knowbe4

人因风险管理的战略框架

何为人因风险管理？企业为何需要它？

这不只与技术有关

尽管企业在网络安全技术上投入了大量资金，但“人”依然是安全漏洞的主要因素。多份行业报告显示，68% 至 90% 的安全事件都与人为行为或错误有关。

然而，这并不是意味着可以指责员工。企业必须承认一个现实：人难免会犯错。在当今的工作环境中，员工普遍面临工作繁忙、注意力分散以及远程办公等情况，即便他们意识到网络攻击的危险性，也往往没有时间去充分理解和警惕这些风险。尤其是在人工智能（AI）助力下，社会工程攻击的复杂性和隐蔽性大幅提升，使其更具欺骗性，也更难被察觉。

当传统检测技术都无法识别这些攻击时，我们又怎能苛求员工做到呢?

现代职场压力与高级社会工程手法的结合，已经清楚地表明：传统基于合规性的安全意识培训已不足以应对持续且普遍存在的威胁。因此，许多组织的安全体系中都存在一个关键的战略缺口。而弥补这一缺口的最佳方式，就是人因风险管理（HRM, Human Risk Management），一种超越单纯“意识提升”的战略，通过持续的数据驱动过程，系统性地识别、衡量并缓解人因风险。

本白皮书阐述了现代 HRM 的核心原则，并介绍了一个基于四大支柱的实施模型：防御（Defend）、教育（Educate）、赋能（Empower）、保护（Protect），简称 DEEP。该模型以成熟的组织行为学原理为理论基础，其核心目的在于培育坚实的安全文化。最后，本文建议采用一个集成的、AI 驱动的 HRM 平台，作为最有效的员工参与手段。此类平台能够提供风险评估、个性化教育、实时辅导与自动化响应等必要工具，使企业能够将员工从潜在的安全弱点，转化为坚韧的防御层。

人因挑战的持续存在

传统工具往往效果有限

网络犯罪分子不仅仅是在攻击系统，更是在利用人性。他们会利用我们与生俱来的本能，比如乐于助人、尊重权威、害怕错过机会，甚至只是一瞬间的分心进行攻击。因此，“人”这个因素在安全漏洞中始终是一个核心主题。

几十年来，解决人为漏洞的方法通常是“增加培训”或者“加强技术”。然而，事实证明，单纯的“打勾式”培训以及传统检测技术，并不能真正解决问题。

近年来，网络犯罪分子越来越擅长设计能够轻松绕过传统检测技术（如安全邮件网关，SEG）的攻击方式。与之相反，安全意识培训却往往流于通用化，缺乏吸引力，几乎从未根据某个特定岗位或特定个人的实际风险进行定制。

KnowBe4 一直反对这种千篇一律、通用化的安全培训方式，因为这种方法几乎从未奏效。

新的行动手册：战略性 HRM 的崛起

企业需要摆脱那种只关注“培训”或只关注“技术”的孤立思维，转而采用一种以人为核心的整体性方法。

这就是人因风险管理（HRM, Human Risk Management）的由来。

它并不仅仅是给“安全意识与培训（SAT）”换了个更贴切的名字，而是一种战略性、持续性的过程。它结合了技术、人类行为动机的理解，以及不断改进的策略。

向 HRM 转变，意味着我们要从全局视角出发——通过把关注点放在人上，打造一个具备韧性的组织，保护来之不易的声誉。这一理念可以借助平台化的方式进一步强化：借助平台，企业能够更好地理解并优化员工与技术的互动方式，进而建立网络韧性。该平台整合了AI驱动的防御机制、安全意识教育、员工赋能与保护措施，旨在营造一种让安全行为自然形成的环境。

整个过程强调的是与人的协同，而非对立。

战胜恶意软件：明智之举背后的行为科学

一个有效的 HRM 战略，必须对其所要解决问题有清晰的理解。这包括对过去方法的局限性、导致人为脆弱性的行为因素，以及强大安全文化的决定性要素等方面的全面分析。

传统安全意识培训的不足

从历史经验来看，应对与人相关的风险，主要是依靠定期的、通常由合规驱动的 SAT（安全意识培训）。然而，这种方法已被证明存在很多不足：

缺乏参与感

传统的SAT（安全意识培训）通常由演示文稿和测验组成，既不能吸引员工的注意力，也难以激发真正的学习兴趣。员工往往只是匆匆完成，把它当作一项"打勾式任务"。

内容过于通用

"一刀切"的培训方法并没有考虑到不同员工的岗位、职责和风险点。例如，财务主管所面临的风险与市场专员截然不同，但他们往往接受完全相同的培训。

认知与行动的差距

了解安全政策，并不意味着员工能在压力下真正执行。单纯的"意识"往往不足以克服根深蒂固的习惯或即时的认知偏差，从而导致员工在面对现实威胁时，"知道"与"做到"之间始终存在差距。

