

# 制定信息保护的全球实践标准

2014年9月24日  
中国，北京  
Dr. Fred Cohen



- 在过去的70年间，信息世界发生了很大的改变，计算机逐渐成为我们生活中不可或缺的组成部分。但实际，信息安全的科学理论自上世纪80年代以来，就一直没有有什么新的重大发展
- 政府机构往往把更多的精力用于研究如何入侵并获取情报，而对于自身网络安全系统的安全防护则明显投入不足。但恰恰在此同时，支撑政府工作的各种公共基础设施已经开始越来越多的接入网络，并且非常依赖于网络所提供的信息支持。
- 信息安全技术迫切的需要重大的革新，这是一个世界性的课题。重新构筑一套完整的理论体系可能需要很长的时间，而制定合理的实践标准（**Standard of Practice**，**SoP**）却是可行的，而且很多实践标准实际上正在被广泛的使用。
- 实践标准可以推动理论体系的发展，而理论体系又可以指导实践标准的改进。本次演讲将主要对实践标准与理论体系之间的互动过程进行深入的阐述和分析，这一过程也需要我们共同的参与和努力。

## 历史与背景

- 恐惧、不确定、怀疑 与事实
- 信息保护的艺术（非科学）
- 合理化决策（选择、决策）

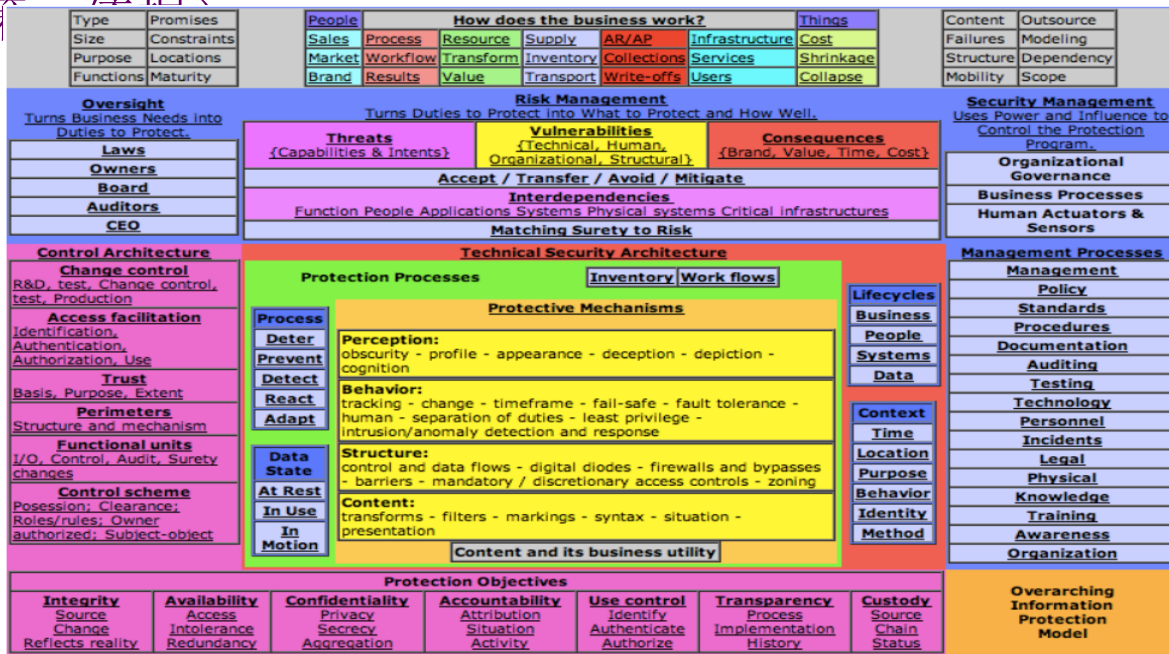
## 实践标准SoP

## 理论体系的构筑

## SoP的更新



讨



- “计算机安全”已经成为一种有价值的商业活动
  - 赚钱是商业的主要目的
  - 如果厂家把安全服务做得太好，让您感觉不到威胁的存在，您也就不再需要安全服务了？
  - 但反之，如果厂家把安全服务做得不好，那么你为什么还要花钱去购买它呢？
  - 那么，我们该怎么去向消费者推销我们的安全软件呢？**FUD**
  - **F**恐惧
    - 坏事即将发生在你身上，他已经在被人身上发生了
  - **U**不确定
    - 您怎么知道自己是安全的，谁在看着你的守护者？
  - **D**怀疑
    - 即便是NSA（国家安全局）也不能保住自己的秘密
- 在制造恐惧、不确定与疑惑后，你就需要帮助消费者释放这些恐惧
  - 快来使用我们的产品吧：用了你就安全了，NSA已经在使用我们的产品了

