认知时代的网络安全

率先建立数字免疫系统

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，网络犯罪给全球经济造成的损失在每年 3750-5750 亿美元之间。没有地区或行业可以置身事外。IBM 拥有广泛的集成式安全软件和服务组合，可满足企业在预防、检测、响应和纠正安全问题方面的需求，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。IBM 安全事业部帮助客户建立安全免疫系统，并由分析系统、实时防御系统以及公认的专家提供强大的支持。要了解有关 IBM 如何与企业携手保护数字基础架构的更多信息，请访问：**ibm.com**/security

在充满挑战的时代培养新能力

安全领导正在努力弥补三个方面的能力欠缺 – 情报、速度和准确性。一些企业开始研究认知安全解决方案的可能性，以便填补这些缺口，主动预防风险和威胁。人们对认知技术抱有很高的期望。在我们的调研中，57% 的安全领导相信认知技术能够有效抵御网络犯罪。22% 的受访者已经开启网络安全认知时代之旅，他们认为自己对网络安全很了解、很熟悉，而且具备所必须的资源。我们将这个群体称之为“捷足先登型”。要开启认知安全之旅，就必须研究自己的弱点，这将决定如何运用认知技术扩充自己的能力，以及如何为利益相关方制定教育培训和投资计划。

执行摘要

网络安全的状况正在经历拐点。安全风险程度和安全事件数量呈指数级增长，安全运营团队疲于应对，苦不堪言。威胁形势瞬息万变，各种威胁的复杂度越来越高，数量越来越大，传统方法已完全无法有效应对。安全事故和安全违规的影响越来越大，伴随而来的是经济损失和安全风险迅速蹿升。许多企业因缺乏具备相应技能的安全专家，处境更加窘迫。所有这些压力都使得企业更难维持良好的数字免疫系统，因此无法保护自身的安全。

在本报告中，我们采访了 35 个国家或地区 18 个行业中的 700 位首席信息官 (CISO) 和其他安全领导。我们的目标是揭示这些领导所面临的挑战、他们的不足以及正在采取哪些计划来弥补这些不足之处。我们还希望了解他们对于认知安全解决方案的看法 – 他们认为这些解决方案有多大帮助，他们对于实施这些解决方案的准备情况以及存在哪些阻碍因素。

我们发现安全领导所面临的挑战主要是威胁越来越复杂，而他们无法快速加以应对。这些领导担心安全事故会严重影响目前的业务运营以及将来的企业声誉。安全领导感觉到自己在保护网络和数据安全以及迅速作出智能威胁响应方面的效率并不高。但是，他们希望在未来几年内弥补这些缺陷。获得合适的资源解决这些问题非常困难。面对越来越高的成本和越来越严重的安全技能资源短缺情况，安全领导希望能够更好地向业务领导证明安全投资的合理性。

目前和未来所面临的**主要网络安全挑战**是**缩短响应和解决事故的平均时间**。

57% 的安全领导认为**认知安全解决方案**能够有效**抵御网络犯罪**。

他们希望在接下来 2-3 年使**实施认知安全解决方案**的专家数量**增加三倍**。

随着企业收集越来越多的安全数据，应用越来越多的分析功能，不断增加的工作量即将达到通过人工方式进行处理的极限。一些企业希望通过认知安全解决方案来应对这种状况，帮助弥补在情报、速度和准确性方面的缺口。尽管安全认知技术还处于初级阶段，但人们对其潜力抱有很大的希望并持乐观态度。我们的调研受访者表示，他们希望从认知安全解决方案中获得的主要收益包括：提高威胁检测速度，改进响应决策能力，显著缩短事故响应时间，增强在辨别是安全事件还是真正事故方面的信心。尽管前景光明，但要大范围采用这种解决方案，仍需要进行大量的教育培训和准备工作。

我们在调研中发现了一个在安全解决方案方面“捷足先登，率先进入认知时代”的群体。我们在研究安全有效性、对认知的准备情况和认知度时，发现了一些充满热情的安全领导，他们认为自己的企业已经做好充分准备，可以立即进入安全解决方案的认知时代。总体而言，这些领导往往更熟悉认知解决方案，对自己企业的安全防御能力以及减少资源获取障碍方面有更强的信心。

随着认知安全解决方案越来越成熟，应用越来越广泛，任何企业都将能够从中受益。如果您认为自己的企业已经做好准备，并决定开启认知之旅，那么第一步就是确定自己希望在哪些薄弱环节运用认知安全解决方案。然后，了解可能的用例，并与自己的薄弱环节对应。如果业务利益相关方要求证明投资的合理性，那么还需要花时间与他们进行交流，说明认知安全解决方案的优点。要强调一点，那就是必须使用高管能够理解的业务语言，证明这些解决方案可以改进企业的整体安全态势。通过采取这些前期步骤，您的企业就可以捷足先登，率先进入网络安全的认知时代。