利用认知偏差

网络犯罪分子非常善于利用人类思维中可预测的捷径即认知偏差。他们常常利用的关键偏差包括：

权威偏差（Authority Bias）

倾向于服从权威人物的请求，导致员工容易受到冒充高管或政府机构邮件的欺骗。

乐观偏差（Optimism Bias ）

相信自己遭遇负面事件的可能性低于他人，从而低估了自己遭遇诈骗的风险。

熟悉性偏差与虚假真实效应（Familiarity Bias & Illusory Truth Effect ）

更倾向于相信熟悉的事物，以及反复接触过的信息。攻击者通过伪造类似合法通信的钓鱼邮件来利用这种偏差，使其看起来更具可信度。

可得性启发（Availability Heuristic ）

倾向于高估那些容易被回忆起来的事件发生的概率。可能导致员工对近期广为人知的威胁高度警觉，却忽视对较少见攻击方式的防御。

作为核心元素的安全文化

薄弱的安全文化本身就是一个重大的风险因素。文化可以理解为影响安全行为的共同观念、习俗和社会行为。当安全文化较为薄弱时，员工会缺乏自觉保持警惕的动力，一旦觉得无人监督，就更容易掉以轻心。

因此，积极的安全文化是抵抗人因风险的重要保障。

- 在 KnowBe4 的理念中，成熟的安全文化包括多个关键维度：

- 规范的安全保障
- 高质量的安全沟通
- 对政策的认知度
- 安全知识水平
- 对安全的态度
- 共同的责任感

从这些角度培养安全文化，对任何 HRM（人因风险管理）项目而言都是核心要务。

人因风险管理方法

要解决复杂多样的人因风险问题，需要一种超越基础手段的新方法。
简而言之，人因风险管理（HRM, Human Risk Management）方法是一种战略性、以人为中心的网络安全框架，它既结合了技术防御手段，也关注人们行为背后的“原因”。HRM 认识到人的行为受文化、心理和我们所处的社会体系的影响，因此它并非仅仅是制定规则，而是试图理解驱动员工决策的动机与日常压力。
需要注意的是，HRM 方法不同于 HRM 平台。HRM 平台是一种帮助组织有效落实 HRM 方法的工具。关于平台的部分将在本文后续介绍。

现代人因风险管理方法的核心原则

一个有效的 HRM 方法应建立在以下核心原则之上：

- **识别薄弱环节**

  尚未察觉的问题无法被修复。风险评估是第一步——弄清楚谁更可能点击什么，以及背后的原因。

- **个性化定制**

  方法必须针对不同团队和岗位的威胁和学习需求进行定制。

- **借助人工智能与自动化技术**

  借助智能技术是扩大方法应用规模、实现干预个性化、并提供数据驱动洞察的关键。

- **持续测试与改进**

  HRM 是一个迭代过程，需要通过追踪关键指标来衡量行为变化，并不断优化策略。

- **让政策更“有人情味”**

  政策与流程不应像法律合同那样晦涩。如果希望员工遵守规则，就必须让他们理解。这意味着要使用通俗的语言，减少时间限制，并确保内容贴近实际场景。

- **以人为本的设计**

  安全措施应当是赋能而不是阻碍业务运营。这需要同理心、清晰沟通，并在流程设计时兼顾用户体验。

- **领导层参与**

  高层管理者的支持至关重要，它能彰显 HRM 的战略重要性，并推动责任落实。

- **保有人文关怀**

  技术固然强大，但有时一句提醒、一点指导，或者让员工感受到自己是解决方案的一部分，往往能产生意想不到的积极效果。

支撑模型：DEEP 框架

为了更好地落实人因风险管理（HRM）方法的核心原则，一个概念性模型——DEEP（防御 Defend、教育 Educate、赋能 Empower、保护 Protect）——能够发挥重要作用。该模型由四个相互独立但紧密关联的支柱组成：