- 现实情况——无知并不等于幸福
  - 政府更倾向于攻击而不是防御
    - 用于攻击的费用和用于防御的费用各是多少
    - 最好的防御是进攻？
    - 用于收集情报和用于反间谍费用是多少？
    - 对情报的需求超过了对安全操作的需求。
  - 然而，我正处在一个信息的时代
    - 社会建立在大量的基础设施至上
      - 水、食品、燃料、电力、空气、金融系统, record-keeping, 医疗卫生系统、警察和消防等等
    - 这些基础设施越来越依赖于信息系统与网络
  - 关键基础设施越来越依赖于电脑
    - 我们恐怕无法摆脱这种依赖

- 就象炼金术一样，信息保护更像是一门艺术，而不是科学
  - 关于安全防护的一些经验法则和安全概念
    - 应该定期更改您的密码
    - 安全防护措施越多，安全防护效果就会好
  - 绝大多数的经验法则并没有多少理论依据
    - 定期更改密码实际上是二战时期使用的安全策略
    - 而安全措施越多越好的概念则完全是一种主观认识，没有任何客观依据
  - 绝大多数的安全概念也并非来自于理论基础
    - 概率风险评估（PRA）——在安全领域很少被使用
    - 通过标准化的方式来改进防护策略——目前使用的也很少
  - 绝大多数的理论基础在实践中也确实很难发挥作用
    - 概率风险评估很多因素根本没有办法精确的量化
    - 绝大多数的标准很容易被执行，但却不能带来什么实质性的好处

- 选择
  - 可以选择的方式是有限的
  - 举例: Duties to protect in what form?  
Written / Verbal / Email / Web site / Database w/workflows /etc.
- 决策
  - 可以用于决策的因素只基于的事实是有限的
  - Example: If maturity > “managed” → Database w/workflows
- 依据
  - 选择什么样的因素用于决策才是明智的?  
This maturity level requires systematic approaches to process and this (typically today) works via a workflow system
  - 为什么选定这些条件因素, 或者说, 为什么选定这样的场景  
But we may have a paper workflow system → no database

- 目前还不是——但将来会是
  - 更成熟的模型有助于减少错误和遗漏
    - 如：飞行安全是通过不断的检查而提高，等等（许多研究表明）
    - 如：医疗服务是通过不断的检查而提高，等等（一些研究表明）
  - 更成熟的模型可以促进有效的控制和验证过程
    - 但是目前并未针对信息保护进行有关研究
- 我们需要进行更多科学研究使以下方面更加明晰
  - 系统中是否存在成熟的元素
  - 系统防护中是否存在错误或遗漏的盲点
  - 检验假设的度量与分析
    - 是否是越成熟的模型越有效？总是有效？成熟到什么程度才有效？
    - 我们在什么时间，需要什么样成熟度的模型？