目前环境

如果只看当前网络安全态势的表象，从我们所调研的安全高管那里可以获得这样一种印象：即目前的状况都在掌握之中。事实上，这些专业人士非常相信自己不断壮大的技术和组织能力。我们问到网络安全的准备情况时，大多数 (77%) 的受访者认为自己的企业与同行处于同一水平。这些受访者对于接下来 2-3 年自己企业的网络安全状况也非常乐观，86% 表示他们将会比同行做得***更好***。

这些回答可能并不令人惊讶，但是检验他们能否做到才更重要：安全领导认为他们并不比任何人做得差，而且很有信心地认为目前正在进步，而且还将继续进步。将近四分之三的受访者表示他们在解决企业基本安全问题方面非常有成效，72% 表示他们在“IT 保障”方面非常有成效，71% 表示他们在提高整个企业的风险意识方面非常有成效。但我们需要深入探讨一下挑战、影响、能力、资金和安全投资回报方面的实际情况。

速度要求

对于安全领导而言，目前所面临的最主要挑战是缩短响应和解决事故的平均时间。45% 的受访者认为缩短这些时间是当今最主要的网络安全挑战。企业并不了解这种挑战在未来 2-3 年会朝什么方向发展。展望未来，53% 的受访者认为提高响应速度仍将是最主要的网络安全挑战（见图 1）。

“这简直就像是海盗盛行时代的商船船员 – 没有海军的保护，没有警力的支持，一切都得靠自己。最重要的是，许多人还不知道如何驾船行驶，而且他们不能回击攻击者，因为这是非法的。我们几乎是把双臂绑在背后，在充满敌意的世界中苦苦挣扎。不过，您确实可以使用一些非常有趣且精巧的工具，了解自己面临的所有威胁。”

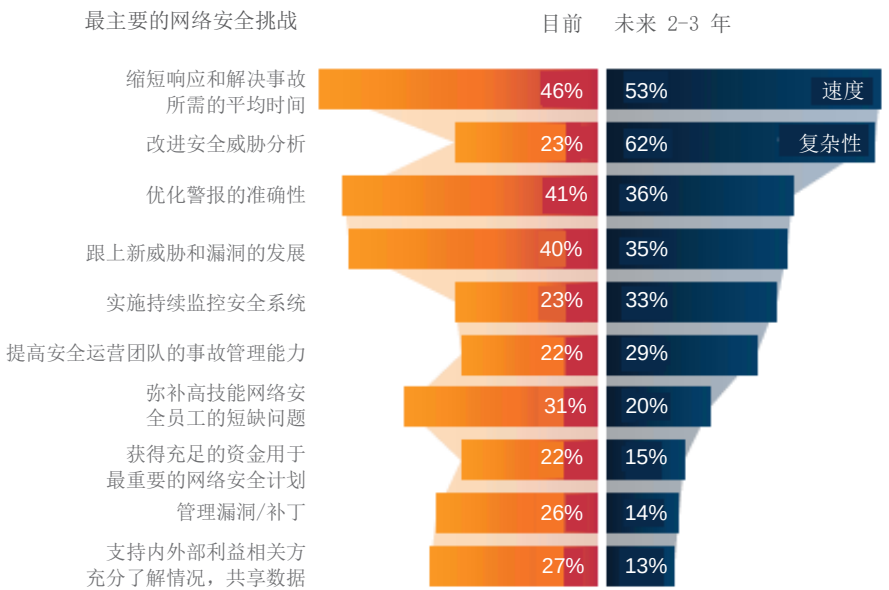
David Shipley，新布伦纽克大学信息技术服务系战略计划主任

应对时间越长，风险越大

Ponemon Institute 在 2016 年的一项调研中指出，发现一项安全违规平均需要 201 天，控制一项安全违规平均需要 70 天。该研究所还发现，如何有效使用事故响应团队，是降低数据违规成本的最大决定性因素，没有之一。[1]

图 1

安全领导指出了目前最主要的网络安全风险以及他们认为不久的将来会出现的挑战。



尽管有 80% 的企业告诉我们，他们的事故响应速度已经比两年前快了很多（平均快了 16%），但上述问题依然存在。86% 的企业希望在未来 2-3 年内进一步加快响应速度（平均目标是加快 24%）。

响应速度对于企业而言极其重要。企业响应事故的时间越长，事故造成的损失就可能越大，处理危机所花的资金就可能越多。时间无疑会增加风险所造成损失。

对于安全领导而言，另一个越来越重大的挑战就是如何改进安全风险分析。我们的调研中 23% 的受访领导认为这是目前的主要挑战之一，但是 52% 的受访领导认为改进安全风险分析将成为未来 2-3 年最主要的网络安全挑战。安全分析员必须帮助收集资讯，确定哪些威胁的严重性最高，并快速发现活动中的模式和偏差。安全领导必须想尽一切办法提高威胁响应速度，管理风险复杂性。

