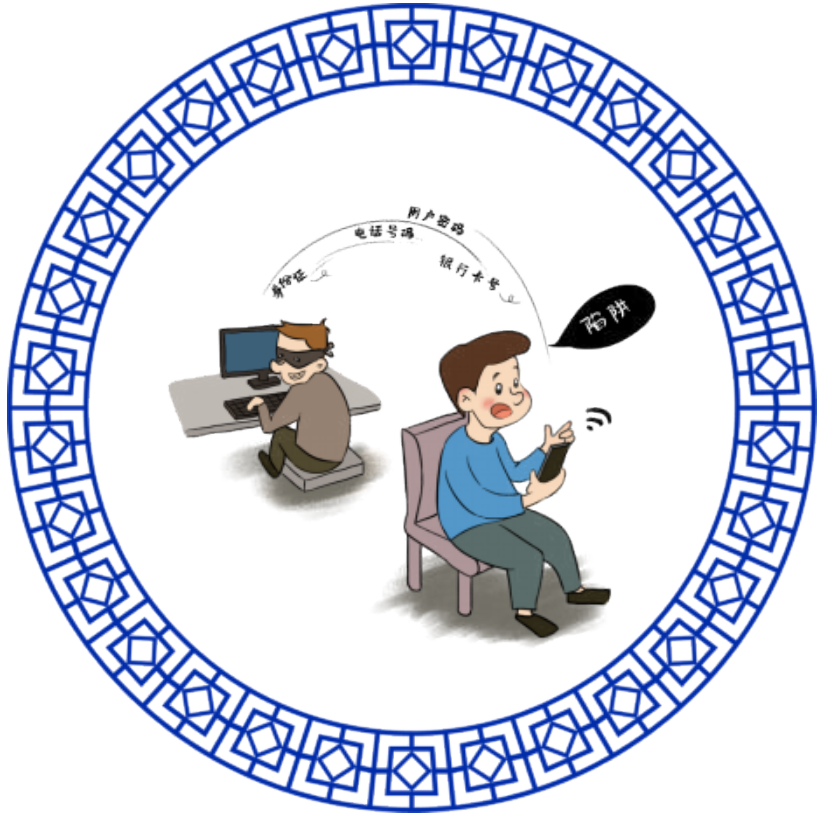
处置规程I应急演练I应急预案



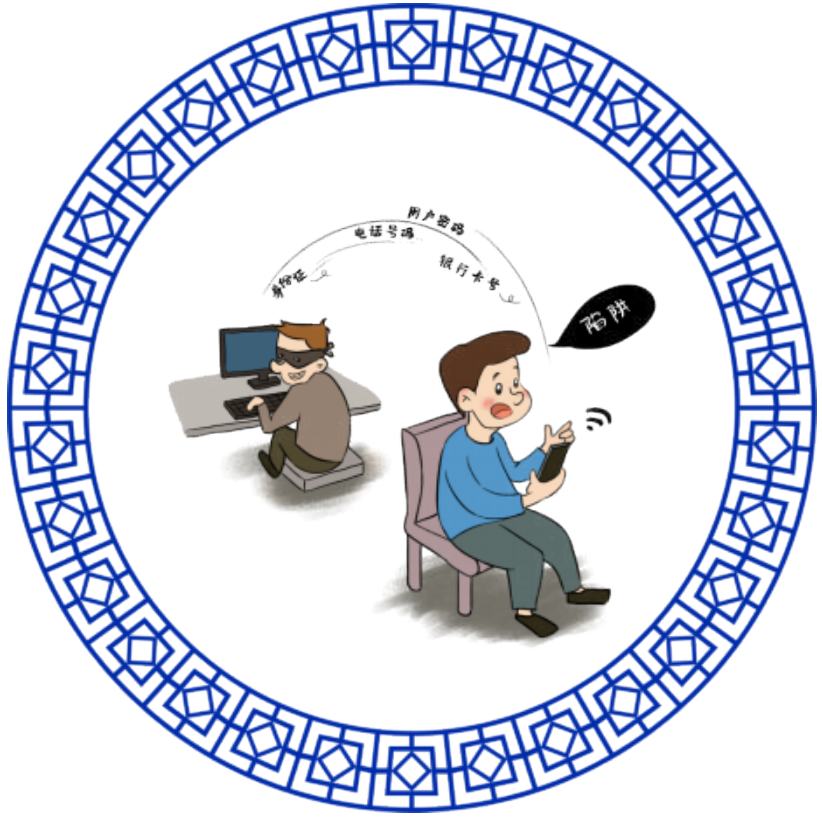
信息安全应急响应处置方案

Information Security Emergency Response Plan Training Courseware PPT

讲 授 ： XXX　　日期：2023.7

目 录

contents



PART ONE

信息安全应急响应及处置规程

处置规程I应急演练I应急预案

应急响应定义

应急响应

组织为了应对突发/重大信息安全事件的发生所做的准备，已及在事件发生后所采取的的措施。信息安全应急响应是指在计算机系统或网络上的威胁安全的事件发生后采取的措施和行动。——（信息安全应急响应计划规范GB/T 24363-2009）

响应对象

指针对信息系统所存储、传输、处理的信息的安全事件。事件的主体可能来自自然界、系统自身故障、组织内部或外部的人为攻击等。按照信息系统安全的三个特性，可以把安全事件定义为破坏信息或信息处理系统 CIA 的行为，即破坏保密性的安全事件、破坏完整性的安全事件和破坏可用性的安全事件等。 ——（信息系统等保体系框架GA/T 708-2007）

