信息安全的问题，困惑及新方向

江明灶, 博士，信息安全系统认证CISSP专家
思科系统亚太区、大中华区首席信息安全官

主要议题

- 信息安全的对立
- 信息安全原则的循环特性问题
- 响应式安全

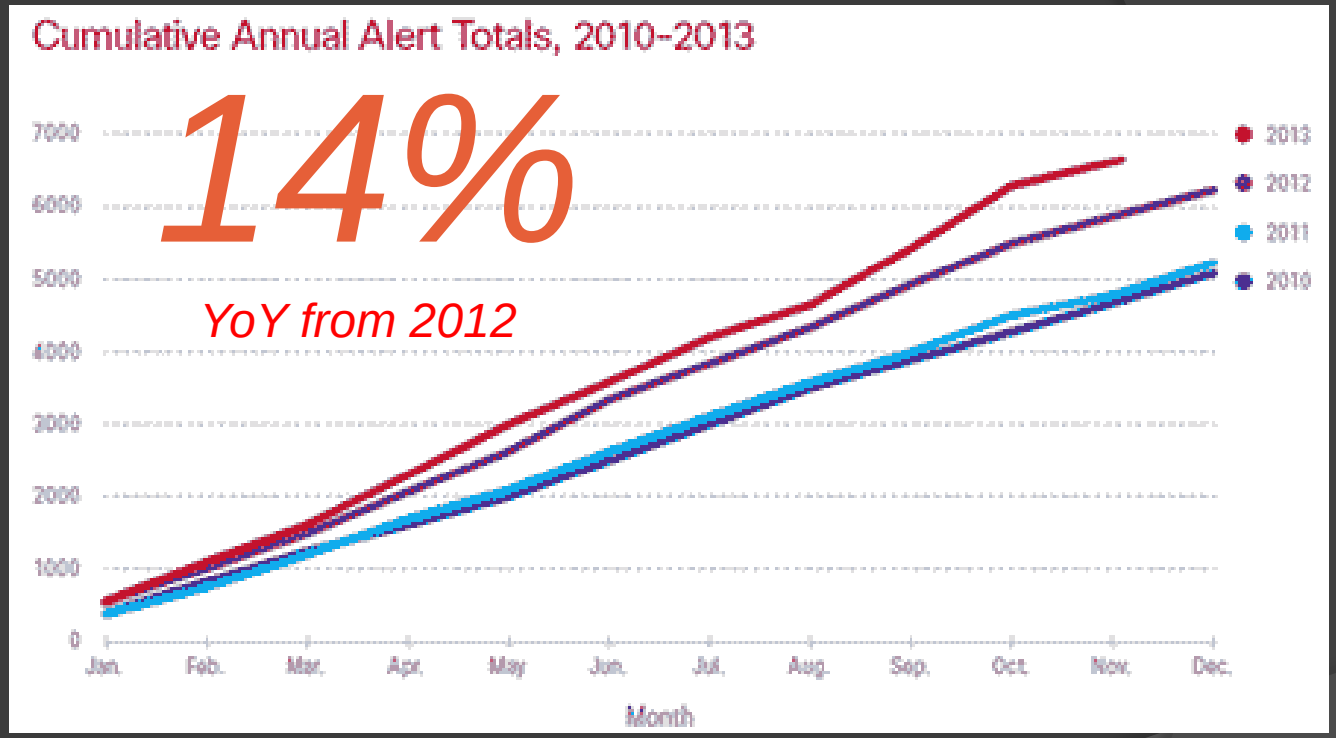
信息安全的对立

- 安全的结果 – 会是什么样?
- 不安全的后果如何?

1.5 million

Monitored cyber attacks in the United States in 2013

IBM Security Services 2014 Cyber Security Intelligence Index, April 2014



Source: Cisco Annual Security Report 2014

Source: Maryam Runiassy, Sep 19, 2014: http://prezi.com/pflqhvvpb2nm/important-cybersecurity-incidents-and-statistics/

