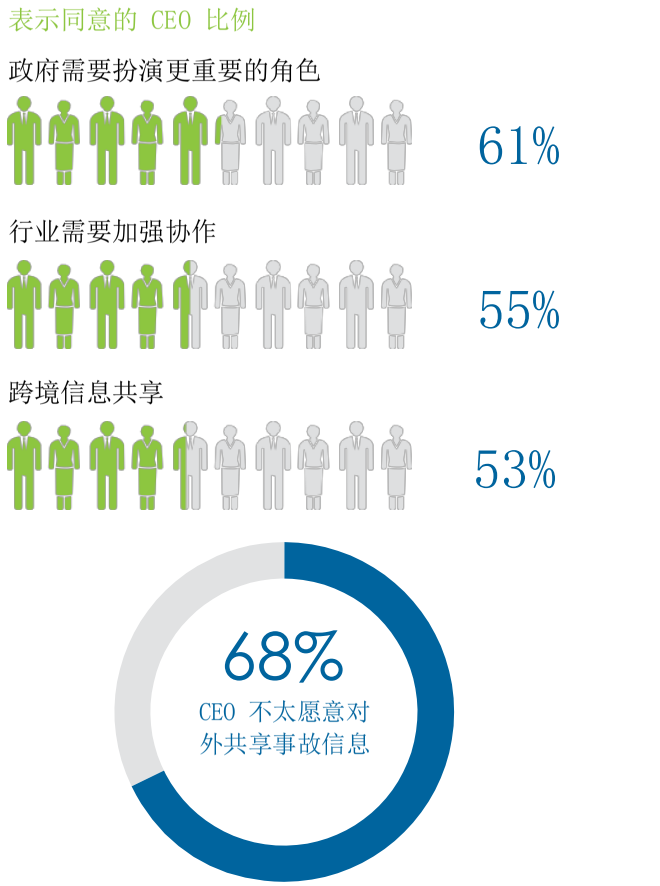
CEO 二元论

在对外共享事故信息方面，CEO 似乎有些矛盾。尽管做出这种决定可能会感到不安，但只要掌控有度，共享事故信息可带来积极的效果。

在谈到外部参与方在打击网络犯罪方面所扮演的角色时，61% 的 CEO 认为政府需要扮演更重要的角色，55% 的 CEO 表示必须加强行业协作，53% 的 CEO 指出跨境信息共享很有必要（见图 4）。

图 4

CEO 一方面比较看重获得外部支持，但又不太愿意开展外部协作



来源：IBM 商业价值研究院。

然而，当我们询问 CEO 希望在何种程度上向内外利益相关方披露网络安全事故信息时，68% 的 CEO 表示不赞同对外共享事故信息。不过，加强外部协作可加速形成集体智慧，深入认识威胁来源及其策略。领导层需克服这种抵触情绪，适当地与通过审查的外部各方共享信息，抓住机遇，利用分析，运用不断加强的成熟认知能力，强化并自动执行安全解决方案，缓解风险。

信心矛盾体

65% 的受访高管表示，他们对于自身企业的网络安全计划完善度很有信心。但是，并非所有高管均持有相同的观点。77% 的首席风险官 (CRO) 和 76% 的首席信息官 (CIO) 表示，企业的网络安全计划十分完善。不过，持有同样看法的 CEO 仅略高于上述比例的一半。与 CEO 持有相同观点的首席市场官、首席财务官和首席人力资源官的“信心指数”不到 CRO 的一半（见图 5）。原因主要在于，这三类主管是客户、财务和员工数据的最终掌管者，而这些是最令网络犯罪分子垂涎的信息。