1 Defend：防御 —— 阻止攻击接触到员工

这一部分侧重于技术防护。通过技术控制（例如，AI增强型邮件安全）主动减少攻击面，从而最大限度降低真正攻击到达员工的可能性。

2 Educate：教育 —— 教会员工识别威胁

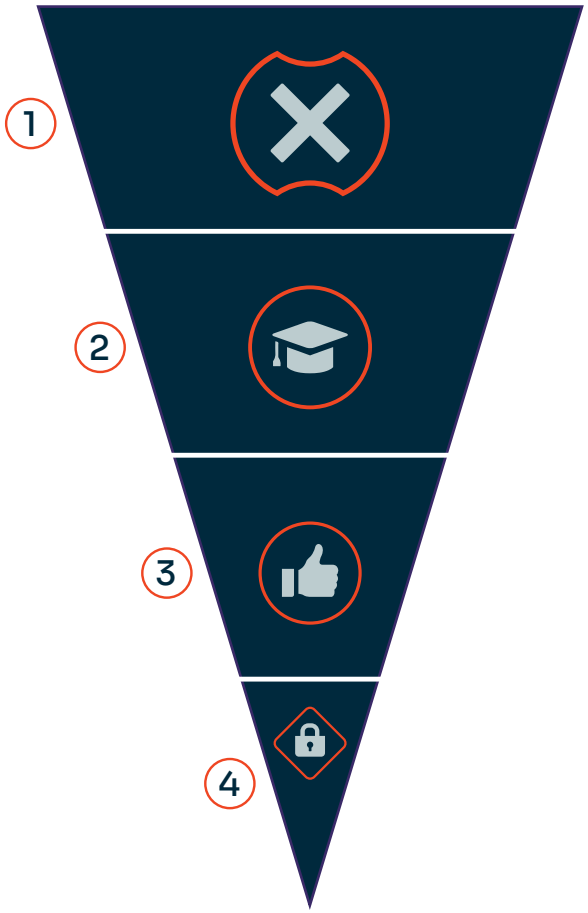
不仅仅是中和威胁，更是提升人的理解力。通过个性化、自适应和相关性强的培训，让员工掌握识别与应对威胁的知识与技能。

3 Empower：赋能 —— 打造积极的安全文化

知道该怎么做是一回事，能在关键时刻自信地去做又是另一回事。组织需要营造支持性的文化，并提供用户友好的工具（如一键式报告按钮、实时辅导、交互式反钓鱼提示横幅），让安全选择变得轻松直观。

4 Protect：保护 —— 减少错误带来的损失

再强大的安全策略也无法完全避免人因错误。因此，组织必须制定健全的响应计划，以将事件的影响降至最低，并利用这些事件的数据不断改进前面三个支柱。



这并不是一个僵化或线性的过程，而是一个持续循环。从 **保护**阶段获得的经验，会反过来改进**防御**的方式、**教育**的重点，以及**赋能**的手段。一切紧密相连，就像一台**高度安全且**运行顺畅的机器。

建议：实施一体化 HRM 平台

为了有效执行战略，我们建议采用一个现代化、集成化的人因风险管理（HRM）平台。这种方式能够提供所需的规模化支持、数据整合和自动化能力，而这些是**散点化的**解决方案及其孤立数据集所无法实现的。

在 KnowBe4，我们相信，要在当今时代真正有效地应对人因风险，远不止依靠良好的意愿和一套培训视频库，而是需要一个坚实的基础。这意味着要充分利用 AI 的力量、智能自动化，以及安全能力的无缝集成，从而构建一个能够学习、适应，并帮助员工真正实现更高安全性的智能系统。这一理念正是 HRM+ 平台的核心。

KnowBe4 HRM+ 平台

KnowBe4 HRM+ 是一个全面的平台，旨在将组织自身的战略性 HRM 方法付诸实践，并直接与 DEEP 四大支柱相对应。它的设计具有个性化、相关性和自适应性，能够增强组织抵御复杂威胁的能力，并将员工从最大的攻击面转变为最有价值的安全资产。

核心能力包括：

安全意识培训（SAT）与合规 Plus（Compliance Plus）
一个涵盖丰富、具有吸引力、本地化和个性化培训内容的完整资源库，作为 “教育” 支柱的基础。

