内部风险管理

内部风险管理

由被授权人员造成的内部威胁都有很多的研究记录和法庭案件记录。根据美国的 ACFE 的记录，企业每年因诈骗而受到的损失大约在 6520 亿美元。不幸的是，内部威胁不只是诈骗，还要考虑到怠工，懒散，人为误差和外部的利用。如果你还没有认真审视过你的组织内部的威胁管理，那么现在就应该看看了。

数据结构和影响

组织内部的威胁控制的执行过程，要以把重要信息按照影响级别分为机密性，完整性和可用性。

- 风险管理：数据结构和影响分析

基线管理与控制

影响类别的基线控制标准可以分为高、中、低控件附录的基线。一些情况下，基线控件是程序化与技术化相对的（比如，存储加密和密钥状态下的敏感文件，同时使用跨削减碎纸机（cross-cut shredder）来处理这些文件 ）。知情人员熟悉内部控件，就可以找到一种方法，进入某个单一控件或执行较差的控件。尤其要注意其后的控制类型。副标题简介

- 风险管理：基线管理与控制
- 风险管理：基线控制的执行

风险管理审计

了确保敏感数据和宝贵资产得到适当的保护，需要风险管理审计功能。仔细检查哪些人有权访问敏感数据，以及这些访问是否恰当。审计功能也应该可以监控系统和内部人员，以检测非法活动。审查审计跟踪，以寻找安全事件和滥用权限。核实目录许可，薪金控制和会计系统配置。确保备份软件得到合适配置，并备份无误。在完全开放的允许下存储审查敏感信息的网络共享部分。进行办公场所的审查，以确定安全策略和程序在实际中是否得到遵守。

- 风险管理审计

风险管理参考文献

这一部分提供了内部风险管理的一些参考文献。

- 风险管理参考文献

风险管理：数据结构和影响分析

由被授权人员造成的内部威胁都有很多的研究记录和法庭案件记录。根据美国的 ACFE 的记录，企业每年因诈骗而受到的损失大约在 6520 亿美元。不幸的是，内部威胁不只是诈骗，还要考虑到怠工，懒散，人为误差和外部的利用。如果你还没有认真审视过你的组织内部的威胁管理，那么现在就应该看看了。

组织内部的威胁控制的执行过程，要以把重要信息按照影响级别分为机密性，完整性和可用性。NIST SP 800-60 提供了信息类别和影响解析的例子。

数据类型	机密性	完整性	可用性
商业机密	高	高	中
人力资源	高	中	低
金融	高	高	中

既然数据已经按照机密性，完整性和可用性解析分类，就要识别系统边界。边界应该包括系统，数据流，网络，人才和硬拷贝输出。

(作者：SearchSecurity.com 译者：Tina 来源：TT 中国)

风险管理：基线管理与控制

下一步，建立可以详细确定影响类别的基线控制标准。NIST SP 800-53 提供了可以分为高、中、低控件附录的基线。澳大利亚 NSW 基线控制标准（Australian NSW Baseline Controls）和 VISA 支付卡行业数据安全标准（VISA PCI Data Security Standard）都很成功。一些情况下，基线控件是程序化与技术化相对的（比如，存储加密和密钥状态下的敏感文件，同时使用跨削减碎纸机（cross-cut shredder）来处理这些文件 ）。知情人员熟悉内部控件，就可以找到一种方法，进入某个单一控件或执行较差的控件。尤其要注意其后的控制类型。

人力资源

人力资源部应当遵循明确定义的正在处理和无法处理的程序。对所有员工进行犯罪背景调查、信贷检查和雇用认证，包括承包商、临时工和保洁人员。定期对高敏感职位的人员重复进行背景核查。要求所有的员工签署一份文件，证明他们已经阅读并理解了信息安全策略。确保第三方承包商和服务提供者遵守你的安全要求（比如，对新员工进行雇用和背景核查）。建立一个匿名欺诈、浪费和滥用职权的报告机制。许多内部犯罪，都是雇员所为。当雇员被确定为受到困扰或心怀不满时，要警告信息安全部。

安全意识程序

所有的员工必须熟悉安全策略和安全程序。建立一个综合的意识程序，包括带有测试的年度安全培训，邮件提示，海报，来自高层管理层的支持信，自我评估调查，认知午宴及安全网站。最好再用认知简报进行补充培训。简报可以给员工提供提出问题的机会，并且可以让信息安全团队主动提倡安全。