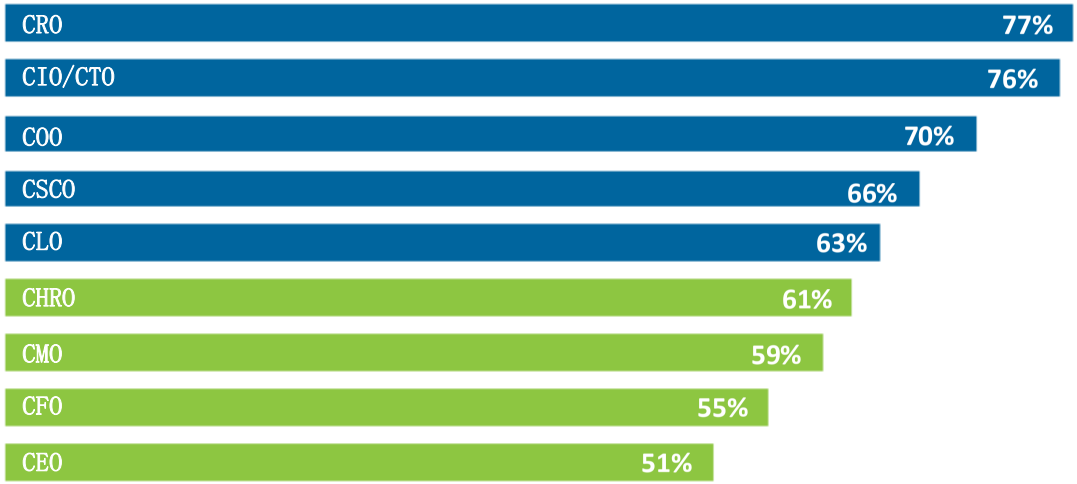
CIO 和 CRO 可能因职务原因而自信度较高。从历史上而言，网络安全一直主要由 IT 部门负责，CIO 可能认为他们解决了技术层面问题，对整个企业网络、应用及笔记本电脑和移动设备远程访问实施了有力的保护措施。假设这些保护措施足够有力，企业也不能因此而忽视业务流程、信息管理及第三方解决方案领域。云正是这方面的典型，很可能造成最高管理层对于网络安全的不同看法。企业对于利用第三方云产品的判断失误（未能与 IT/安全部门合作，或者未考量供应商的网络风险状况）势必会增加风险。

与此类似，负责评估和规划企业风险的 CRO 很可能已将网络安全风险纳入企业风险管理 (ERM) 框架。但是，这并不一定能转化为实际的风险“防御方案”。ERM 的目标是制定事后风险事件响应计划。应当针对具体的战术步骤审视计划，确保通过增强安全性而缓解风险。CRO 可能自认为制定了计划和措施，但企业的最高管理层同事需要的是切实应对各类具体风险。

图 5

网络安全计划优势（按角色划分）

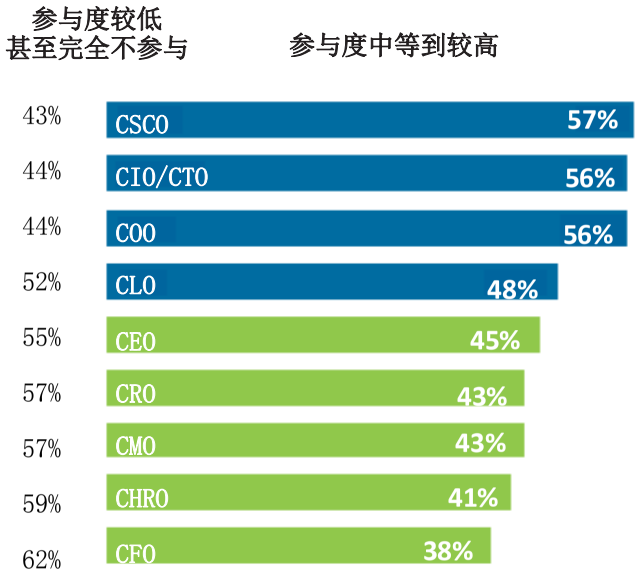
表示企业具备完善的网络安全战略的受访高管的比例。



来源：IBM 商业价值研究院。

图 6

最高管理层的网络安全威胁管理活动参与度（按角色划分）



来源：IBM 商业价值研究院。

最高管理层协作 - 从 IT 部门到业务部门

最高管理层一致认为建立成熟的安全态势越来越重要，IT 部门和业务部门负责人尤其表示认同。我们研究了具体的调研问题的回答，确认这些角色的看法的一致性。

在网络安全计划是否实现整个最高管理层共同参与和协作这个问题上，CIO 的信心指数几乎是 CEO、CFO、CMO 和 CHRO 的两倍。

CIO 之所以信心满满，很可能是因为从 IT 角度而言，在了解和采取措施保护 IT 部门认定的最高风险领域取得了长足进步。不过，CIO 的关注重点则更多集中于原有的 IT 系统（如网络、运营系统和财务系统），很少着眼于市场、人力资源和供应商/合作伙伴生态系统。

