构筑以数据为中心的安全环境

依靠卓越的安全基础
规避隐蔽的数据漏洞

埃森哲安全服务

缺乏基本的数据安全防护是企业遭受数据泄露的重要原因。

重新审视此类工作将为企业和高价值信息资产带来更佳的安全性。

引言

让我们先来看看这些令人震惊的数字：

- 一家领先的信用报告机构泄露了超过1.4亿条客户记录，其中包括社会安全号码、出生日期和驾照信息等利用价值极高的个人身份识别数据。
- 一家领先的互联网服务提供商遭黑客入侵，致使超过5亿名用户的帐户资料外泄，其中包括姓名、电子邮件地址、电话号码、出生日期、密码信息等。
- 一家健康保险公司8千万名患者和雇员的记录遭窃，姓名、出生日期、社会安全号码、电子邮件地址、就业信息和收入数据等信息或已流出。
- 两家领先的零售商当中，分别有超过5千万和4千万个信用卡账户信息被盗。

类似事件不胜枚举。深究其背后的安全原因，如果上述企业有效部署了以数据为中心的基本安全措施，那么损失程度将大幅降低。

如今，对任何一家企业而言，审视并实施以数据为中心的安全基础措施，由此加强数据保护亟不可待。

重大数据泄露事件的共同特征

我们从显而易见的事实开始剖析。首先，毫无疑问，上述实例中的大规模数据泄露**代价高昂**——任何一次严重事件不但会导致数千万、乃至上亿美元的经济损失，还将引发品牌和商誉的折损，更将带来持续性的财务和法律风险。因此，无论是对受害企业、还是其合作伙伴抑或客户来说，这份冲击都势必巨大而持久。

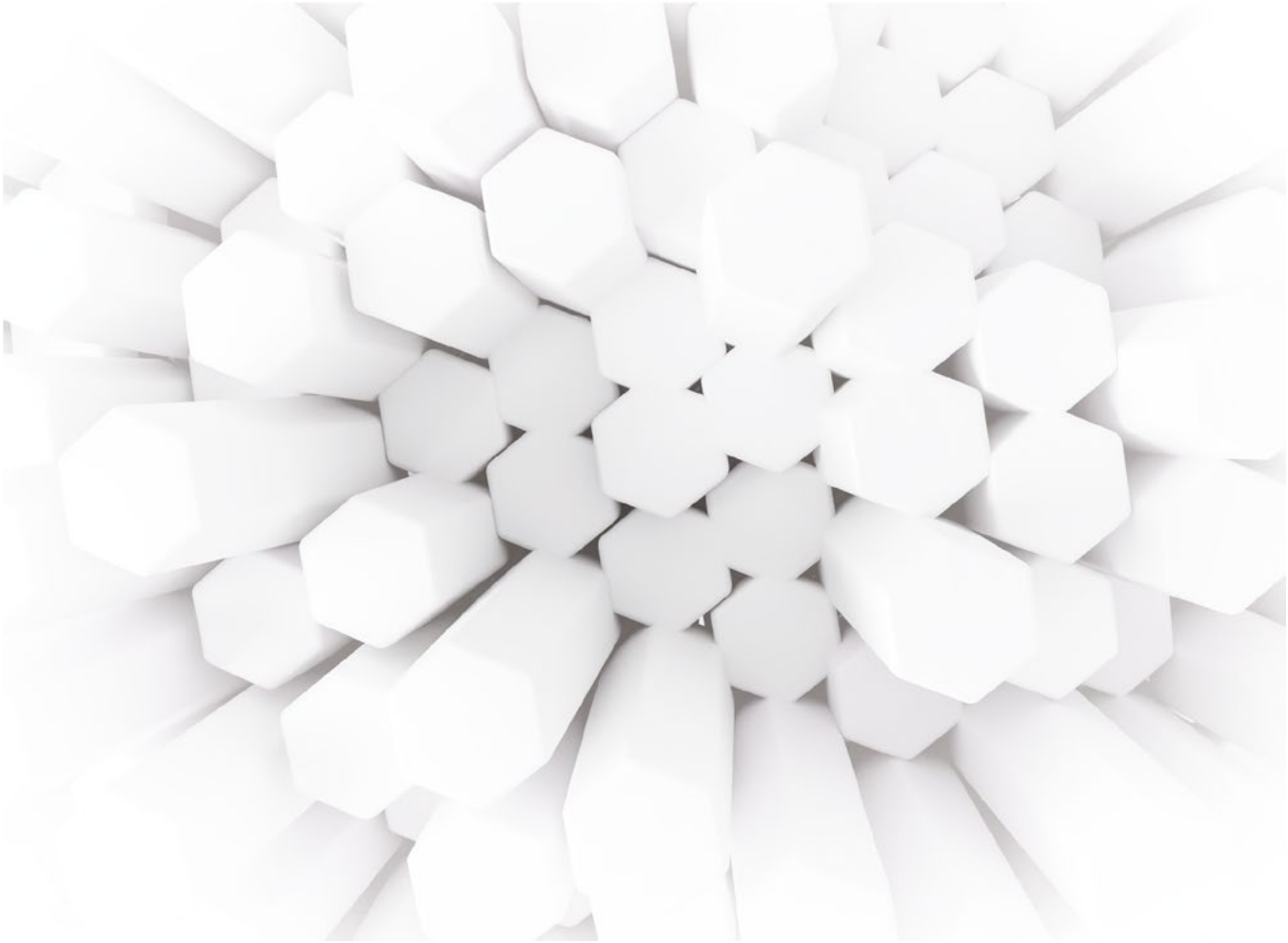
不过，即便是那些规模相对可控的日常数据泄露，也有可能产生严重的财务和声誉影响。据由埃森哲资助的Ponemon Institute所做的研究估算，去年一年，网络犯罪带给普通企业的平均损失上升了23%，已高达1,170万美元。