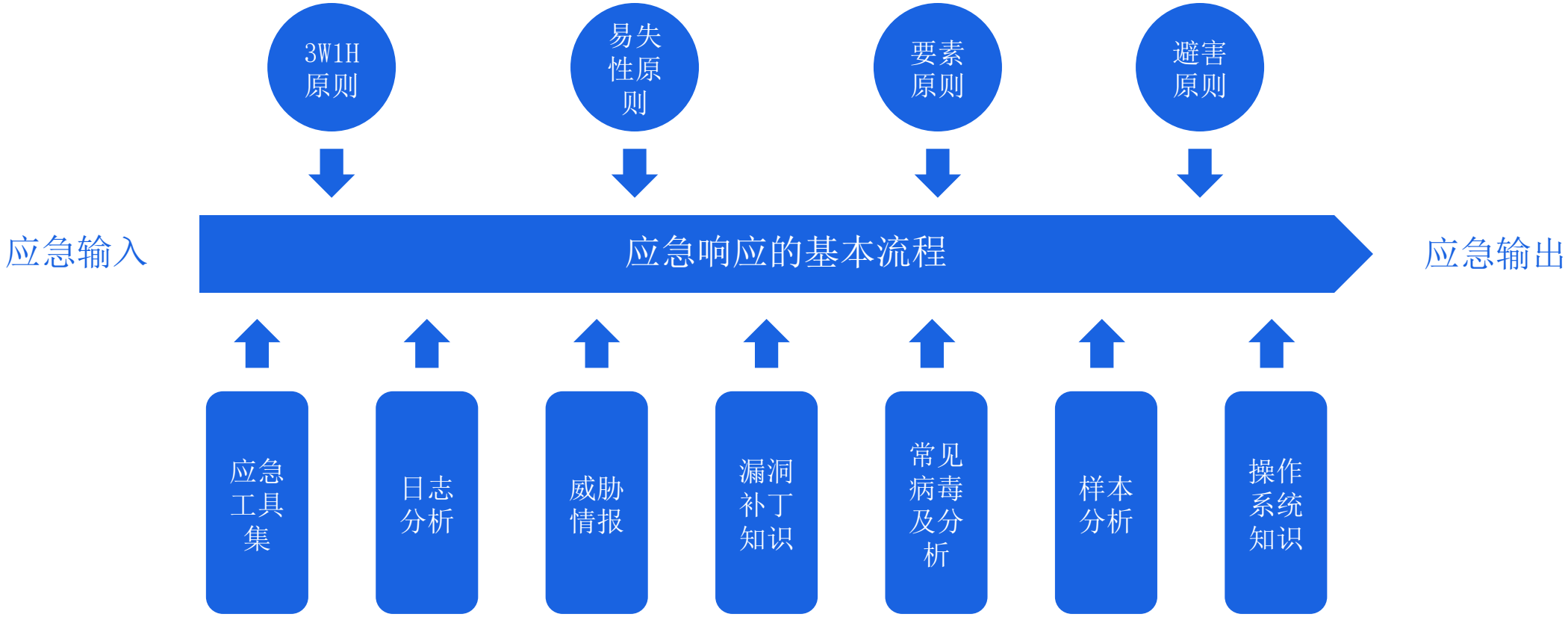
应急处置

启动应急响应计划后，应立即采取相关措施抑制信息安全事件影响，避免造成更大损失。在确定有效控制了信息安全事件影响后，开始实施恢复操作。恢复阶段的行动集中于建立临时业务处理能力、修复原系统的损害、在原系统或新设施中恢复运行业务能力等应急措施。——（信息安全应急响应计划规范GB/T 24363-2009）

信息安全应急响应要求—信息安全等级保护

应急预案管理	a）　应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； b）　应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； c）　应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次； d）　应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期； e）　应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。
安全事件处置	a）　应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点； b）　应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责； c）　应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； d）　应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等； f）　对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

信息安全应急响应要求—总体指导思想与原则



信息安全应急响应要求—总体指导思想与原则

3W1H原则

3W即Who、What、Why，1H即How，做应急响应要带着疑问来做事，一定要收集清楚这些信息。网络拓扑是怎么样的？需求是啥？发生了什么事？你能做什么？用户用了什么产品？产品版本多少？病毒库版本多少？多少主机中了？主机是普通PC还是服务器？服务器是做什么的？……信息收集越多，对应急响应越有利。

避害原则

做应急响应，要做到趋利避害，不能问题还没有解决，反而引入了新的问题。譬如，自己使用的工具被感染而不知情；给用户使用不恰当的工具或软件造成客户主机出现问题；给别人发样本，不加密，不压缩，导致别人误点中毒，最极端的场景就是给别人发勒索样本不加密压缩，导致别人误点中毒。