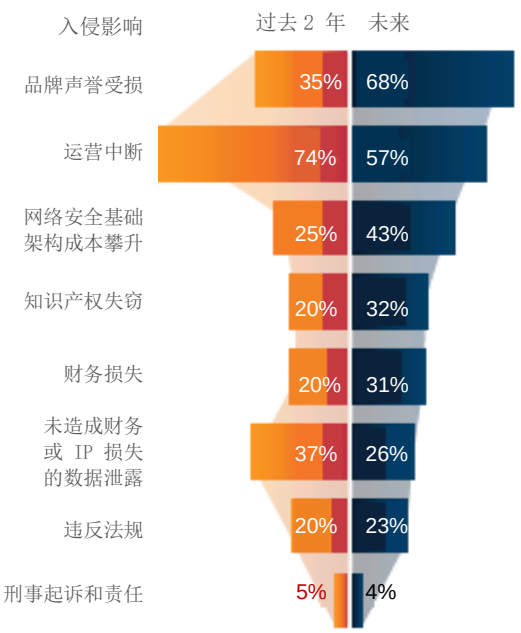
更广泛的忧虑

在我们的调研中，接近四分之三的受访者表示，在过去两年中，安全入侵导致了严重的运营中断事件。但受访者对未来几年安全入侵造成损失的看法发生了显著的变化。

企业越来越担心在将来，安全入侵会导致企业品牌声誉受损 – 担忧程度远远超过运营中断。受访者展望未来时，担心声誉受损的人数几乎翻了一倍，只有 35% 的人将声誉受损确定为过去两年安全入侵的结果，而 68% 的人担心未来会出现这个问题（见图 2）。这种转变表明许多安全领导害怕安全入侵不断扩大的影响。安全入侵的后果已经不仅仅关乎运营，还在于声誉；声誉受损会造成收入下降、信任减退和客户流失。

图 2

企业报告了过去两年由于入侵事件导致的各种后果，但是期望未来结果能有所改变。



网络安全基础架构不断攀升的成本也成为未来更实质的问题，与目前相比，对这个问题的关注人数已经显著增加。由于成功入侵的风险一直存在，因此默认情况下企业需要花费更多资金来加以应对。安全领导通常假设，如果他们遭遇入侵事件，一定要亡羊补牢的话，他们会选择升级人员技能、针对特定问题的解决方案以及基础架构，以便保持安全。

安全缺陷

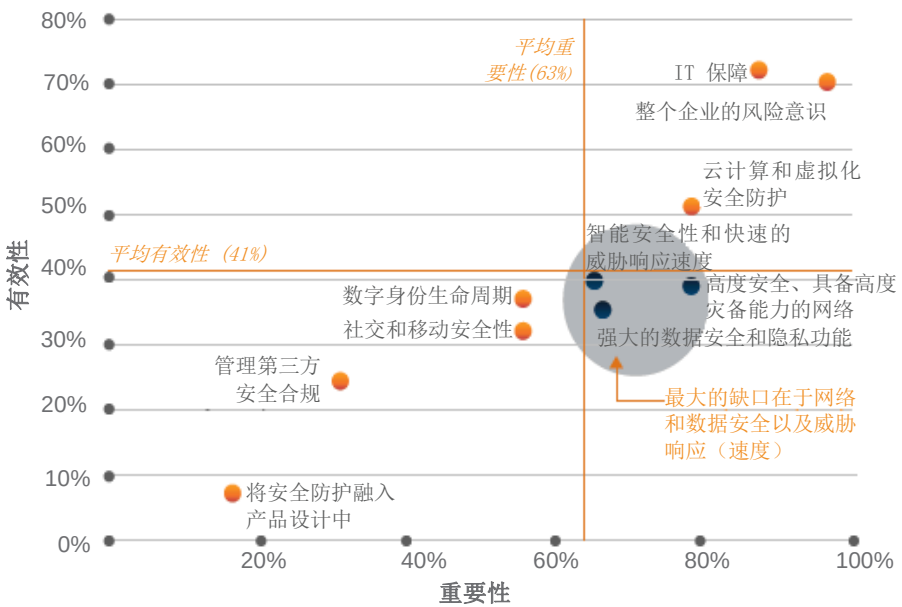
我们询问受访者：在各种安全能力中，他们认为哪些对于他们的安全状况最重要，以及他们认为自己擅长哪些能力。安全领导普遍认为自己在所有方面都一碗水端平，因为他们不想漏掉任何事情。但是，在资源有限的情况下，不可能做到面面俱到，特别是在新技术、新方法和新挑战层出不穷的情况下。