收入下降

司法调查

声誉

信任丧失

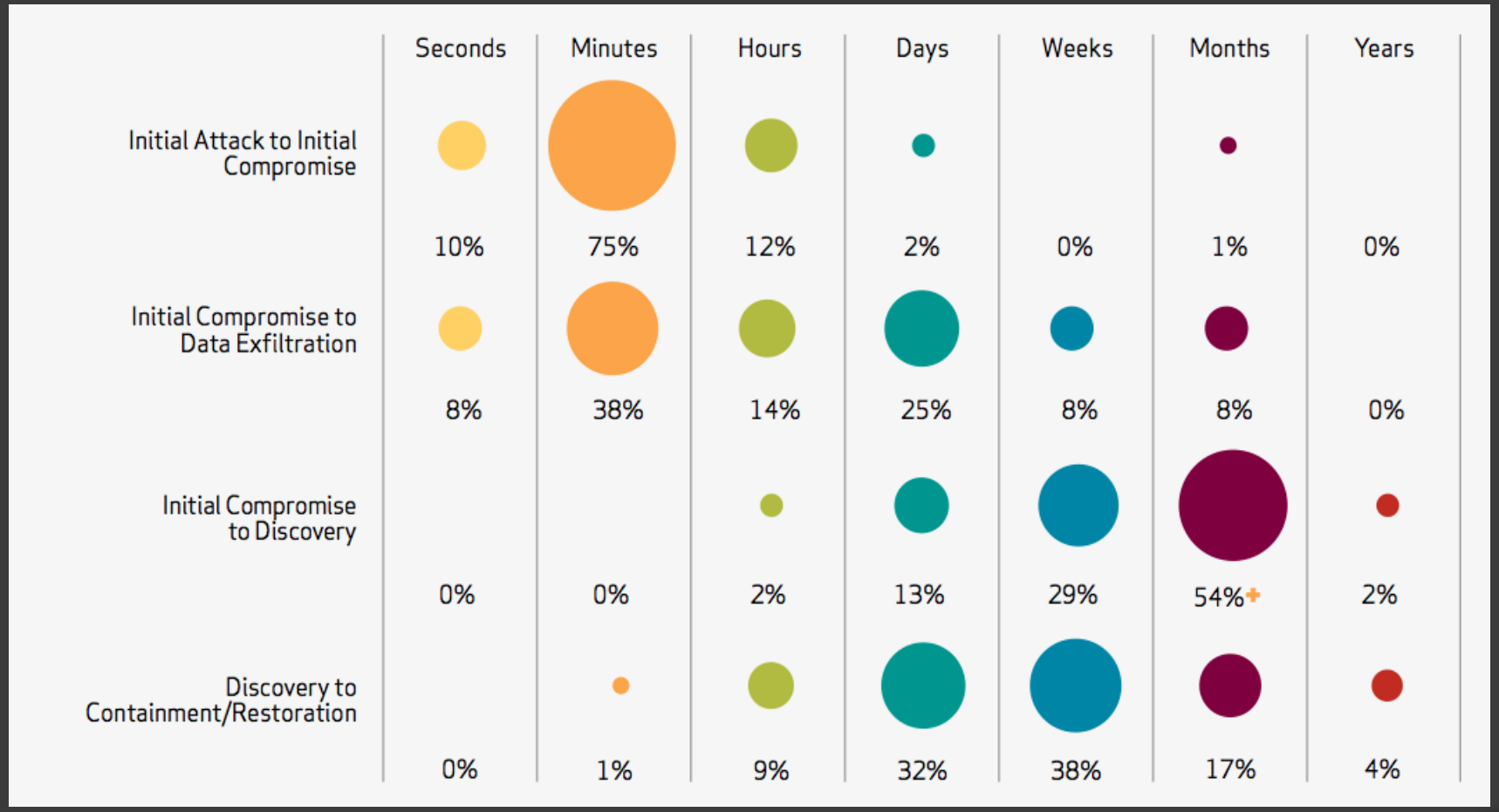
品牌受损

生产力下降

技术支持

安全合规

安全漏洞时间跨度