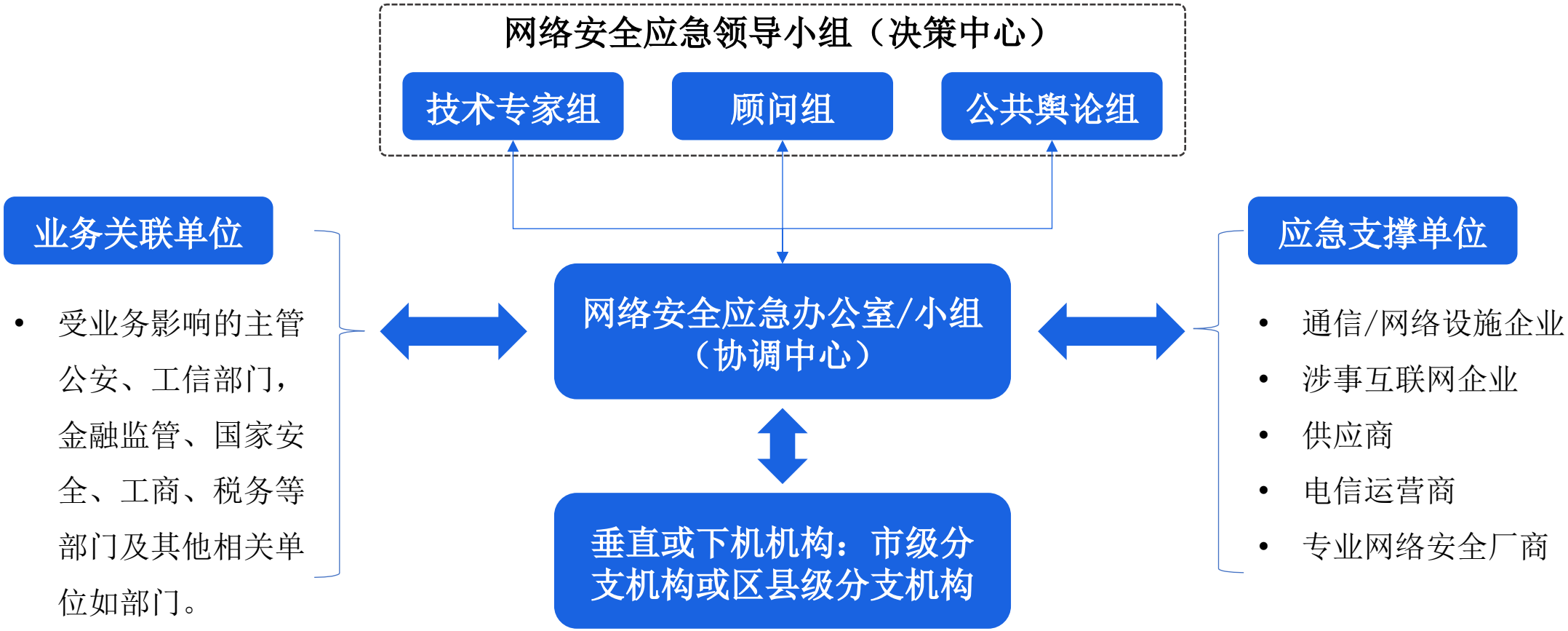
易失性原则

做应急响应免不了要做信息收集和取证的，但这里是有一定的先后顺序的，即最容易丢失数据，应该最先收集，其它的依次类推。

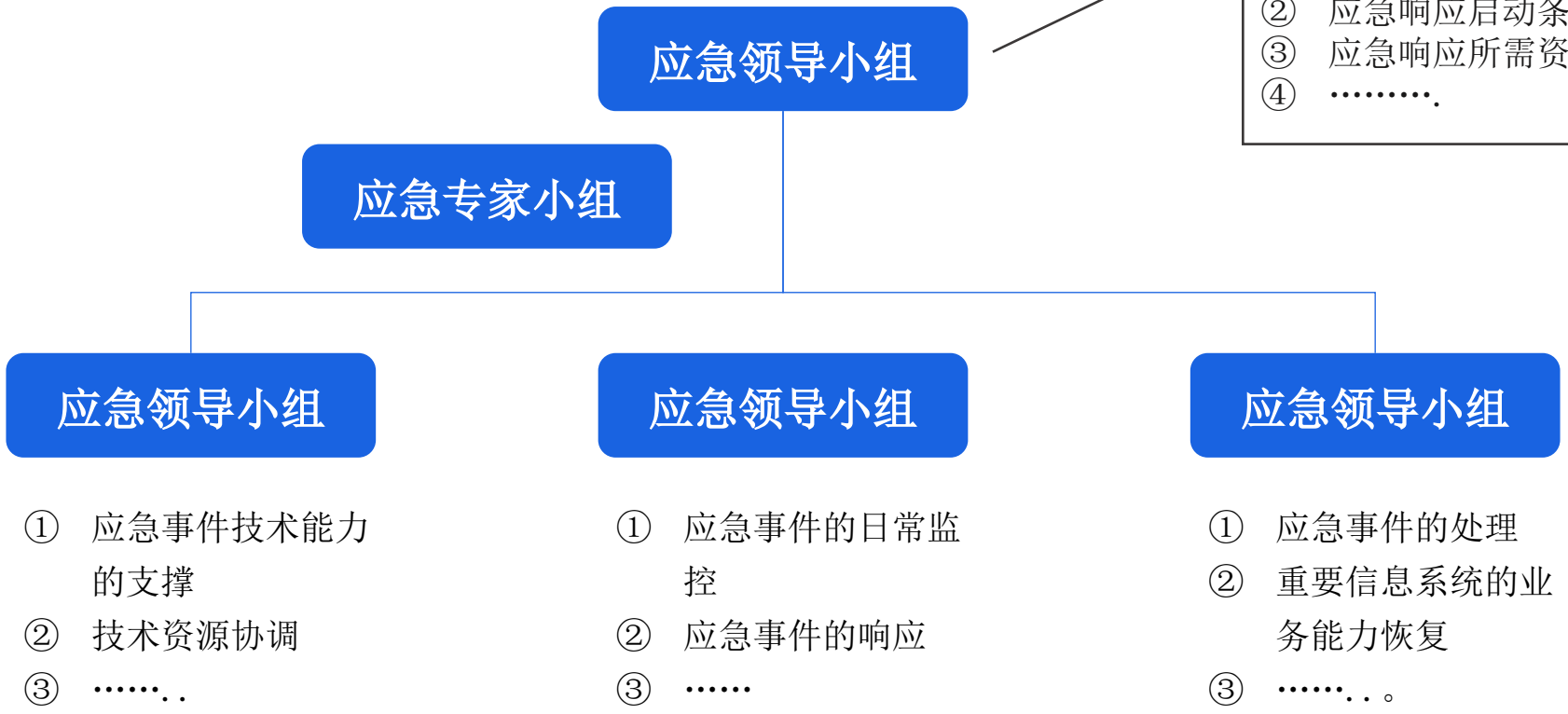
要素原则

做应急响应，主要是抓关键证据，即要素，这些要素包括样本、流量、日志、进程及模块、内存、启动项。

网络安全应急响应管理机制



应急响应组织结构及职责



应急事件类型

有害程序事件

- 计算机病毒事件
- 蠕虫事件