其次，与日常泄露状况没能得到足够重视相似，诸多数据泄露的受害企业**仍未充分认识到：数据是企业的命脉**。对于美国中情局、英国军情六处和以色列摩萨德等情报组织而言，数据丢失就意味着生命无法保障。因此毋庸置疑，保护数据是性命攸关的紧要任务。就商业领域来看，尤其是在能源、化工和医疗保健等行业中，数据丢失同样可能危及生命安全，更会致使竞争优势的丧失以及品牌和声誉受损，甚至是重大的法律和财务后果。企业的运转需要、也依赖于数据的安全处理，因此，数据保护这一要务应当得到足够程度的关注、重视和投入。在数字时代，数据即是价值。与那些疏于防范的企业相比，守护这份价值的机构必将获得更显著的优势。

数据失窃受害企业的第三项共同特征是**多种类型的安全漏洞并发存在**。我们面临的挑战并非在于，犯罪分子是否利用受害企业无法修复的已知网站漏洞，或是发起零日攻击；真实的问题是，必定会存在能够使得多达数千万、乃至数亿条客户记录被窃取的多个流程和程序缺陷，并且泄漏情况持续数天、数周或数月仍难以被察觉。

“加固”企业最具价值的资产。

综合思考上述特征，我们建议企业采取这些行动：一，井然有序地构建数据保护基本要素。二，为防范数据泄露并最大限度地减少其影响，他们必须“加固”数据资产，着手部署以数据为中心的卓越安全基础工作。



打造卓越安全基础

明确高值资产

这些数据可谓是企业“皇冠上的宝石”——不仅对业务至关重要，且处置失当会招致最严厉的监管处罚；此外，它们也是商业秘密和市场优势的关键组成部分。

加固高值资产

“加固”高值资产意味着，使不法分子在达到目的过程中遇到尽可能多的困难并为此付出高昂成本，同时尽力缩减对方一旦得手可能造成的损害。这里是进一步的行动建议：

- **模拟攻击者心态。**他们最想得到什么？由此设计和执行威胁与漏洞检查程序，以及整体安全解决方案，从根本上阻断其可能性。
- **考虑多种技术并用，**包括加密、标记化、微隔离、权限分配与数字化职权管理、选择性校验、数据加扰等等。
- **如果企业的高值资产位于陈旧系统中，切勿尝试一次性加固所有资产。**与之相反，应首要厘清所有的数据访问点及安全控制点并考虑添加新的保护措施，直到完成对原有系统的迁移或更新改造。如果现有系统无法得到适当加固，则需设法限制访问权限并提升监控水平。企业务必全力以赴，实时监测自身的薄弱环节。
- **请谨记，所有安全工作的焦点均为数据保护——对数据进行加密，将其保留在系统中最安全的位置。如果同样的控制手段无法适用所有访问数据的人员，那么充其量也只是移动了问题出现的节点。**为了充分保护高值资产，企业必须始终从“人员维度”出发进行思考。