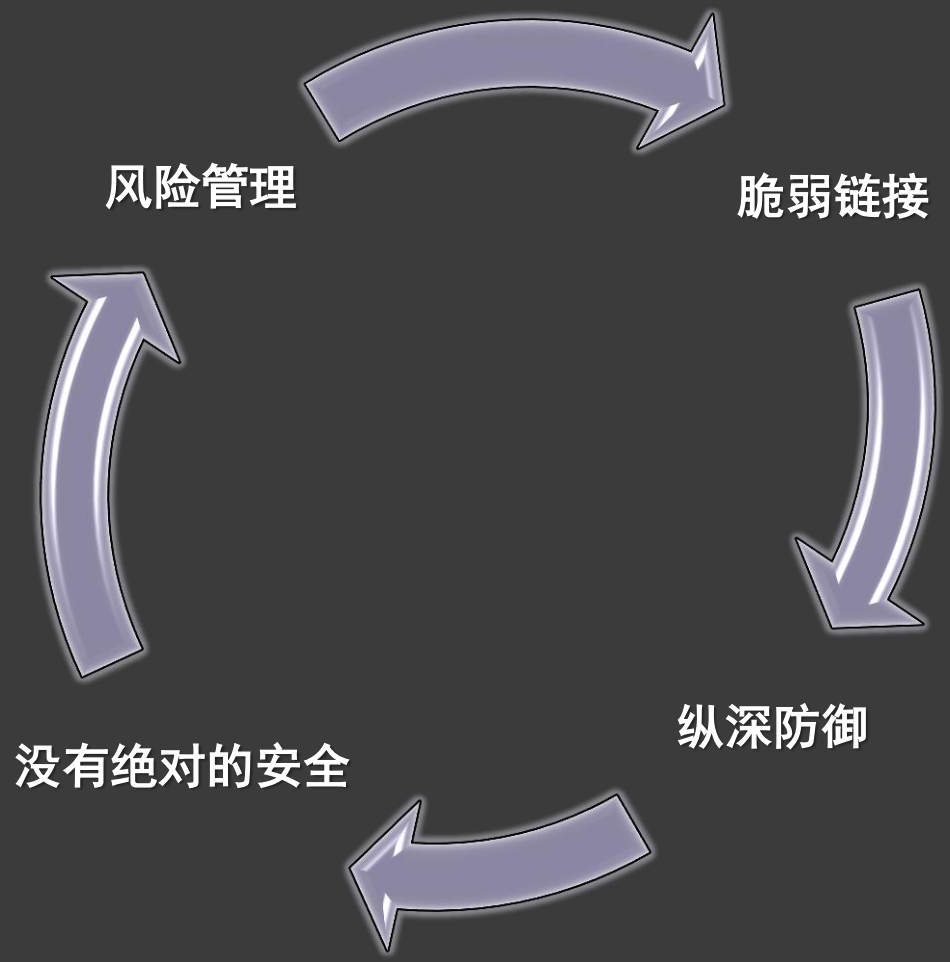


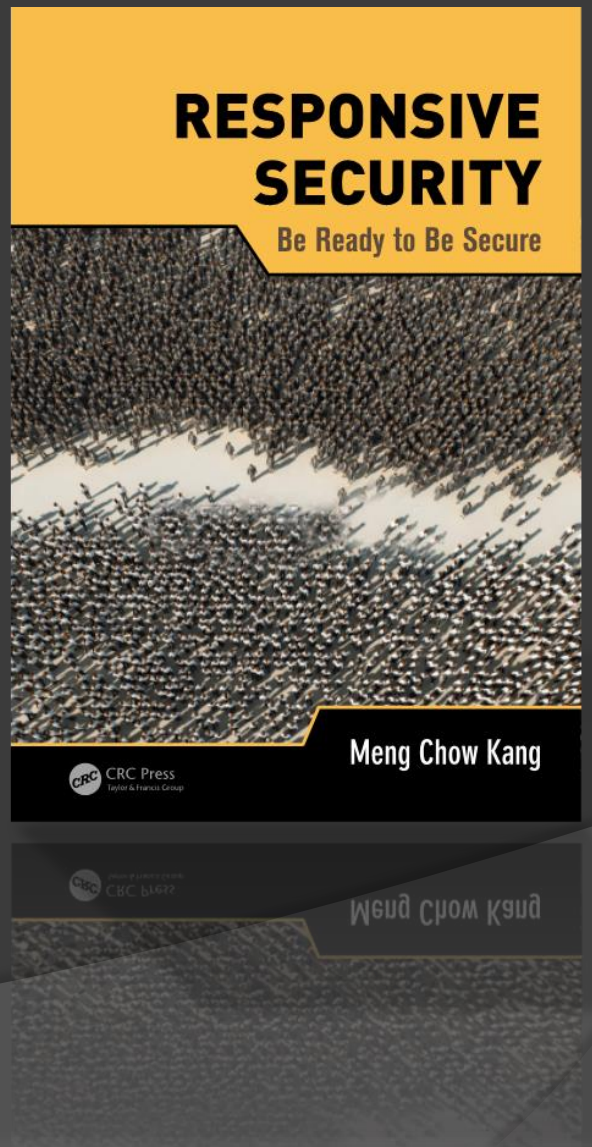
Source: Verizon Data Breach Investigation Report 2012