尽管 CIO 表达了信心，但 69% 的高管受访者表示，网络安全计划未能充分体现最高管理层的集体协作。就具体的角色而言，近 3/4 的 CEO、CHRO、CMO 和 CFO 指出，他们认为网络安全计划并未将他们纳入跨职能合作范畴。

在重点关注于网络安全计划战术执行方面的问题中，我们询问职能高管在最高管理层会议上的参与安全威胁管理活动的程度（见图 6）。近 60% 的职能高管表示，他们认为自己并未在最高管理层会议期间参与过这样的主题。按角色分类，57% 的 CMO、59% 的 CHRO 及 62% 的 CFO 表示，他们并未在最高管理层参与这些话题和讨论。

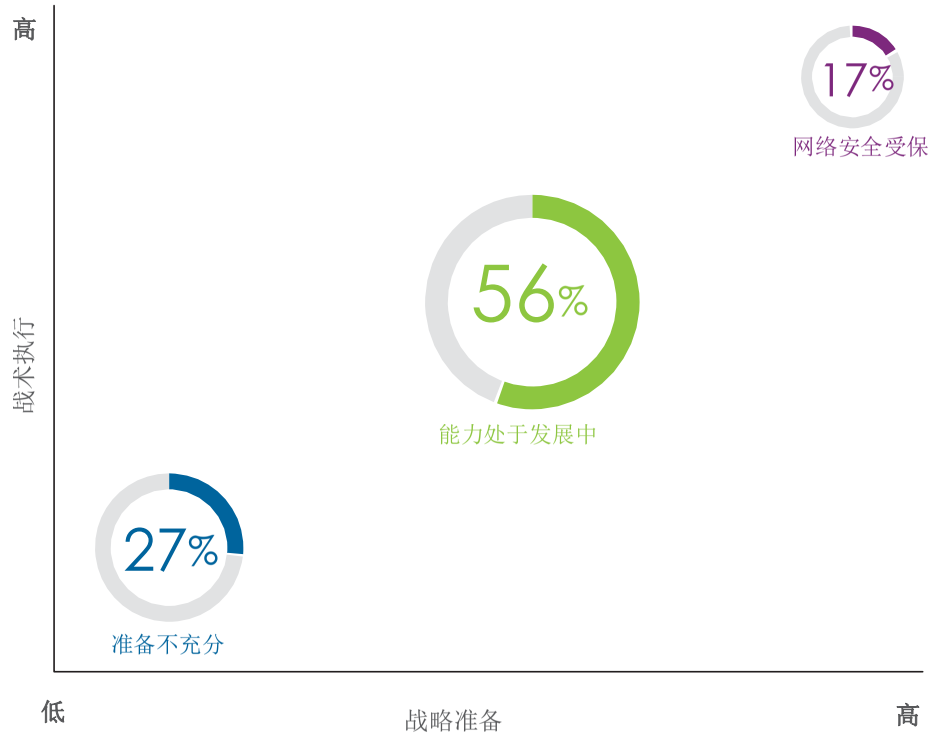
考虑到最高管理层级别的互动是受访高管与同事开展网络安全讨论的主要对话场所，所以这三类高管的参与度如此之低着实令人担心。

网络安全受到保护

我们分析了有关网络安全的战略和战术准备情况方面的一些问题的回答。通过分析，我们将受访者归入三个组。其中一组称之为“网络安全受保护”组，这组中的企业所具备的网络安全能力最高，已经实施安全战略，并在战术层面执行计划，从而缓解网络风险；通过研究这组企业，我们可以获得网络安全方面的一些深入洞察。该群体占调研受访者人数的 17%，具有极大的差异化优势（见图 7）。

图 7

高管网络安全能力模型



来源：IBM 商业价值研究院。

网络安全能力模型

一组受访企业的最高管理层表现出最高水平的网络安全防御能力，准备工作也做得最好。我们将这一组称为“网络安全受保护”组。他们对于风险的态度最为乐观，认定需要开展跨职能治理，并且比其他各组更倾向于将这些风险纳入企业的 ERM 计划中。最重要的是，这一组企业中最高管理层参与方式的均衡度和协作度均较高。

