信息资产的分类与控制

一、前言

根据《光明日报》2004 年 2 月 9 日的统计数字，国内 2003 年电子政务信息安全市场规模超过 5 亿元，金融信息化安全市场规模约有 4.5 亿元，电信行业信息安全市场规模不低于 10 亿元，石化、电力、交通运输、制造、教育、卫生等行业和个人市场的安全市场规模约有近 10 亿元。从 2003 年的总共将近 30 亿元市场情况看，防火墙、防病毒、入侵检测系统、虚拟专用网设备等占了整个安全产品市值的绝大部分，企业花费在信息安全管理、咨询、安全意识、培训、教育方面的费用微乎其微。

从统计数据我们可以分析出，目前在用户中普遍比较流行的信息资产保护观点是：通过部署防病毒软件、防火墙及入侵检测系统等边界保护与检测设备来保护储存在计算机中的数据资产免受非法入侵。

然而信息资产真的只是储存在计算机中的数据吗？

英国泰晤士报曾对企业中知识的储存方式做了一个调查，结果发现在一个企业的知识结构中，26%的知识以纸质文件的形式储存，20%的知识以电子文件存储，42%的知识储存在员工的头脑中，12%以其他形式存在。

Ernst &Young 在 2002 年经过调查发现：国家政府和军队信息受到的攻击 70%来自外部，而银行和企业信息受到的攻击 70%来自于内部。中国国家信息安全测评认证中心提供的调查结果也得出了相似的结论。
这就是说我们花了绝大部分的钱，保护了只占信息资产 20%的数据资产！而且我们的技术手段还谈不上 100%地有效保护这 20%的数据资产。

也许，我们应该重新定义一下什么是信息资产了。

二、什么是信息资产？

信息可以理解为消息、情报、数据或知识，它可以以多种形式存在，可以是组织中信息设施中存储与处理的数据、程序，可以是打印出来的或写出来的论文、电子邮件、设计图纸、业务方案，也可以显示在胶片上或表达在会话中消息。所有的组织都有他们各自处理信息的形式，例如，银行、保险和信用卡公司都需要处理消费者信息，卫生保健部门需要管理病人信息，政府管理部门存储机密的和分类信息。

无论组织对这些信息采用什么样的共享、处理和存储方式，都需要对敏感信息加以安全、妥善的保护，不仅要保证信息处理和传输过程是可靠的、有效的，而且要求重要的敏感信息是机密的、完整的和真实的。为达到这样的目标，组织必须采取一系列适当的信息安全控制措施才可以使信息避免一系列威胁，保障业务的连续性，最大限度地减少业务的损失，最大限度地获取投资回报。

在 ISO17799 中，对信息的定义更确切、具体：“信息是一种资产，像其他重要的业务资产一

样，对组织具有价值，因此需要妥善保护”。

我们习惯于把计算机、通讯设备、磁介质等看成信息资产，而不习惯于把对组织有重要价值的档案资料、人员、企业形象、服务等看作是资产，往往忽略了对这些资产的保护，而实际上这些资产对组织的业务持续性来说是至关重要的。

ISO17799 列出了常见信息资产有：
●数据与文档：数据库和数据文件、系统文件、用户手册、培训材料、运行与支持程序、业务持续性计划、应急安排
●书面文件：合同、指南、企业文件、包含重要业务结果的文件。
●软件资产：应用软件、系统软件、开发工具和实用程序
●物理资产：计算机、通讯设备、磁介质（磁盘与磁带），其他技术设备（供电设备、空调设备）、家具、办公场所
●人员：员工、客户
●企业形象与声誉
●服务：计算和通讯服务，其他技术服务（供热、照明、电力、空调）

组织在实施 ISO17799 时，不一定要拘泥于以上资产类型，还可以列出适合自身需要的其他信息资产。

下面我们结合 ISO17799 在这个领域的措施目标与措施，来详细讨论如何识别信息资产，并进行科学而有效的分类，然后在各个管理层对资产落实责任，进行恰当的管理。

三、控制目标与控制措施

1、控制目标－落实资产责任

应当为所有主要财产确定所有权人，并且为维护适当的管理措施而分配责任。可以委派执行这些管理计划的责任。被提名的资产所有者应当承担保护资产的责任。

控制措施－资产的清单

应该列出并维持一份与每个信息系统有关的所有重要资产的清单。

在信息安全体系范围内为资产编制清单是一项重要工作，每项资产都应该清晰地定义，合理地估价，在组织中明确资产所有权关系，进行安全分类，并以文件方式详细记录在案。

具体的措施如下：

组织可根据业务运作流程和信息系统基础架构识别出信息资产，按照信息资产所属系统或所在部门列出资产清单，将每项资产的名称、所处位置、价值、资产负责人等相关信息记录在资产清单上。