大多数受访者从技术和组织立场出发，表示他们很满意自己处理“IT 卫生”和管理企业风险意识的方式。受访者认为非常重要但自己没有能力应对的领域正是我们想要研究的领域（见图 3）。网络和数据保护以及威胁响应都属于这个范畴。

受访者表示，在威胁响应速度、安全信息事件管理（SIEM）、网络活动检测、筛选和数据分类以及预防损失方面，他们缺乏所需的有效性。当然，面对数量越来越多和越来越复杂的安全风险，企业必须抢先一步，集中精力提高响应速度、降低管理复杂性，并借助更好的威胁分析技术，从而显著提高自身的防御能力。

图 3

各种安全能力的重要性与有效性对比



“我们发现，通过安全监控和分析，企业显著节省了大量有形成本。我们通过大幅减少垃圾邮件等措施，降低了带宽成本，淘汰了使用率比较低的资源，并提高了员工生产力。”

加拿大某理财企业的金融保护主管

管理资产负债表

安全领导需要关注的方面非常多。他们预计要实现有效的网络安全性，成本会大幅增加，而且在短期内没有下降的可能。78% 的受访者表示过去两年网络安全的成本在不断增加，84% 的受访者预计未来 2-3 年成本还会继续上升。事实上，超过 70% 的受访者在网络安全方面的花费超过总体 IT 预算的 10%（大部分受访者的支出在 10%-15% 之间）。这些支出大部分都用在预防和检测方面。极端情况下，我们看到金融机构每年在网络安全方面的支出最多达 5 亿美元。[2] 因为更多的资金投入并不一定保证得到更有效的保护，这种增加投资的做法长期而言是不可持续的 - 安全领导在证明投资有效性方面承受着与日俱增的压力。

92% 的受访者表示，当他们为网络安全计划申请资金时，需要提供投资回报分析或其他财务分析，以便证明投资合理性，获得高层批准。在论证过程中，用于证明投资合理性的两个最主要因素包括在企业内清楚地说明当前的风险状况（61% 的受访者指出这一点），以及从财务高管、风险管理高管、运营高管和其他主要高管那里获得支持（51% 的受访者指出这一点）。安全领导必须使用业务语言说明自己的需求，确保获得其他主要高管的支持。[3] 从现在开始，他们必须寻求新的方法来证明网络安全投资成本的合理性并展示价值。认为安全措施仅仅是买了一份保险，或者认为这是开展业务所产生的成本的观点必须予以消除。

弥补不足

好消息是，我们采访的安全领导似乎意识到了自己的欠缺之处，并打算在不久的将来加以弥补。企业正在寻求实施各种计划，提高自己的网络安全风险应对水平（见图 4）。现在的工作主要集中在通过教育和培训，改进员工的行为表现 – 67% 的企业正在这方面采取措施。40% 的受访者还实施身份监控软件。这些通常被认为是比较基本的选项。

图 4

安全领导为了提高网络安全风险应对水平而采取的措施

当前排名		2-3 年后的排名	措施
1	▼-30%	5	通过教育和培训改进员工的行为表现
2	▼-25%	7	实施身份监控（用户活动）软件
3	▲+8%	4	使用新的分析工具报告运营/战略安全措施
4	▲+28%	1	**提高对网络、应用和数据层面安全的监控水平**
5	▲+17%	3	**改进事故响应方法、流程，提高响应速度**
6	▼-9%	8	聘请和培训更多的安全分析师
7	▼-16%	10	应用安全测试（包括移动电话、API）
8	▲+36%	2	**建立或更新 SOC 能力**
9	▲+14%	6	实施认知技术支持的安全解决方案
10	▲+1%	9	将取证能力融入到安全运营中

“高管越来越厌倦于将大量的资金投在安全方面，之前的所有投入并没有让他们感觉到更安全。安全领导需要进一步证明投资的合理性 – 不仅仅要做评估，还要确定缺口，然后寻求资金来弥补这些缺口。”

Chad Holmes，安永会计师事务所主管兼网络战略、技术和发展负责人 (CTO)

我们预计未来 2-3 年这些改进举措会发生很大的变化。事实上，受访者指出，排名前三的举措将与目前完全不同。57% 的受访者认为排名第一的将会是提高网络、应用和数据层面的安全性。建立或更新 SOC 能力排名第二。榜单上新的第三名是提高事故响应速度。所有这些方面都与之前所确定的有效性缺陷相一致。

可以看到安全领导正在弥补自己的不足，这非常好，但是优先措施的大幅变化可能会产生新的缺口或扩大现有的问题。无论如何，安全领导应确保解决与业务最相关的问题。真正的问题在于，这些预期的未来努力是否足够。