我们对调研中用于确定网络安全计划完整性和计划战术执行度的问题进行了分析。每个问题均要求受访者对自身企业进行评分，按 1 至 5 分划分等级，1 代表“完全无效”，5 代表“极其有效”，分别对每项要素进行评分。

该能力模型的战略维度需要在三个重点领域不断发展：

1. 建立安全治理模型，包含企业级的协作；
2. 发现并保护关键数据和应用，以及；
3. 制定并实施有效的应对计划。

成熟度模型的战术维度则表示受访者对网络安全计划各个要素（共四个）有效性的评价。

图 8

CISO 角色普遍性（按能力组划分）

设立信息安全办公室并任命首席信息安全官 (CISO)

来源：IBM 商业价值研究院。

网络安全团队通常会选择 CISO 作为领导者

为加强网络安全能力，需要设立信息安全办公室并任命 CISO。“网络安全受保护”的企业采取这项措施的可能性比其他企业要高出 2.5 倍（见图 8）

在“网络安全受保护”的企业中，最高管理层以团队形式开展协作

“网络安全受保护”企业的高管了解整体跨职能方法对于实现网络安全的价值。他们认识到参与业务问题的重要性，相较于准备不充分的企业，他们在网络安全计划中包含最高管理层跨界协作内容的可能性要高出 5 倍。“网络安全受保护”的企业更有可能将最高管理层协作纳入网络安全治理（见图 9）。另外，他们在治理网络安全方面也比其他组更出色，61% 的高管表示最高管理层会议经常讨论网络安全主题，而其他组的这一比例仅占 31%。最重要的是，我们发现不同角色的参与度同样高于平均值，尤其是首席市场官、首席人力资源官和首席财务官。

在董事会层面，“网络安全受保护”的企业（56%）将网络安全提上一般议事日程的可能性是其他企业（27%）的近两倍。董事会成员不必成为网络安全专家；但是，他们对网络安全风险的了解必须至少达到以下程度：

- 要求管理层向董事会描述所部署的适当控制手段，并保证董事会时刻掌握最新动态；
- 定期监控控制措施，确保它们按预期正常运行；
- 要求迅速报告重大事故。

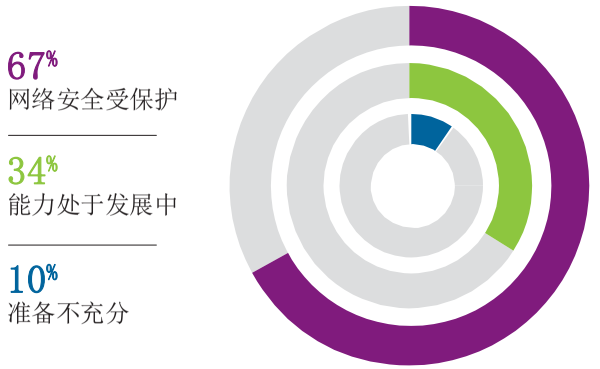
“网络安全受保护”的企业与外部各方的协作更紧密

成功的网络犯罪分子通过彼此协作而获益，因此企业之间就安全管理和事故开展协作，同样有助于降低风险。网络犯罪分子开展协作的形式如下：一方发现薄弱环节，将发现结果出售给其他方以发动攻击。“网络安全受保护”企业的 CEO 更愿意与外部各方共享事故数据。他们与行业竞争对手开展协作的可能性是其他组的三倍，与第三方安全服务公司和供应商/合作伙伴开展协作的可能性是其他组的两倍。为抵御风险，高管应考虑外部协作的价值，将其作为一种有力的进攻性战术。有关攻击者、攻击来源和战略的事故数据在不断增长。企业开展协作共同了解网络犯罪分子及其活动的程度越高，部署风险缓解解决方案的针对性也越高。