投资失衡影响预见能力

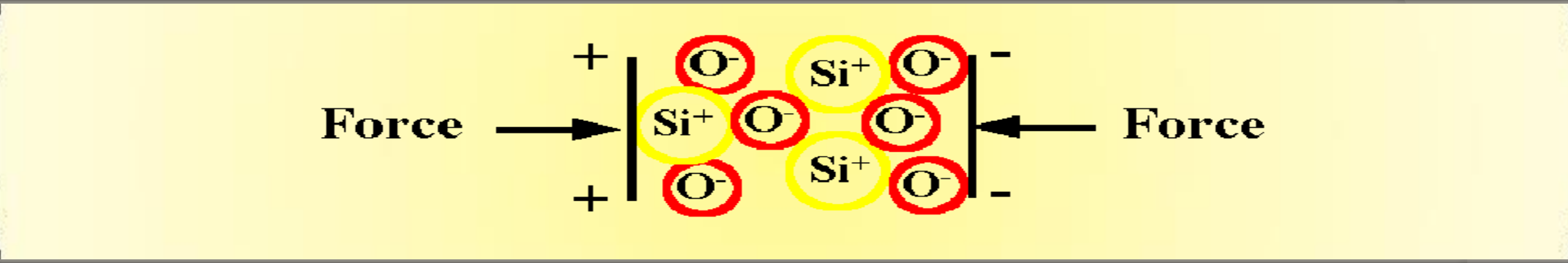
预防缺乏抑制新兴攻击与快速恢复的能力

信息安全原则的循环特性





压电理论



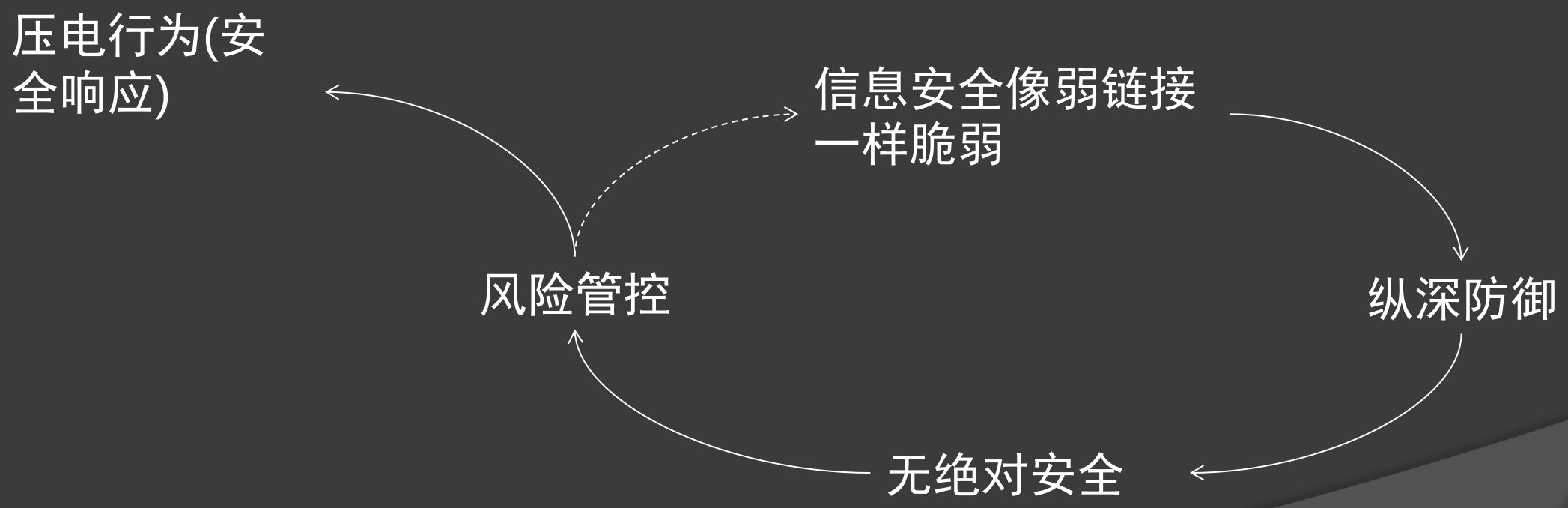
压迫/放松 → 触发 → 调整

压电行为

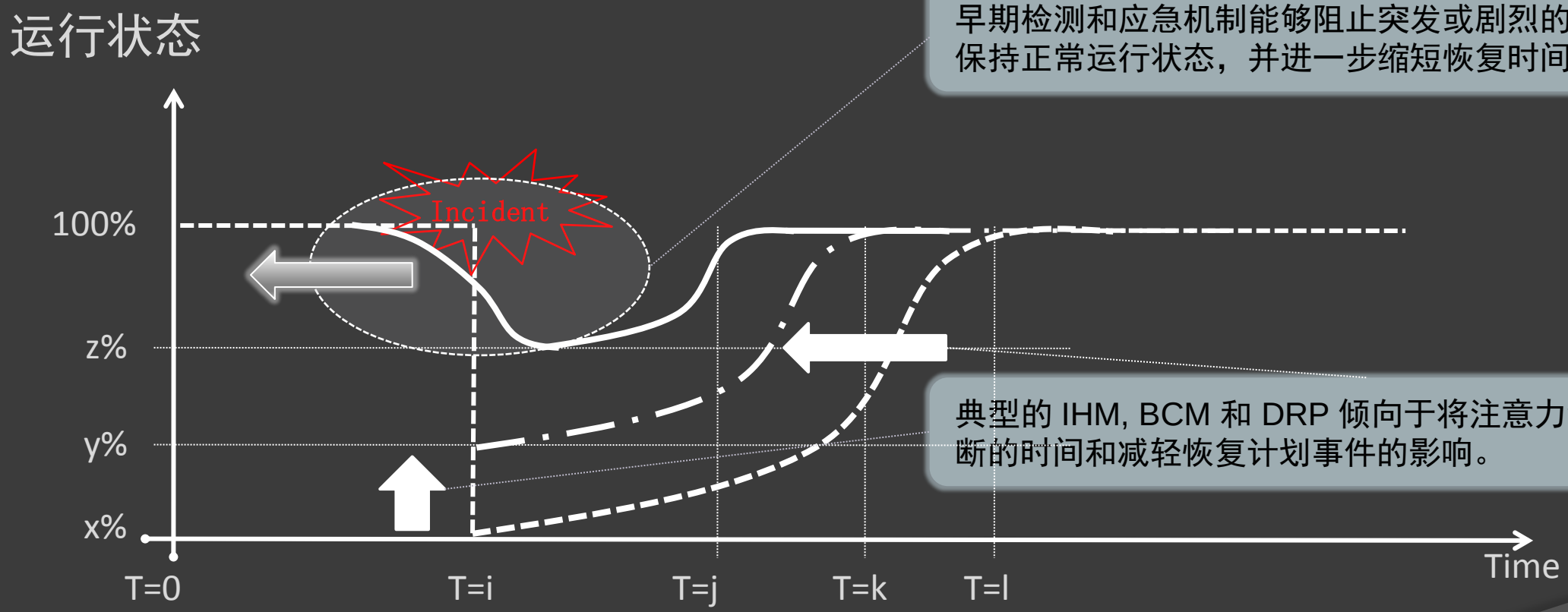
响应行为

改变事件 → 情景感知 → 临界调整

利用压电行为攻破信息安全原则的循环



响应系统