暴露缺口

所有这些挑战、薄弱环节、努力和压力都突出了三个关键缺口 – 情报、速度和准确性。安全领导必须弥补这些缺口，同时有效控制成本和投资回报压力。

情报缺口

- 65% 的受访者表示，由于资源不足而承受最严峻挑战的方面是威胁研究。
- 40% 的受访者表示，跟上新威胁和漏洞的步伐是重大的网络安全挑战。

速度缺口

- 当今和未来最严峻的网络安全挑战是缩短平均事故响应时间和问题解决时间，尽管事实上，80% 的受访者表示他们的事故响应速度已经比两年前快了很多。
- 受访者期望在未来几年加强对这个方面的关注。只有 27% 的受访者表示他们目前实施了旨在提高事故响应速度的计划，但是未来 2-3 年这个比例将会增加到 43%。

准确性缺口

- 受访者表示，目前排在第二位的挑战是优化警报的准确性（现在的误报太多）。
- 61% 的受访者表示由于资源不足导致的另一个备受压力的方面是威胁识别、威胁评估以及了解哪些潜在事故会进一步升级。

受访者提到最多的期望从认知安全解决方案中获得的收益

1. **情报**

提高威胁检测和事故响应决策能力

2. **速度**

显著提高事故响应速度

3. **准确性**

增强在辨别是安全事件还是真正事故方面的信心

增加三倍

未来 2-3 年计划采用认知安全解决方案的人数增加三倍

采用认知安全解决方案

为了弥补缺口，需要不同的技术和方法。长期来看，企业不能仅仅针对目标来投资或聘用人员。近几年来安全技术在不断发展，已经从简单的网络边界控制（例如，专注于静态防御）转变为更高级的安全情报功能（例如，专注于实时信息和模式偏差）。

现在，我们开始进入安全认知时代 – 这是一个由各种解决方案定义的时代，通过分析结构化和非结构化的安全数据了解背景信息、行为和含义。认知安全能力的目标是在安全分析人员及其技术之间建立新的合作关系。这些解决方案能够解释和组织信息，说明信息的含义，还提供基本原理总结。它们还能随着数据的积累不断学习，并从互动中获得洞察。

认知安全解决方案的优点

想象一下，通过一系列由认知技术支持的解决方案，您可以：

- 为初级 SOC 分析人员提供原本需要多年经验才能积累的最佳实践和洞察，增强他们的能力。
- 应用博客和其他来源的外部情报，提高响应速度，以便可以在征兆显现之前采取行动。
- 利用高级分析方法快速发现风险，加快检测存在风险的用户行为、数据泄露和恶意软件感染。
- 通过自动收集和推理本地数据和外部数据，获得有关安全事故的更全面的背景信息。

如何使用认知安全技术？

认知系统用于分析安全趋势，将海量的结构化和非结构化数据提炼为切实可行的知识。安全领导和分析人员不可能消化吸收所有人类生成的安全知识，包括研究文档、行业刊物、分析报告和博客等。而认知系统有能力将上述信息与更为传统的安全数据组合在一起。认知安全解决方案可以将数据驱动的自动化安全技术、方法和流程结合起来，确保实现最高水平的相关性和准确性。

认知安全解决方案有助于增强 SOC 分析人员的能力 – 帮助他们提高响应速度，更好地发现威胁，提高应用安全性，降低整个企业范围的风险。认知解决方案的目标是让分析人员从日常重复性的安全任务中解放出来，从而能够集中精力处理最具智力挑战性的工作。

前景和挑战

在我们的调研中，许多受访者认为认知安全解决方案产生的收益能够弥补他们面临的缺口。尽管认知安全是一个新兴技术领域，但是 57% 的受访者认为认知安全解决方案可以减缓网络犯罪的速度 – 他们看到了这种解决方案的前景和潜在的收益。

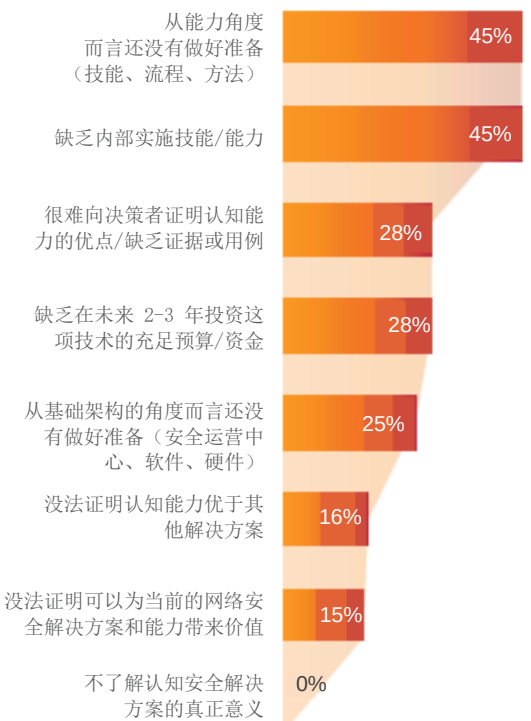
当我们要求安全领导选择认知安全解决方案的收益时，40% 的人提到它们有助于提高检测速度和事件响应决策能力，37% 的人指出它们显著提高事故响应速度，36% 的人表示它们有助于增强在辨别是安全事件还是真正事故方面的信心。受访者希望认知安全解决方案能够弥补他们主要的缺口。他们需要这些解决方案在情报、速度和准确性方面提供帮助。