同时在本地和云端开辟网络飞地，由此构建防御体系

企业边界已不再固若金汤，于对手而言，发现缺口窃取信息已并非难事。那些原本希望在边界构筑稳固壁垒的企业如今需要将防线延伸至围墙以外，直至云端、业务现场和远程控制室。企业应考虑建立多个“网络飞地”（Enclave）——并依靠这种设于内部或外部的安全环境，更有效地监视用户的登陆和退出、以及应用程序的运行状况，从而限制攻击者的可操作性。这样一来，即使企业边界被突破，飞地仍可保持安全。我们不妨将其想象为一艘船——即便船体破损，下层舱室的硬质隔板也能避免沉船事件的发生。同理，网络中硬性分区的飞地亦可防止数据裂缝在整个企业中的横向扩大。

建立并执行威胁搜寻程序

曾几何时，企业普遍认为，在入侵行为发生时再启动响应方案也为时不晚，不过这种策略已然失效。当下，最妥善的办法是采取持续响应模式——始终假设企业已被攻破，并积极调动事件响应和威胁搜索团队不断寻找下一次可能出现的数据泄露（“在对手找到你之前发现他们”）。

网络飞地可以防止对手在整个企业中横向移动和连续获取敏感数据。

打造卓越安全基础

及时修补系统固然不易，其优先级却毋庸置疑。

建立并启用攻击模拟和重大灾难等情境

搭建这些情境并开展测试，实时观察端到端的有效性。通过此举，您可以判断和验证能否有效侦测到攻击者，同时确保自身人员已为此做好准备。

对应用系统进行安全扫描

安全扫描工作非常重要，因为其有助于识别实际存在的漏洞——理想情况下，这些漏洞一旦出现就应被及时察觉并报告。不过，它只是整个安全框架的组成部分之一。为了优化安全扫描工作，企业首先需要尽可能地掌握企业信息资产状况，即全面了解所需扫描的对象。其次，明确资产归谁所有、以及由谁修复。接下来，确保您的安全团队能够验证扫描结果并快速消除误报。此外，还应将安全工作集成到应用系统开发生命周期当中，争取在扫描之前便能修补错误，以此降低成本。扫描还可估算出消除薄弱环节所需的时间，帮助企业优先处理高风险部分。应用安全扫描不仅需要使用工具，还需建立端到端的工作计划，以经济高效的方式降低安全风险。

修补系统

这听起来并非难事，但却需要周全的筹划。企业之所以无法修补自身系统，往往是因为身处不断变化的系统环境之中。他们不清楚全部系统中有多少正处于活跃状态。即便手握系统清单，也很难准确掌握平台上所有软件的不同版本——而针对操作系统特定版本的补丁，或许会破坏正在运行的应用程序。面对此种境况，企业需要的是一套威胁情报解决方

案助其一臂之力：当保存高值资产的某些应用程序需要得到修补以避免被利用时，威胁情报平台将自动发出通知；威胁情报解决方案还必须具备对异常情况的协调能力，例如修补程序要求重启系统，但系统却禁止了这一功能。

限制、监视和访问隔离

企业应尽可能多地使用双重验证技术，并基于工作职能自动分辨人员可访问的具体数据和系统。在推动访问控制向微隔离方向发展的过程中，企业应清晰认识到，即使不同职能的人员、出于不同目的，必须利用敏感数据作出判断时，他所看到的也不应是全部数据。微隔离可以根据每位员工的角色和职责，向其展示所需看到的内容，同时遮蔽其余部分。此举还可最大限度地降低泄露事件引发的损害——即便不法分子盗用了任何一名用户的身份凭证，也只会得到部分数据。若想获取全部或更多数据，那对攻击者来说可谓是困难重重。