早期检测和应急机制能够阻止突发或剧烈的事故的发生，保持正常运行状态，并进一步缩短恢复时间。

典型的 IHM, BCM 和 DRP 倾向于将注意力集中在缩短中断的时间和减轻恢复计划事件的影响。

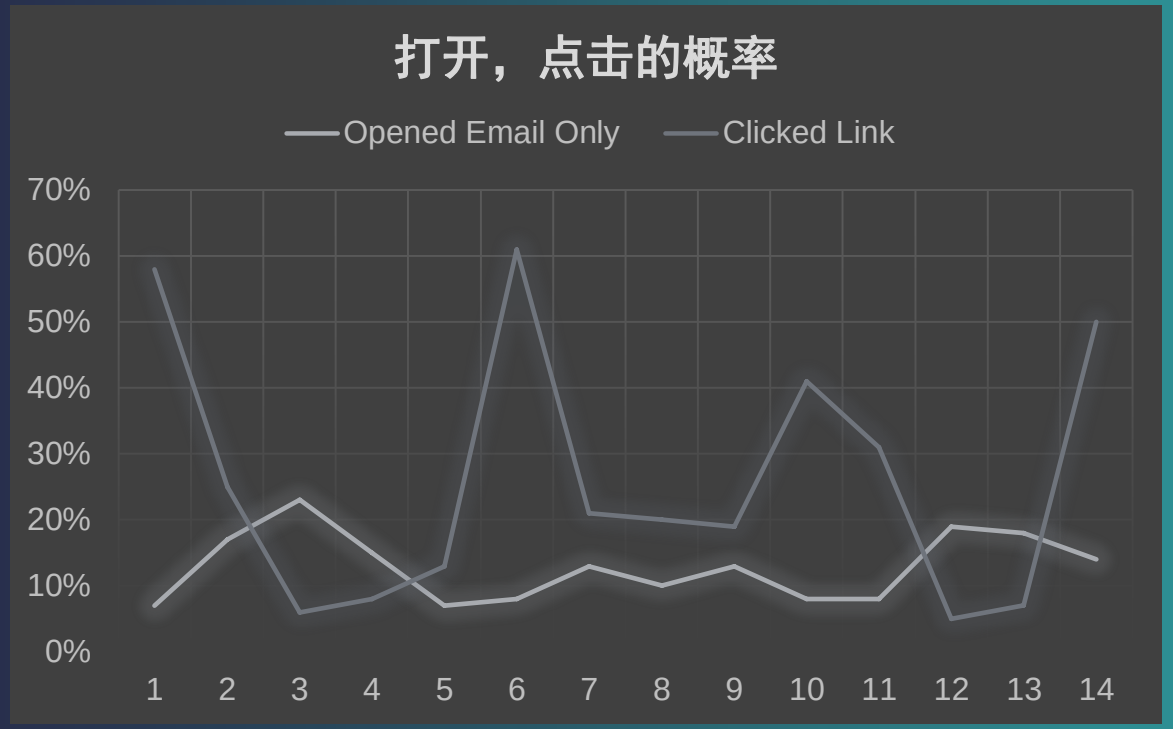
实行IHM, BCM, 或 DRP前的效果

实行IHM, BCM, 或 DRP后的效果

安全响应的预期效果(注重事前预防)

我们有多脆弱?

- 目标 – 300 IT 技术和管理人员，东部时区10点正式启动
- **主题：您的有薪假期需求**