现在，受访者中仅有 7% 正在实施认知安全解决方案，以改善网络安全风险准备情况。由于认知能力是新生事物，因此目前采用率低可以理解。然而，不久的将来实施认知解决方案的企业有望翻 3 倍，达到 21%。未来几年，我们会看到认知能力的采用率迅速蹿升，因为安全领导需要这种能力以增强自身的数字免疫系统。

受访者也认识到了采用认知安全解决方案的潜在挑战。安全领导并非不了解这种技术理念，他们也并非不相信认知能力可以比其他解决方案带来更多的价值或好处；挑战主要在于技能、流程和方法等方面。45% 的受访者表示，采用认知能力所面临的最主要挑战在于从能力角度而言还没有做好准备，而且缺乏内部实施技能（见图 5）。要减轻这些担心，有大量的培训和准备工作要做。

图 5

安全领导确定了实施认知安全解决方案的最主要挑战。



“我们已经准备好运用认知和智能解决方案采取下一步行动，以便高效地采集和组织海量的安全信息和知识，并提供丰富的上下文内容，避免像现在这样需要耗费大量的时间和资源。”

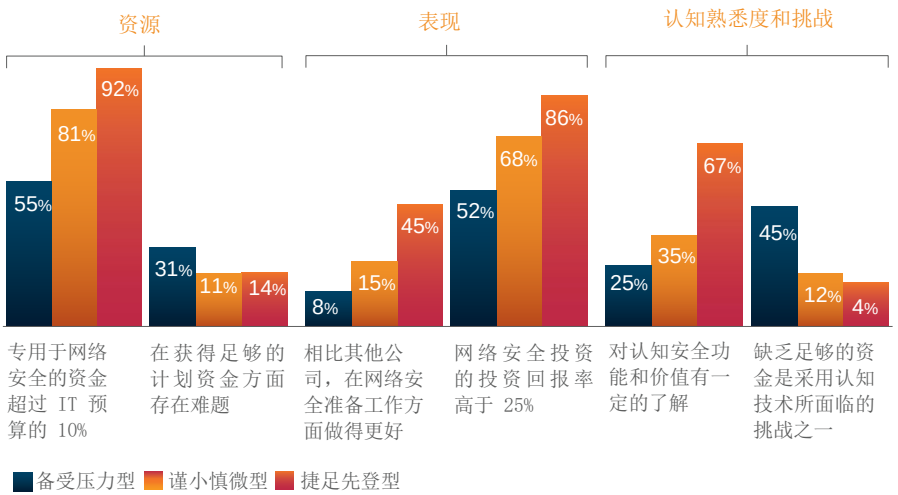
加拿大某理财企业的金融保护主管

率先进入认知时代

为了了解谁已经准备好率先进入安全认知时代，我们根据受访者自己描述的安全有效性水平、认知了解程度和准备情况，对他们进行了特征分析。通过对受访者的回答进行分析，揭示出三个截然不同的群体（见图 6）。

图 6

备受压力型、谨小慎微型和捷足先登型企业表现出不同的准备情况特征



备受压力型占我们样本的 52%，特征是企业遇到资金和人员方面的挑战，对认知安全的功能和价值的熟悉度较低。这些企业通常分配给网络安全的 IT 预算百分比较低，在获取足够的资金和解决人员短缺问题方面存在挑战的可能性更大。他们还表示缺乏足够的资金是采用认知技术所面临的挑战之一。

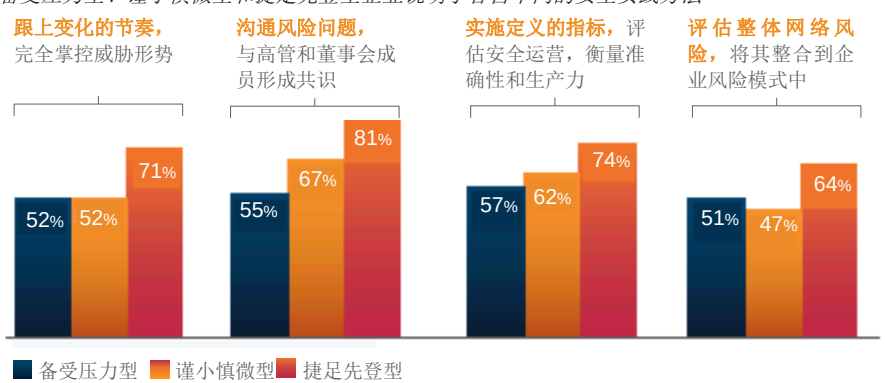
（有关我们如何划分和定义这些群体的详细信息，请参见第 20 页的“群体统计和方法”部分。）

