

信息安全简介

1. 信息的概念

自上世纪 90 年代，随着互联网在全球范围内的兴起，我们的世界被“第三次浪潮”推进了信息的海洋，我们的社会生活跨入了“信息的时代”。“信息”，“information”，这个词汇绝对可以排进本世纪前十年最常用词汇表。

但是，如果请哪一位来给“信息”下个定义，或者解释一下什么是“信息”，想必还是很有难度的。

信息是“我们在适应外部世界，控制外部世界的过程中同外部世界交换的内容的总称”。

——《控制论——动物和机器中的通讯与控制问题》，美国数学家、控制论的奠基人诺伯特·维纳。

信息是反映事物的形成、关系和差别的东西，它包含于事物的差异之中，而不在事物本身。

——《信息论：新的趋势与未决问题》，意大利学者朗高。

笔者是物理专业毕业，从物理学的角度来看，我们的世界就是能量不同形式的表现，电、磁、声、光、热等等，并且还处于不停地转化和耗散之中。物质是能量的表现形式之一，属于有形实体，还有无形实体，比如电磁场、引力场等。而这些实体的变化和相互作用的表现就是信息，这是广义的信息。而我们正是通过这些“表现”，认知和识别这些实体及其相互关系。信息同样借助于这些有形实体和无形实体存在和传递。

我们这个世界就是能量以各种形式的展现及其不停地转化的表现。尽管能量

是守恒的，但是能量的变化所散发出的信息是无穷的，信息代表了能量的变化。

2. 信息的价值

信息充斥着我们所存在的世界，随着科技的不断进步，获取、收集信息的手段不断翻新，分析、识别、处理信息的能力不断增强，愈来愈多的信息呈现在我们面前，我们正在前所未有的发现信息的价值。

每一个事物的存在都会在我们这个世界上留下印记，因为它的存在必然以与这个世界的交互才得以被感知，交互的发生会以多种形式显现，比如我们所熟知的声音、影像、文字等等这些听得到、看得见的感官输入信息形式，以及那些听不到、看不见的比如电磁辐射等形式。

我们与外部环境的每一个交互都会产生以不同形式存在的信息，其中一些的存在是我们所知晓的，另一些可能是我们所忽视的。举个例子，当我们使用电脑敲击键盘进行输入时，输入的内容会出现在显示器上，同时敲击键盘还会发生声响，这种声响同样携带着输入内容的信息，当第三者可以收集这些声响并通过特定的方法和手段对其进行分析后，他可以重放输入的内容。类似的情况也出现在针式打印机打印作业时，对于喷墨或激光打印机的类似研究也在进行中。

当我们认为某一类或某一条信息没有价值而被我们忽略或者摒弃时，往往是因为我们还未发现其所具有的价值，但其实信息的价值与生俱来，只是在其存在的生命周期过程中是否被我们发现，是否能够被我们所识别、所利用。

3. 信息资产

通过前面的论述，我们可以得出信息是具有价值的这一结论，有价值的东西是什么？我们一般称之为“资产”。因此，信息也可以被称为“信息资产”

(Information Asset)。

信息资产的表现形式是那些用于存储、传输、计算以及输入、输出信息的物理实体。

我的名字、电话属于信息，通讯录存储了这些信息，通讯录可能是一张纸，也可能是一个电子文档，那么这张纸或电子文档是信息资产。

网络是用于传输信息的设施，因此构成网络的路由器、交换机等设备也是信息资产。

PC 服务器或小型机等主机设备是通过计算对信息进行处理和设备，因此它也是信息资产。

操作系统、中间件、数据库、应用程序等构成了具备对特定信息的处理能力的计算环境，因此这些软件也是信息资产。

键盘、显示器是输入和输出信息的交互界面，它们也是信息资产。

那么我们一般如何面对有价值的事物呢？

——适当的保护，因为信息具有价值！价值不是金钱，但价值的折损往往带来金钱方面的损失！

4. 信息安全

信息安全似乎还没有一个确切的定义，西方人在这种情况下通常使用模型或要素的概念来应对这种难于用文字语言完整描述的情形，就像对软件质量的定义，也是通过软件质量模型来描述，这样的—个好处是在定义的同时还给出了可以度量或测量的对象模型。

4.1 信息安全的经典模型

信息安全的经典模型是 CIA 模型，即：

机密性（Confidentiality）

完整性 (Integrity)

可用性 (Availability)

4.2 信息安全的“帕克里安”六角模型

在传统的“CIA”三角模型基础上增加了三个要素，形成了“The Parkerian Hexad”模型，即“帕克里安”六角模型。它包括了6个安全要素：

Confidentiality (机密性)

指信息不为其他不应获得者获得。信息不应被未经授权的主体所知悉。比如电话通话内容被窃听，就是典型的机密性丧失的案例。

Possession or control (拥有或控制，即所有权)

财务上能否确认一项资产，很重要的一个判断标准是看该项资源是否为本单位所拥有或能够控制。

Integrity (完整性)

指信息在传输、存储的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现。

Authenticity (真实性)

指信息确实来自其所有者，能够对伪造的信息进行鉴别。

Availability (可用性)

保证合法用户对信息和资源的使用不会被不正当地拒绝。

Utility (实用性)

信息能够被用于特定的目的。比如对文档进行加密后忘记了密码，导致文档不可访问。

通过以上6个要素来标识一个信息资产的安全。

“帕克里安”六角模型目前还在信息安全专家们的辩论之中。因为业界虽然普遍认为传统的 CIA 模型应该被扩充，但对于扩充的新要素一直存在争论，比如“不可否认性（不可抵赖性）”、“可审计性”等等。