截至下午4点, 共发送294封邮件, 其中有125 (42.5%) 位用户打开邮件**并**点击了链接. 在电子邮件事件中有69 (23.5%) 位用户在前15分钟内点击链接。

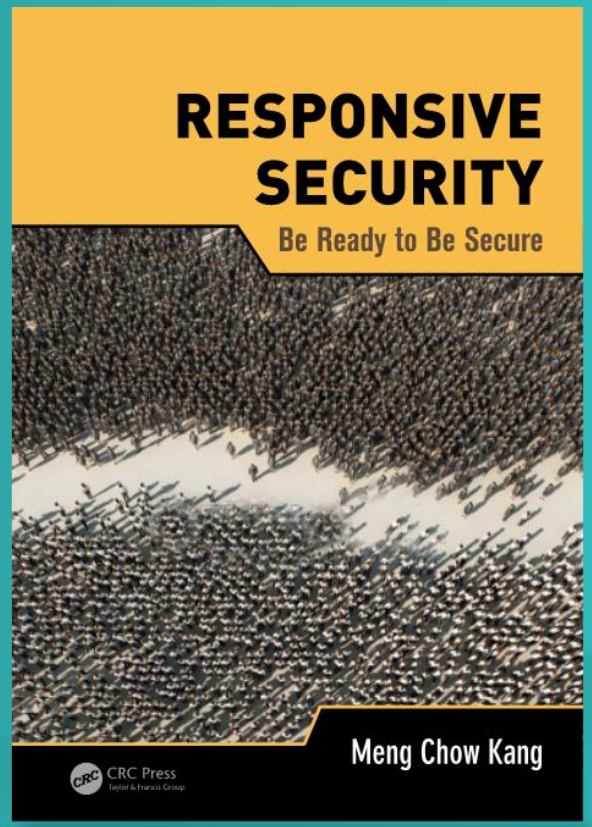
在活动的7分钟内, 通知计算机安全事件响应小组，5分钟后域名被黑。

知晓

减缓

面向临界调整

Intelligence 情报	预见性	临界调整
Knowledge 知识	认知	能力
	性能	*容量*



“緩慢思考最費心力的形式，是那些需要你去快速思考的形式。”

– 丹尼尔 卡恩曼《思考，快与慢》