谨小慎微型占样本的 27%，他们不存在备受压力型企业所遇到的那些资源挑战，但是他们还没有完全准备好立即实施新一代认知技术支持的安全解决方案。

捷足先登型占样本的 22%，是最了解和最热衷于认知安全解决方案的企业群体。捷足先登型企业对认知安全比其他群体有更高的熟悉度和信心，可以获得更多预算，实现更出色的投资回报。他们认为自己在安全实践方面运用了更成熟的方法，他们当中更高比例的人表示其安全运营团队能够跟上威胁方面的变化。他们有效地与高管和董事会成员沟通风险问题，并且将网络风险问题整合到企业风险模式中（见图 7）。

图 7

备受压力型、谨小慎微型和捷足先登型企业说明了各自不同的安全实践方法



“存在大量的‘杂音’；人类的大脑无法处理每天发生的一切事情。我们需要某些解决方案提供帮助，比如人工智能或认知技术。”

Chad Holmes，安永会计师事务所主管兼网络战略、技术和发展负责人（CTO）

“ 24/7 式的安全运营对于大多数企业而言，在人员方面的成本过于高昂，而这正是认知安全解决方案的用武之地 – 它们不需要睡觉，也不会感到疲劳。”

Michael Pinch，罗切斯特大学首席信息安全官

安全领导希望从认知安全解决方案中获得什么？在与这些捷足先登型企业领导的对话过程中，我们发现他们希望认知安全解决方案能够：

- 永续运营，提供持续的支持
- 帮助减少误报，发现行为异常现象
- 更好地理解威胁形势，提供事故的背景信息
- 根据独特的行业、地区和其他法规要求支持监管、风险管理与合规
- 改变安全工作的性质，帮助分析人员更智慧地开展工作，提供更高的价值

可以预料，感觉自己足够成熟而且资源限制比较少的安全领导会率先利用像认知安全这样的新兴技术。然而，必须认识到，具备其他知识和经验的每个人都可以应用认知技术来弥补他们的不足并消除分析人员的限制因素，从而改进安全运营。

建议

我们研究了目前的安全形势，以便了解受访者所面临的压力、挑战和优先任务。我们根据自己的观察汇总了一些建议，旨在帮助您和您的企业为进入认知时代做好准备。

认清自己的弱点

安全领导希望提高反应速度，降低复杂性，他们越来越担心安全事故导致企业声誉受损。了解您的企业的主要弱点和漏洞。它们有什么联系？优先任务是什么？

- 您是否缺乏所需的情报和威胁研究？
- 事故响应和解决速度对于支持运营而言是否足够快？
- 您在区分安全事件和真正事故方面，或在与更合适的背景环境整合方面是否存在困难？

熟悉认知安全能力

采取整体和正式的方法了解有关认知安全解决方案的信息。您的企业可能在能力、成本和实施方面存在很多误解。

- 因此需要了解认知安全解决方案的可能用例，并将这些用例与企业的薄弱环节对应起来。是否希望获得有关安全事故的更多背景信息，从而提高决策水平，或者采用新方法主动评估风险？
- 计划如何与技术和业务利益相关方沟通认知安全解决方案的益处，为团队和高管制定培训方案。

“认知安全具有如此之多的潜力 – 有助于弥补劳动力缺口，改善风险态势，提高响应效率。它可以帮助您理解事件脉络。人们使用故事来叙述前因后果人员影响。另外，认知技术可以降低从事网络安全工作的技能门槛。它支持您使用来自非 IT 背景的新视角来解决问题。”

David Shipley，新布伦纽克大学信息技术服务系战略计划主任

- 发现和弥补可能会阻碍您的企业采用该技术的技能缺口。

制定投资计划

如果一项技术在市场上崭露头角，而且未经过验证，那么构建投资案例就非常困难 – 没有太多的例子来证明其合理性，而且很难建立信任。因为我们的大部分受访者表示，他们的资金申请需要提供投资回报分析或其他财务分析，所以安全领导非常有必要为企业采用认知解决方案准备一套独特的证明方法。

- 需要认识到认知安全解决方案的独特性质。不能仅仅关注于传统的安全投资理由，例如修复成本。而是要关注一个事实，即认知安全有能力提高安全运营的整体有效性。
- 自己制定培训计划，并使用该计划说服企业中的其他高管，让他们帮助构建投资案例。
- 创造性地思考，采用新颖的方式为认知安全解决方案寻求投资，证明它们能够为企业带来的帮助远不止投资回报。