云邮件安全
一款 AI 驱动的邮件安全产品，利用预生成建模与深度神经网络来 “防御” 高级入站钓鱼攻击和邮件中的数据泄露。

PhishER Plus
一款安全编排、自动化与响应（SOAR）产品，通过自动化事件响应来 “保护” 组织，并减轻安全团队的工作负担。

Security Coach
一款实时辅导工具，可与现有安全堆栈集成，在用户发生风险行为时即时提供反馈与指导，从而 “赋能” 用户。

人工智能防御代理 AIDA（Artificial Intelligence Defence Agents）
一套贯穿整个平台的 AI 代理，支持培训个性化、生成逼真的模拟场景，并实现现代 HRM 方法所需的动态风险评分。

个体风险评分的作用

现代 HRM 平台的一项关键能力，就是使用动态、个性化的风险评分。通过分析广泛的行为数据（包括钓鱼模拟表现、培训参与度和真实安全事件），像 KnowBe4 的 SmartRisk Agent™ 这样的 AI 引擎，能够为每位用户生成细致的风险画像。

这使得安全领导者能够：

- **有针对性地干预**
  将资源和更深入的辅导聚焦于最高风险群体。
- **识别系统性问题**
  利用整体风险数据定位普遍存在的漏洞或无效流程。
- **证明投资价值**
  向高层管理者展示整体风险可量化的下降趋势。
- **实现个性化学习路径**
  自动化推送适当层级的培训，确保项目高效且有效。

组织如何实现有效的人因风险管理（HRM）方法？

人为相关的网络风险具有持久性和不断演变的特点，这要求组织必须在传统安全意识培训和遗留技术之外，进行战略性提升。一个基于行为科学、持续改进和文化建设原则的全面 HRM 方法，并辅以系统化的 HRM 项目，已经成为当今企业的必然选择。

实施这一方法的最有效路径，是借助一个集成化、由 AI 驱动的 HRM 平台。通过统一防御、教育、赋能与保护四大能力，该平台能够为组织提供识别风险、推动有意义的行为改变，以及培养具备韧性的安全文化所需的工具。

独立的 ROI 分析表明，这一方法不仅能显著降低员工驱动型安全事件的发生概率，从而强化组织的整体安全态势，还能带来切实的运营效率提升与财务回报。采取战略性的 HRM 方法，是对组织韧性的一项关键投资，它将人为因素从潜在的薄弱环节转化为坚固可靠的防御层。

KnowBe4 的方法

在KnowBe4，整个HRM+平台均以首席信息安全官级别的战略考量为设计基石。我们秉持以人为本的理念，并通过人工智能与自动化技术实现强大赋能。四大支柱——风险识别与评估、个性化教育与赋能、技术整合与自动化、持续监控与改进——旨在为组织构建全面、数据驱动且适应性强的员工风险管理体系。

管理人为风险已不再是"软技能"或次要考量。在人工智能驱动攻击与数字交互日益频繁的时代，这已成为战略性需求。而拥有智能化的集成式HRM平台，正是实现精准管理的关键所在。

免费钓鱼安全测试
了解贵司员工中有多少比例容易受钓鱼攻击影响

免费自动化安全意识计划
为您的组织定制个性化的安全意识培训方案

免费钓鱼警报按钮
员工可一键安全上报钓鱼邮件

免费邮箱泄露检测
在攻击者发现之前，确认哪些邮箱地址已被暴露

免费域名伪造测试
检测黑客是否能伪造贵司域名的邮箱

关于 KnowBe4

作为全球最大安全意识培训与模拟钓鱼平台的提供商，KnowBe4 帮助组织应对安全中的人为因素挑战。通过由国际知名网络安全专家研发的新一代方法，提升员工对勒索软件、CEO 欺诈及其他社会工程学攻击的认知与防御能力。

艾体宝（itbigtec）公司是 KnowBe4 的官方授权合作伙伴，携手将 KnowBe4 的前沿安全意识培训和钓鱼攻击模拟平台推广至中国企业用户，推动企业安全从“技术防护”走向“全员防护”。

全球超过 70,000 家组织 信赖 KnowBe4 平台，以强化其安全文化并降低人为风险。
更多信息请访问：www.itbigtec.com

knowbe4

itbigtec 艾体宝

itbigtec.com
sales_it@itbigtec.com
400-999-3848

分部：广州 | 上海 | 苏州 | 北京 | 西安 | 成都 | 台湾 | 香港 | 日本 | 韩国

版本：V3.0 - 25/09/06

网络安全与监控方向
(T: 135 3349 1614)

网络安全交流2群

获取更多案例