根据资产的相对价值大小来确定关键信息资产，并对其进行风险评估以确定适当的控制措施。

对每一项信息资产，组织的管理者应指定专人负责其使用和保护，防止资产被盗、丢失与滥用。

定期对信息资产进行清查盘点，确保资产账物相符和完好无损

以上措施中，确定资产的价值是难点，信息资产的价值不仅仅要考虑其自身的价值，还要考虑其对业务的重要性和一定条件下的潜在价值。比如：以同样价格的购买了二台同样配置的服务器，一台用于办公自动化，另一台用于处理财务总帐数据，这二台服务器的账面价值虽然一样，但作为信息资产进行评估时，其信息资产价值是不一样的，用于财务处理的服务器的相对价值一般要大于办公自动化服务器的相对价值。

资产价值常常是以安全事件发生时所产生的潜在业务影响来衡量，安全事件会导致资产机密性、完整性和可用性的损失，从而导致企业资金、市场份额、企业形象的损失。为了资产评估的一致性与准确性，组织应当建立一个资产的价值评估标准，对每一种资产和每一种可能的损失，例如机密性、完整性和可用性的损失，都可以赋予一个价值。

但采用精确的方式给资产赋值是较困难的一件事，一般采用定性的方式，按照事前建立的资产的价值评估标准将资产的价值划分为不同等级。

经过资产的识别与估价后，组织应根据资产价值大小，进一步确定要保护的关键资产。

在评估过程，为了保证没有资产被忽略和遗漏，应该先确定信息安全管理体系范围，这样资产的评审边界就建立起来了。评估资产最简单的方式就是列出组织业务过程中、安全管理体系范围内所有具有价值的资产，然后对资产赋予一定的价值，这种价值应该反映资产对组织业务运营的重要性，并以对业务的潜在影响程度表现出来。例如，资产价值越大，由于泄露、修改、损害、不可用等安全事件对组织业务的潜在影响就越大。基于组织业务需要的资产的识别与估价，是建立信息安全体系，确定风险的重要一步。

资产的价值应当由资产的所有者和相关用户来确定，只有他们才最清楚资产对组织业务的重要性，才能较准确地评估出资产的实际价值。

在对资产赋予价值时，一方面要考虑资产购买成本及维护成本，另一方面也要考虑当这种资产的机密性、完整性、可用性受到损害时，对业务运营的负面影响程度。在信息安全管理中，并不是直接采用资产的账面价值，比较实用的做法是以定性分级的方式建立资产的相对价值，以相对价值来作为确定重要资产的依据和为这种资产的保护投入多大资源的依据。

这种定性分级可以参照下表所示的方式：

资产定性分级表

分级类型	定性分级程度
相对较粗的分级	低、中、高
详细分级	可忽略、低、中、高、非常高
更详细的分级	（低）0、1、2、……、10（高）

2、控制目标－信息的分类

目标：确保信息资产得到适当程度的保护

应当将信息分类，指出其安全保护的具体要求、优先级和保护程度。

不同信息有不同的敏感性和重要性。有的信息资产可能需要额外保护或者特殊处理。

应当采用信息分类系统来定义适当的安全保护等级范围，并传达特殊处理措施的需要。

控制措施－信息资产分类原则

信息的分类及相关的保护控制，应适合于企业运营对于信息分享或限制的需要，以及这些需要对企业营运所带来的影响。

信息的分类和相关保护措施应当综合考虑到信息共享和信息限制的业务需要，还要考虑对业务的影响，例如对信息未经授权的访问或者对信息的破坏。一般说来，信息分类是一种处理和保护该信息的简捷方法。

信息分类时要注意以下几点：

信息的分类等级要合理

信息和处理分类数据的系统输出应当按照其对于组织的价值和敏感性加以标识。应当仔细考虑分类范畴的数量以及使用这种分类所带来的好处。过于复杂的分类规划可能很累赘，而且使用和执行起来也不经济实用。解释其它组织发送过来的文件上的标签时应当十分小心，相同或者相似的标签名称可能具有不同的含义。

信息的保密期限

经过一段时间以后，信息常常会变得不再敏感或者不再重要了，例如在敏感信息被公开发布以后，原来的分类就没有意义了。如果把安全保护的分类划定得过高就会导致不必要的业务开支。对于任何信息的分类都不一定自始至终固定不变，可能按照一些预定的策略发生改变。组织制定信息分类指南时应当考虑到这些情况。