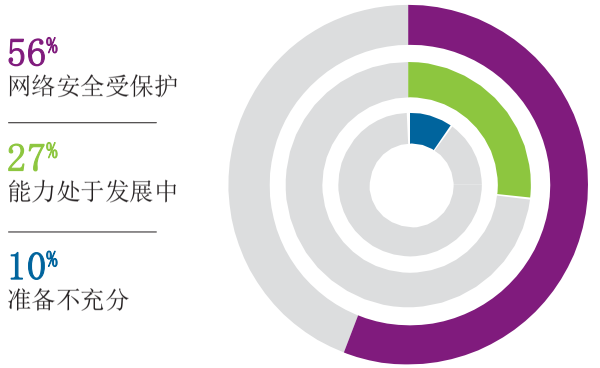
图 9

协作普遍性和董事会透明度（按能力组划分）

最高管理层协作已纳入网络安全计划（治理）



网络安全主题经常提上董事会议事日程



人力资源主管不可或缺的网络安全作用

仅有 57% CHRO 表示已经面向员工推出了网络安全培训。身为最令黑客垂涎的员工个人敏感信息的掌管者，CHRO 应处于企业网络安全工作的最前沿。他们的职责包括：

保护员工个人敏感信息，HR 需要具备保护员工个人敏感信息及业务流程的治理权，从招募到离职的整个生命周期中使用并维护这些数据。

网络安全培训和实施
访问企业系统的个人移动设备日益普遍，带来了新的漏洞。人力资源主管可以帮助制定明确的安全政策以及惩戒措施（包括开除）。

从招聘到离职的实践
HR 可协助各利益相关方规划清晰的职业角色和职业道路，然后帮助完成搜寻和遴选人才的流程，包括在遴选候选人时考虑安全风险，防止无意中招入可能成为“内部”威胁的人员。HR 应帮助评估职位敏感度，并根据需要在进行这些职位的招聘时额外进行详细审查。

建议：从 2016 年开始，最高管理层必须参与网络安全工作

了解风险

- 评估行业、地域和业务生态系统/合作伙伴以确定风险；
- 开展安全风险评估，并对超过一年的各项评估进行更新；
- 确定哪些领域可能成为威胁来源，相应地进行投资以采取防范措施；
- 酌情将安全评估纳入企业风险计划；
- 开展强制的员工教育和培训，定期更新培训内容，严格实施合规流程。

协作、教育和支持

- 建立安全治理模型和计划，鼓励企业范围的协作；
- 支持 CISO 行使管理整个企业信息安全风险的职责，最高管理层要起到率先垂范的作用；
- 在最高管理层和董事会议事日程中定期讨论网络安全问题，至少要求风险、财务、市场、人力资源和供应链高管参加会议；
- 编制基础材料，开展高管层面的培训；
- 邀请最高管理层参与制定事故响应计划，并与董事会共享以征求意见。

谨慎而迅速地管理风险

- 实施持续安全监控软件，构建或利用第三方安全服务进行事故取证；
- 与通过适当审查的外部机构（如竞争对手、供应商/合作伙伴及安全专家）共享事故数据，利用威胁事件的分析结果，持续保护环境安全；
- 确定企业的数字资产（即数据、应用、系统和基础架构），根据风险级别，针对每一项资产制定风险缓解计划；
- 制定并实施网络安全政策，包括员工、合同工和供应商的工作场所行为，涵盖移动设备管理，尤其是员工的移动设备 (BYOD)；
- 将网络安全作为业务流程和决策的固有组成元素。

CISO 应发挥怎样的作用？

在企业、政府和非盈利机构，在组织中设立 CISO 或相应职能职务已然成为标准。CISO 角色对于大型组织运营至关重要，因为安全性变得极为重要，单凭 CIO 一己之力很难完成。

自 2006 年以来，设立 CISO 职务的组织数目稳步上升，年增长率约为 10%。2006 年仅有 22% 的组织表示设立了 CISO 职务，2011 年比例上升至 80%。[6] 平均而言，在参与本次调研的所有高管中，71% 的高管表示所在组织设立了 CISO 职务。近 80%“网络安全受保护”的企业（参见第 11 页的侧边栏“网络安全能力模型”）设立了 CISO 职务，组织 CISO 的平均任期为近两年。

在董事会层面，高层希望 CISO 能够清晰地说明并量化企业所面临的风险。而在最高管理层，CISO 则需要制定并执行全面的网络安全框架，从而缓解风险。

更多信息

欲获取 IBM 研究报告的完整目录，或者订阅我们的每月新闻稿，请访问：ibm.com/iibv。

从应用商店下载免费“IBM IBV”应用，即可在手机或平板电脑上访问 IBM 商业价值研究院执行报告。

访问 IBM 商业价值研究院中国网站，免费下载研究报告：http://www-935.ibm.com/services/cn/gbs/ibv/

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察力和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