寻求增强自身能力，无论成熟度如何

我们确定为捷足先登型的企业往往拥有更多的可用资源，对其能力有更高的信心，而且对立即实施认知安全解决方案做好了准备，但这并不意味着认知安全解决方案只适用于这个群体。认知安全解决方案是一个新兴的技术领域，它独特的性质可以使所有类型的企业受益。

- *如果贵公司属于备受压力型：*确定认知安全解决方案可以帮助改善的特定业务措施并弥补的技能短缺，然后构建投资案例。
- *如果贵公司属于谨小慎微型：*集中精力进行沟通交流，减轻有关技能缺口的焦虑。
- *如果贵公司属于捷足先登型：*用您的热情感染他人，为认知试点实施选择非常具体的用例，并确保这个用例与贵公司更广泛的安全运营息息相关。

了解更多信息

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，致力于为全球商业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。

合作者

Lisa van Deth，IBM 安全事业部促销活动与思想力领导战略项目营销经理；Christophe Veltsos，位于曼卡多市的明尼苏达州立大学计算机信息科学系副教授。

致谢

Caleb Barlow，IBM 安全事业部全球产品组合营销副总裁；Maria Battaglia，IBM 安全事业部业务连续性 CMO；Wangui McKelvey，IBM 安全事业部产品组合营销/安全服务与 Web 欺诈防御总监；Kevin Skapinetz，IBM 安全事业部战略总监；此外，牛津经济研究院帮助我们管理调研数据的收集工作。

备注和参考资料

1 “2016 Cost of Data Breach Study:Global Analysis.”Ponemon Institute.June 2016.http://www-03.ibm.com/security/data-breach/

2 Friedman, Gabe.“JPMorgan Chase Atty:Bank Will Spend $500M on Cyber Security.”January 29, 2016.https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/.Accessed on September, 21, 2016.

3 Kelley, Diana and Carl Nordman.“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，2016 年，http://www-31.ibm.com/ibm/cn/pdf/Securing_the_C-suite.pdf

群体统计与方法

为了更好地了解企业面临的安全挑战，他们应对这些挑战的方式以及他们对认知安全解决方案及其潜力的看法，IBM 商业价值研究院（IBV）和牛津经济研究院于 2016 年 5 月和 6 月期间采访了来自 35 个国家或地区、代表 18 个行业、均衡分布的 700 多位 CISO 和其他安全专业人员。

为了确定不同的群体（捷足先登型、谨小慎微型以及备受压力型），我们应用了 K-均值聚类法，揭示了三种不同的行为模式。这些行为模式是根据和安全有效性、认知了解程度以及认知准备情况相关的问题而确定的。

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》、《时代杂志》、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

Vijay Dheap 是 IBM 安全事业部的项目总监，专门负责将新兴技术转变为商用产品。他目前负责安全情报方面的产品组合，涵盖高级分析、认知和 SaaS。之前，他负责网络取证和移动安全业务。Vijay 是核心技术专家，荣获了 IBM 发明大师称号。他的专利产品遍及移动电话、企业协作和安全创新方面。他从杜克大学商学院获得国际 MBA 学位，并从加拿大滑铁卢大学获得计算机工程硕士学位。Vijay 的联系方式为：vdheap@us.ibm.com

David Jarvis 是 IBM 商业价值研究院的安全和 CIO 主管。他负责制定和执行计划，探究这些领域的新兴业务和技术主题。他是开发和管理市场洞察、思想领导力和战略远见项目方面的专家，并在 IBM 担任这些领域的多个职位。他撰写了许多网络安全思想领导力报告，包括从 2012 年到 2014 年的 IBM CISO 评估报告。除了研究工作，David 还教授业务远见和创造性解决问题课程。David 的联系方式为 anthony2@us.ibm.com

Carl Nordman 是 IBM 商业价值研究院最高管理层调研项目的全球总监和 CFO 研究主管。他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

© Copyright IBM Corporation 2016

Route 100
Somers, NY 10589
美国出品
2016 年 11 月

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corporation 在全球许多司法管辖区域的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 地址 www.ibm.com/legal/ copytrade.shtml 的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。

本文档是首次发布日期之版本，IBM 可能会随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议的条款和条件获得保证。

本报告的目的仅为提供通用指南。它并不试图代替详尽的研究或专业判断依据。由于使用本出版物对任何组织或个人所造成的损失，IBM 概不负责。

本报告中使用的数据可能源自第三方。IBM 并不独立核实、验证或审计此类数据。此类数据使用的结果均为“按现状”提供，IBM 不作出任何明示或默示的声明或保证。

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

GBE03779CNZH-00