监测异常及可疑活动

持续不断、高度警惕地监视，不仅是为了阻止未经授权的访问，更能防范未知威胁和可疑的用户行为。

根据每位员工的角色和职责，选择性地给予访问权限。

打造卓越的安全基础

兼顾战略及战术威胁情报

企业应建立可持续的威胁情报机制用以收集并整理战略及战术性质的威胁情报。战略性威胁情报是指来自多种来源的内部或开放的人为情报——例如，声称特定版本的Apache Struts系统易受攻击、以及该漏洞会如何被利用的电子邮件。其他形式的战略情报则可能针对某些行业或技术提供相关深入分析、或是会改变攻击者动机的地缘政治趋势信息。战术性威胁情报则涵盖各种自动馈送到企业系统中的自动化数据——例如，通过Palo Alto Networks或Qualys等途径将其直接发送至企业系统当中。一面是当下鱼龙混杂的网络环境，一面是利益相关者一手制造的刻意威胁，企业务必紧随时下最新发展动态，方可保护自身数据免受威胁。

构建安全生态系统

任何一家企业都并非孤岛，他们需要借助多元化的供应商支持系统来填补内部人才与技能之力所不能及。并在必要和适当的时候，寻求安全外包服务机构所提供的帮助。

为应对最坏情况做好准备

企业需要将事件响应计划转变为危机管理机制，一旦触发最坏状况，它便可发挥巨大作用。同时，应确保法务和沟通团队时刻警戒并随时能够采取行动。在不断排练该计划的过程中，企业便能熟稔的应对此类危机事件，并在下一次问题出现之前识别需要改进之处。企业必须做好应对灾难性网络攻击的准备——届时日常所用的电子邮件、IP电话和其他通信系统或许均会中断。面对这样的紧急状况，可以考虑在云端存储重要的联系信息，同时准备好将云系统用作电子邮件和语音通信的辅助平台。

企业一旦下定决心严防重大数据泄漏，就应立即行动，以数据为中心制定安全防护方案。

弥补任何缺陷都将有助于抵御不法行为，并最大限度地降低其负面影响。

更多了解不断发展的网络安全格局，以及可以为您加强防御的措施。

请联系：

杨嵩
埃森哲大中华区基础设施服务
董事总经理
s.yang@accenture.com

贾文军
埃森哲大中华区基础设施服务
总监
wenjun.jia@accenture.com

欢迎访问www.accenture.cn

关于埃森哲

埃森哲公司注册成立于爱尔兰，是一家全球领先的专业服务公司，为客户提供战略、咨询、数字、技术和运营服务及解决方案。我们立足商业与技术的前沿，业务涵盖40多个行业，以及企业日常运营部门的各个职能。凭借独特的业内经验与专业技能，以及翘楚全球的交付网络，我们帮助客户提升绩效，并为利益相关方持续创造价值。埃森哲是《财富》全球500强企业之一，目前拥有约42.5万名员工，服务于120多个国家的客户。我们致力驱动创新，从而改善人们工作和生活的方式。

埃森哲在大中华区开展业务30年，拥有一支约1.5万人的员工队伍，分布于北京、上海、大连、成都、广州、深圳、香港和台北。在新常态时代，我们将更创新地参与商业和技术生态圈的建设，帮助中国企业和政府把握数字化力量，通过制定战略、优化流程、集成系统、部署云计算等实现转型，提升全球竞争力，从而立足中国、赢在全球。

详细信息，敬请访问埃森哲公司主页www.accenture.com以及埃森哲大中华区主页www.accenture.cn。

关于埃森哲安全服务

埃森哲安全服务致力于帮助企业由内及外地打造系统防御力，使其能够安心地专注于创新与增长。依托强大的全球网络安全实验室网络、针对客户价值链各环节的深入行业洞察和贯穿安全生命周期的服务，埃森哲持续为企业的宝贵资产给予端到端保护。依托我们提供的战略及风险管理、网络防御、数字身份、应用安全和网络安全管理服务等全面服务，埃森哲助力全球企业有效应对已知和未知的网络安全风险。欢迎关注我们的推特账号@AccentureSecure或访问埃森哲安全服务博客。