IBM 商业价值研究院

IBM 商业价值研究院隶属于 IBM 全球企业咨询服务部，致力于为全球高级业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。

关于作者

Diana Kelley 现任 IBM 安全事业部的高管安全顾问 (ESA) 兼 IBM 安全新闻编辑部经理。身为 ESA，她利用自己超过 25 年的 IT 安全经验，为 CISO 和安全专业人士提供建议和指导。她一直参与编写 IBM X-Force 报告，经常在“安全情报”博客上发表思想领导力文章。她目前是 IANS 研究院的教学人员，并为 InfoSec World 的顾问委员会和妇女高管论坛的内容委员会提供服务。Diana 经常参加安全会议并发表演讲，被《纽约时报》、MSNBC.com、《信息安全杂志》和《华尔街日报》等多家媒体誉为安全专家。她还与人合著了 Cryptographic Libraries for Developers 一书。Diana 的联系方式为 drkelley@us.ibm.com。

Carl Nordman 现任 IBM 商业价值研究院网络安全和金融转型研究负责人，负责开展两个领域的基础研究。他领导多项研究，揭示当前战略问题的趋势和观点。Carl 拥有 25 年以上的金融风险和欺诈领域从业经验。他此前曾担任 IBM 咨询服务方面的职务，为《财富》1000 强企业的 CFO 提供咨询服务，以客户经理的身份为多家客户运营财务会计 BPO 服务。Carl 的联系方式为 carl.nordman@us.ibm.com

合作者

John Lainhart（IBM 全球企业咨询服务部公共部门合伙人兼网络安全与隐私服务领域负责人）、Gretchen Marx（IBM 安全事业部 IBM 安全产品组合战略项目总监）、Lisa van Deth（IBM 安全事业部活动和思想领导力战略项目市场经理）。

致谢

Peter Allor（IBM 安全事业部高级安全战略师）、Michelle Alvarez（管理安全服务威胁研究员、出版人和编辑人）、Chuck Carney（IBM 安全事业部安全服务副总裁）、David Jarvis（IBM 应用洞察和市场洞察中心经理）、Bob Kalka（IBM 安全事业部战略客户和支持副总裁）、Charles Kolodgy（IBM 安全事业部 IBM 安全战略师）、Jason Kravitz（IBM 网络安全系统和服务技术线专家）、Christopher Poulin（IBM 安全事业部 X-Force 研究战略师）、Michaela Santa Barbara（安全咨询与系统集成项目总监）；还有《经济学人》智库，感谢他们协助管理调研数据的收集工作。

备注和参考资料

1 “Net Losses:Estimating the Global Cost of Cybercrime," June 2014.Center for Strategic and International Studies.http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/ rp-economic-impact-cybercrime2.pdf

2 “Redefining Boundaries:Insights from the Global C-suite Study."IBM Institute for Business Value.November 2015.http://www-935.ibm.com/services/c-suite/study/study/

3 2015 Cost of Data Breach Study:Global Analysis.Benchmark research sponsored by IBM, independently conducted by Ponemon Institute LLC, May 2015.Page 20, figure 15.http://www-01.ibm.com/common/ssi/cgi-bin/sialias?subtype=WH&infotype=SA&htmlfid=SEW03053 WWEN&attachment=SEW03053WWEN.PDF

4 “Fortifying for the future:Insights from the 2014 IBM Chief Information Security Officer Assessment."IBM.December 2014.www.ibm.com/ibmcai/ciso

5 IBM 2015 Cyber Security Intelligence Index - https://securityintelligence.com/ economic-espionage-the-global-workforce-and-the-insider-threat/

6 PricewaterhouseCoopers' annual information security survey, 2011, 2006

IBM 全球企业咨询服务部
Route 100,
Somers, NY 10589

2016 年 3 月
美国出品

国际商业机器中国有限公司
北京市朝阳区北四环中路 27 号
盘古大观写字楼 25 层
邮编：100101

GBE03738-CNZH-06