准入控制

准入批准应该基于那些履行日常工作时，需要知道的人员。如果可能，准入资格的分配要基于职务。将担任 IT 职务的人员考虑在内，包括程序开发者，系统及应用程序的管理员等等。将职务列入帐目和薪水的范畴内。所有的准入申请都要正式入档，并且要由直接的管理员批准。对于敏感系统的准入，还需要得到数据所有者的批准。为了确保极度敏感信息的安全，要实行双人完整控制（例如，商业机秘）。为员工配置出入卡以约束员工履行职务时需要进出的场地和时间。经理每 15 分钟就要对他们直接报告中的特权正式签字。当雇员被调到一个新的岗位，他们可以保留原来职务的准入。

职务的分割应该作为辅助控制。举一些例子：职务分割应该需要创建一个账户并书写一张支票。程序开发者不能进入生产系统。代码检查要由其它人进行，作者不可以。管理员不应是检查日志的唯一团体。想要了解更多信息，请查阅 ISACA separation of duties matrix。

建立应用软件，该软件可以查阅敏感数据，同时拥有下载整个数据库的能力。要防止文下载件，可以利用终端服务器提供数据和系统的远程接入（例如当开发软件的时候）。

管理员

管理员对系统和应用程序拥有完全的控制权。禁止使用默认的管理员账户，以实现责任制。保证 Windows 系统的管理员使用唯一的、并与其姓名捆绑在一起的帐号，且在安装过程中，删除服务器中的默认管理员账户。配置 Unix 和 Linux 系统，迫使管理员实名登陆，然后使用更改用户指令（su）获取根目录管理权限。应用程序的管理员及操作人员在履行职务过程中可能需要访问一些根目录。使用软件派给其访问特定根目录的权限（例如 sudo，RBAC，RSBAC 或 Power Broker）。对数据库进行加密，以防止那些可以进入到备份中的系统管理员和其他任何人浏览敏感信息。

工作站

笔记本电脑可以储存大量的敏感信息，并且经常成为盗窃者的目标。基于商务用途，并考虑信息处理的类型，以此为基础分配笔记本。美国政府最近已经要求对笔记本电脑实

施加密和双因素认证技术。执行他们的要求是明智的做法。设置生物识别密码作为辅助控制。

限制台式机团队进入工作站。这项权限可以用于安装未经许可的软件或绕开安全控制（例如使反病毒软件失效或倒转系统硬化配置）。在履行职责时，有些员工的确需要管理权限。只能给这些人例外，并且需要经理的正式签字。

最后，对准许使用 USB 存储设备的人员进行限制。它们可以用来下载敏感数据，同时也可以将病毒带入网络中。

网络安全

通过最优化的安全措施配置防火墙。把带外流量限制在 HTTP 和 HTTPS 等普通服务上。使用应用程序代理把流量限定在指定的协议。建立单独的规则，把对外文件传输限制在一套授权的用户和系统装置。限制面向办公室和具体的系统、点的部门和协议之间的访问。使用网络隔离来限制对以敏感数据为基础的系统主机的访问（例如 DMZ、外联网和 VLANs）。限制点对点的文件共享服务，限制即时的、允许未授权的外部访问公司网络的通信和服务（比如，GoToMyPC，pcAnywhere 和在线 Citrix）。同样也要限制外部 email 网站。所有的 email 应该在使用公司系统的前提下进行操作。如果一个员工需要访问上面服务中的其中一项，应确认其商业要求，并建立一个特别规则来满足他们的需要。最后，扫描发出的邮件的敏感信息，比如项目代码。应该使用一个 SSL 扫描器来扫描加密的信息流。

社会工程

诈骗犯可能试图从得到授权的员工那里提取信息，或者代表他们采取行动。解决这样的威胁，有三种基本的方法：（1）提高社会工程师使用的技术的意识，（2）建立明确的过程来保护敏感信息和有价值资产，（3）提供升级路径。

备份

每年至少进行一次关键系统的恢复测试。已经知道，心怀不满的雇员通过破坏关键数据，通过脱机备份轮换等待机会传播，来破坏公司或者勒索公司。使用工作站的备份，提供员工活动的记录。加密备份磁带和电子商务跳马数据，以保持脱机时敏感数据的机密性。