- 特洛伊木马事件
- 僵尸网络事件
- 混合攻击程序事件
- 网页内嵌恶意代码事件

网络攻击事件

- 拒绝服务攻击事件
- 后门攻击事件
- 漏洞攻击事件
- 网络扫描窃听事件
- 网络钓鱼事件
- 干扰事件

信息破坏事件

- 信息篡改事件
- 信息内容安全事件
- 信息假冒事件
- 信息泄露事件
- 信息窃取事件
- 信息丢失事件

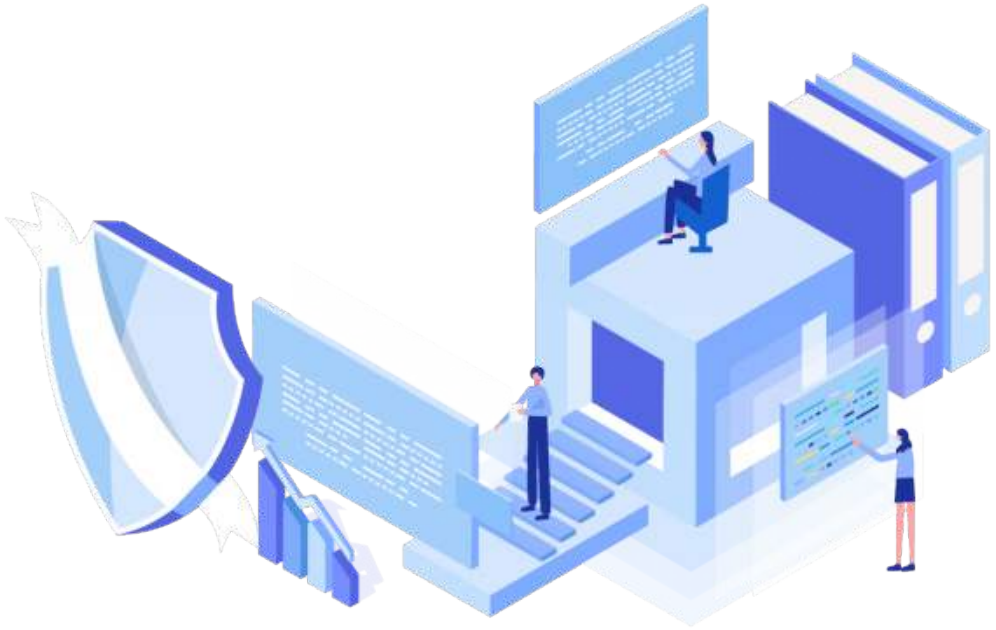
设备设施故障

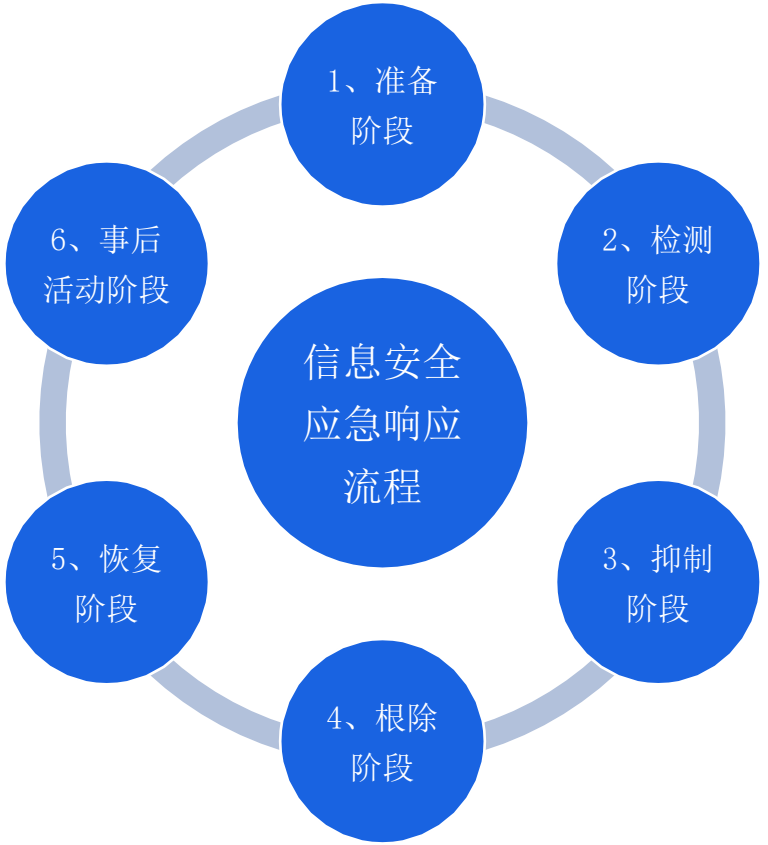
- 软硬件自身故障