谁对信息的分类负责

信息的始发人或指定的所有权人应当承担确定信息类别的责任，例如对一份文件、数据记录、数据文件或者磁盘进行分类的责任，以及定期检查这些分类的责任。

比如：《中国人民共和国保守国家秘密法》第九条对国家秘密是这样划分的等级的，国家秘密的密级分为“绝密”、“机密”、“秘密”三级。“绝密”是最重要的国家机密，泄露会使国

家的安全和利益遭受特别严重的损害；“机密”是重要的国家秘密，泄露会使国家的安全和利益遭受严重的损害；“秘密”是一般的国家秘密，泄露会使国家的安全和利益遭受损害。

控制措施－信息的标识与处理

应当制定信息标识及处理的程序，以符合组织所采行的分类法则。

为信息标识和处理定义一个符合组织分类标准的处理程序是非常重要的。这些程序要涵盖实物形式和电子形式的信息。对于每种分类，应当包含以下信息处理活动的程序：

复制
存储
通过邮局、传真和电子邮件的信息发送
通过口头语言的信息传递，包括通过移动电话、语音邮件和录音电话传送的信息。
销毁

对于那些含有被划定为敏感或者重要信息的应用系统，其输出应当带有适当的分类标识。该标识应当反映根据组织规则而建立的分类。需要考虑的项目包括打印的报告、屏幕显示、存储介质（磁带、磁盘、CD、卡式盒带）、电子消息和文档传输。

一般来说，物理标识是最合适的标识形式，一些信息资产例如电子文档无法加上物理标识时，可以采用电子标识。

四、案例
下面是一个简化的信息敏感性分类策略的案例，供读者参考：

ABC 科技股份有限公司
信息敏感性分类策略

1.0　目标

制定信息敏感性分类政策是为了帮助员工判断什么样的信息的可以向非组织成员开放，什么样的信息属于敏感信息，未经适当授权不得向外界透露。这里所提到的信息是指通过任何方式存储与共享的信息，包括：电子信息、纸质信息和以声音或视频方式共享的信息（如：电话、视频会议）等。

所有员工都应当熟悉本政策规定的敏感信息分类标签办法和敏感信息管理指南。员工可以根据分类定义标准和管理指南来保护信息，另一方面也可以采用通用最佳实践的办法来保护公司的机密信息。（例如，员工不应该把 ABC 公司的机密信息遗留在无人值守的会议室里）

2.0　范围

ABC 公司的所有信息可以分成两种类型：公开信息与机密信息。

公开信息是由公司内的授权人员宣布可公开的信息，这些可公开的信息不会对公司的信息安全造成损害。

机密信息是指公司内部所有不可公开的信息，这些信息属于敏感信息，需要以安全的方式加以保护。有些敏感信息需要非常仔细地加以保护，例如：商业机密，研发程序，潜在收购对象以及其他对 ABC 公司具有重要商业价值的数据。有些敏感信息比如电话号码薄，公司一般性信息，人事情况等，只需采用一般的保护措施，不需要像前一种数据那样严格。

3.0 策略

下面的管理指南介绍如何在不同的敏感级别下保护公司信息(硬拷贝形式及电子格式的信息标签指南)。这些指南仅作为一个参考，在不同的环境条件下，每一种敏感级别下推荐的信息保护办法可能或多或少地会有一些变化。

3.1 最小敏感性信息：公司的一般信息、一部分不重要的人事与技术信息。

在对信息资产做标注时，应在显著位置写上“ABC 机密”。如果信息不作标注，那么这种信息将被默认为

“ABC 机密”，除非由公司授权人员明确地宣布为公开信息。
最小敏感性信息分类及管理策略如下：（略）

3.2 比较敏感的信息：公司的业务、财务、技术信息、大部分人事信息。

由于敏感程度增加了，在对信息资产做标注时，应在显著位置写上“ABC 机密－内部使用”。

比较敏感性信息分类及管理策略如下：（略）

3.3 非常敏感的信息：影响公司成功的核心商业机密、运营信息、人事信息、财务信息、技术信息、源代码等。

对于这类非常敏感的信息，在对信息资产做标注时，应在显著位置写上“ABC 机密－限制使用”。

非常敏感信息分类及管理策略如下：（略）

4.0 执行纪律

对有意或无意地暴露公司信息，对违反此政策的任何员工将要按公司惩戒程序进行处罚，甚至开除，情节严重者还将面临民事或刑事诉讼。

5.0 版本历史

2001 年 10 月 10 正式起用，版本号 1.0
2001 年 12 月 5 日第一次修改，版本号 1.1
2002 年 9 月 19 日第二次修改，版本号 2.0