审计跟踪和监控

到目前为止，我们主要讨论了预防性控制。检测控制是必要的，因为授权的职员需要权限来完成他们的工作。这就使我们考虑到审计跟踪和监控。为每个系统组件（例如，网络设备，操作系统，商业软件和定制的应用程序）配置审计跟踪。研究每个组件的记录功能，并配置它来记录重大事件。记录任何有管理特权的个体所采取的行动（例如命令的执行，和审计追踪的获取）。审计跟踪必须受到文件权限的保护，与中央日志服务器同步实时，以防止修改。一旦集中，自动化程序应当检查日志，并把通知送给合适的人员。数据库管理员可以访问敏感信息，所以他们必须受到监测。使用入侵检测软件鉴别可疑活动。使用文件完整的软件来监控配置文件和敏感数据。

（作者：SearchSecurity.com 译者：李娜娜 来源：TT中国）

风险管理：基线控制的执行

基线层依据数据的机密性，完整性和可用性的分类进行控制。这一步把企业的组织风险和信息安全控制连接起来。很多企业都面临法规遵从和安全最佳实践执行方面的挑战。不要失去大片的线索，控制的目的是把业务和无法接受的风险隔离开来。基于数据敏感性和影响级别的应用控制的简单过程与大部分的法规遵从的关注点相联系。任何基线控制的分离都需要正式的例外，而且要经过信息安全管理和商业的认可。

（作者：SearchSecurity.com 译者：Tina 来源：TT中国）

风险管理审计

为了确保敏感数据和宝贵资产得到适当的保护，需要风险管理审计功能。仔细检查哪些人有权访问敏感数据，以及这些访问是否恰当。审计功能也应该可以监控系统和内部人员，以检测非法活动。审查审计跟踪，以寻找安全事件和滥用权限。核实目录许可，薪金控制和会计系统配置。确保备份软件得到合适配置，并备份无误。在完全开放的允许下存储审查敏感信息的网络共享部分。进行办公场所的审查，以确定安全策略和程序在实际中是否得到遵守（例如，敏感材料没有丢之不理，锁定工作站屏幕以及确保笔记本电脑安全）。

当工作人员离职或者当他们的角色转变时，确保系统地废除访问权限。从人力资源部门获得目前职员的名单，并与活跃帐户（例如网络帐户，远程接入和服务器上的本地帐户）做比较。单机应用程序也要受到检查（例如语音邮件和公司名录）。

检查物理安全访问日志。特别注意工作时间后的和周末的雇员访问。如果发现可疑行动，可以参考监视录像和系统审计审查。

每个季度对上述确定的内容至少进行一次评估。尽可能多地进行自动化审计，以节约资源，并检测发生的安全侵害。如需更多资讯，请参阅 IIA GTAG 连续审计指南。

这篇文章简单介绍了如何减轻内部人士威胁。想要了解更多，请参阅“阻止和发现内部人士威胁的 US-CERT 常识指导”。ACM 职业欺诈和滥用报告提供了如何诈骗的实例，以及预防和发现诈骗指南。雅虎内部威胁组（Yahoo insider-threat group）是一个很好的资源，可以时刻了解当前事件和最新发展，

正如你所看到的，来自内部的威胁是确实存在的。信任是必要的，但是进行控制和监管。

（作者：SearchSecurity.com 译者：李娜娜 来源：TT 中国）

风险管理参考文献

以下列出风险管理的参考文献：

1. ACEF 职务欺诈与滥用职权报告
（ACFE Occupational Fraud & Abuse Report）；

2. 美国安全局信息安全评估方法体系
（NSA INFOSEC Assessment Methodology (IAM)）；

3. Dawn Cappelli: 预防内部怠工
（Dawn Cappelli: Preventing Insider Sabotage）；

4. Kelly Martin: 美国政府部门托管笔记本电脑安全
（Kelly Martin: U.S. Gov't Mandates Laptop Security）；

5. Sharon Gaudin: 内部怠工案例研究
（Sharon Gaudin: Case Study of Insider Sabotage）。

文献连接：
http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1213413,00.html

（作者：SearchSecurity.com 译者：Tina 来源：TT 中国）