- 外围保障设施故障
- 人为破坏事件

应急事件等级

事件描述	等级	信息安全事件影响	信息系统损害程度
特别重大事件	I级	特别严重影响或破坏	特别严重
重大事件	II级	严重影响或破坏	重大
较大事件	III级	较严重影响或破坏	较大
一般事件	IV级	较小影响或破坏	较小

信息安全应急响应流程





信息安全应急响应流程—准备阶段

分析资产的风险

1）明确信息系统网络与系统架构。
2）明确信息系统的管理人员。
3）明确信息系统的保护要求。
4）计算损失和影响。

风险加固

1）根据风险建立防御/控制措施。
2）安全管理及安全技术层面要同时兼顾。

编制应急预案

1）制定应急处理的操作步骤。
2）制定应急处理的报告路线。
3）制定信息系统恢复的优先级顺序。
4）明确配合的人员信息。

信息安全应急响应流程—准备阶段

组建应急响应团队

① 组建管理人员团队。
② 组建技术人员团队。
③ 明确人员职责。
④ 建立应急响应组织人员清单。

保障资源储备

① 信息安全应急响应专项资金。
② 应急响应所需的软硬件设备。
③ 社会关系资源。

技术支持资源库

① 网络拓扑图。
② 信息系统及设备安装配置文档。
③ 常见问题处理手册。
……