## 历史与背景

- 恐惧、不确定、怀疑 与事实
- 信息保护的艺术（非科学）
- 合理化决策（选择、决策）

## 实践标准SoP

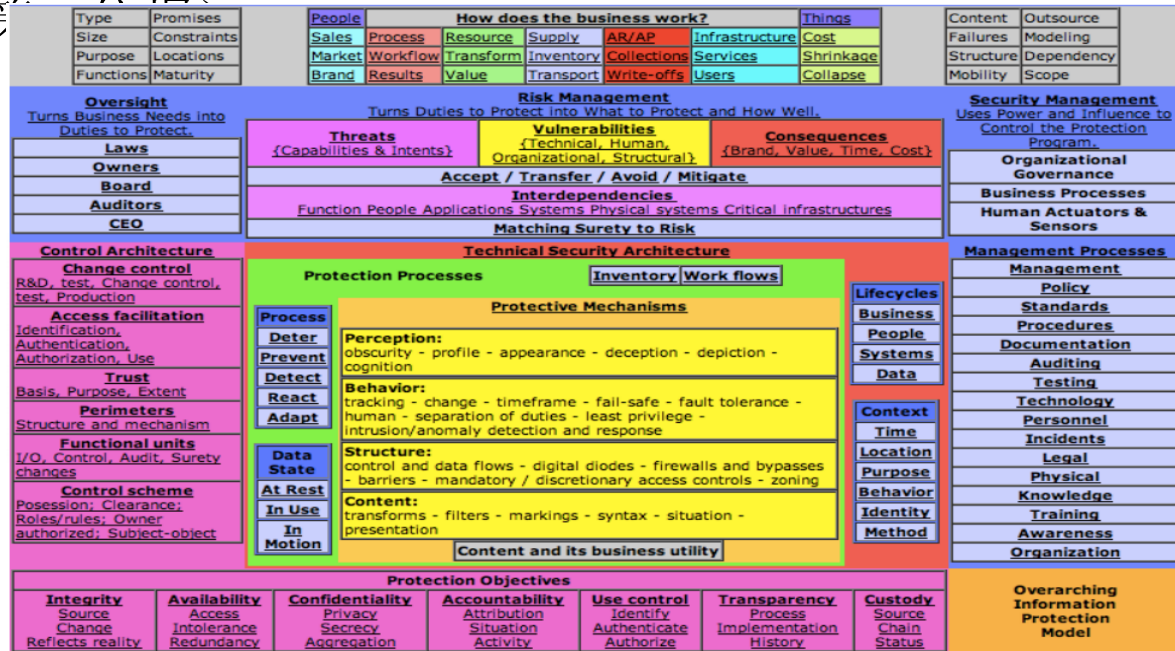
- 理论体系的构筑
- SoP的更新
- 思考与探讨



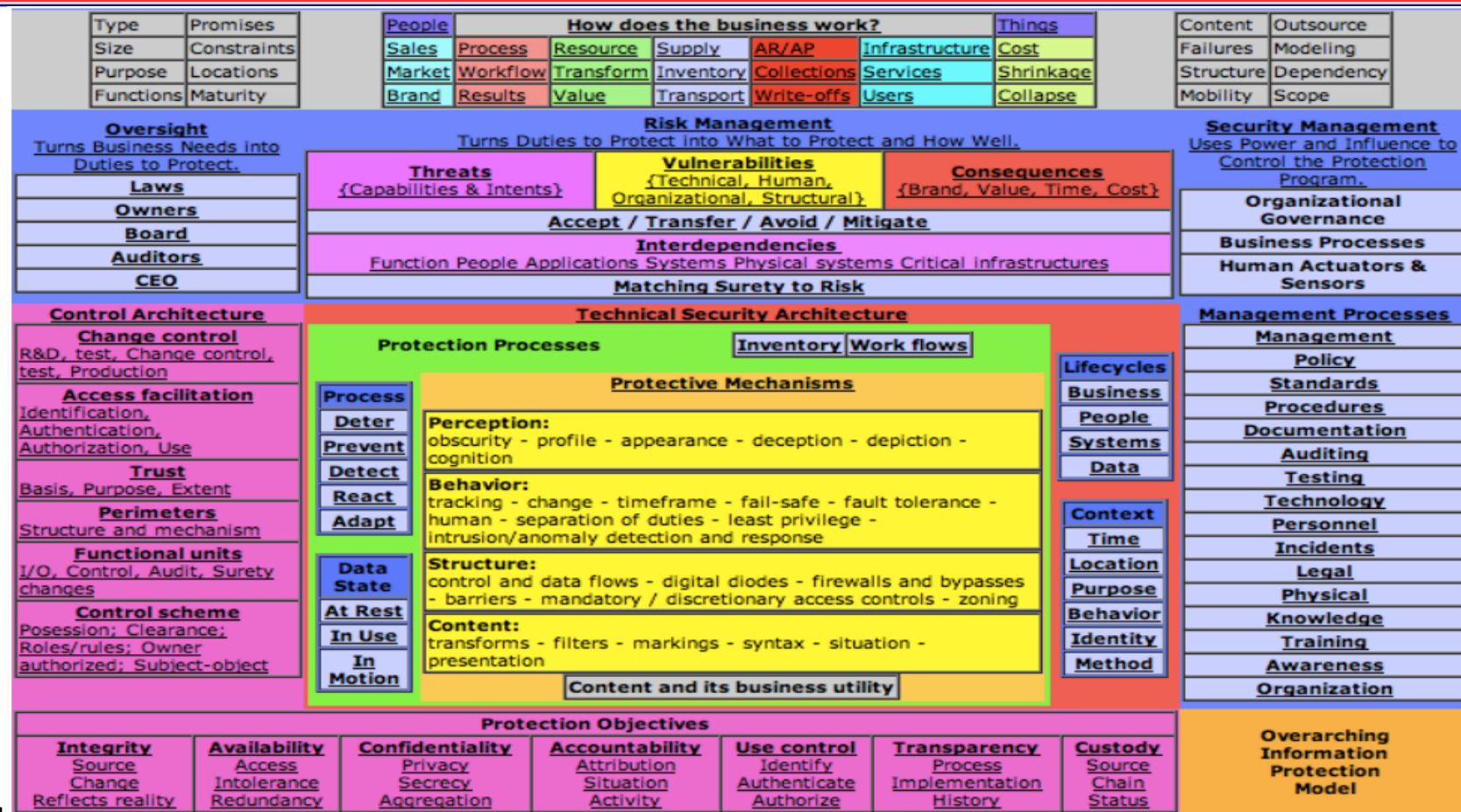
Insurance Solutions Comp



a place of mind  
THE UNIVERSITY OF BRITISH COLUMBIA



- 实践标准（SoP）的定义
  - SoP并不是一种“标准”（你遵循的某项事物）
  - “理性”和“谨慎”的实践（勤勉 vs 粗心）
    - 不是唯一的实践---并不一定适用
  - 开放资源/预览：<http://all.net/>→Protection →SoP ...
- 运用实践标准帮助我们的专家进行分析
  - 提出一系列合理全面的问题
  - 将这些问题用特定逻辑语言进行标准化描述
  - 用预先定义的决策逻辑进行决策
  - 在基准的情况下允许一定的偏差
- 当实践标准有效时，我们将开始使用
  - 当实践标准无效时，我们适时调整与更新



- 取决于结果，能力和成熟度
  - 一些地区认为不安全，因此不执行
  - 一些地区仅有部分流程元素获得认证
  - 当风险、能力、成熟增加，“需要做的重”也随之增加

The suggested approach to real-time interdependency risk management is as follows:

Risk Level	Skill	Maturity	Alternatives
High	High	Optimizing	Real-time interdependencies should be identified in advance as far as they reasonably extend. <b>AND</b> Event sequences leading to potentially serious negative consequences should be examined in detail for specific mitigation sequencing strategies.
High	High	Managed+	Real-time interdependencies should be identified in advance as far as they reasonably extend. <b>AND</b> Interdependent failures should be mitigated in advance by adding redundancy and/or hardening interdependent systems. <b>AND</b> Interdependent failures should be mitigated in advance through failsafes and alternative operating modes. <b>AND</b> Interdependent failures should be mitigated in real-time as part of the incident response process.
High	---	Defined-	This situation should be avoided - do not proceed under this condition.
High	Med-	---	This situation should be avoided - do not proceed under this condition.
Medium	Med+	Defined+	Real-time interdependencies should be identified in advance but only to the borders of the facility or enterprise. <b>AND</b> Interdependent failures should be mitigated in real-time as part of the incident response process. <b>AND</b> Interdependent failures should be mitigated in advance by adding redundancy and/or hardening interdependent systems.
Medium	---	Repeatable-	This situation should be avoided - do not proceed under this condition.
Medium	Low	---	This situation should be avoided - do not proceed under this condition.
Low	Low	Repeatable+	Real-time interdependencies should be ignored as too complex to identify in advance. <b>AND</b> Interdependent failures should be mitigated in real-time as part of the incident response process.
Low	Low	Initial-	This situation should be avoided - do not proceed under this condition.

*Real-time interdependency risk management*



## 历史与背景

- 恐惧、不确定、怀疑 与事实
- 信息保护的艺术（非科学）
- 合理化决策（选择、决策、依据）

## 实践标准SoP

## 理论体系的构筑

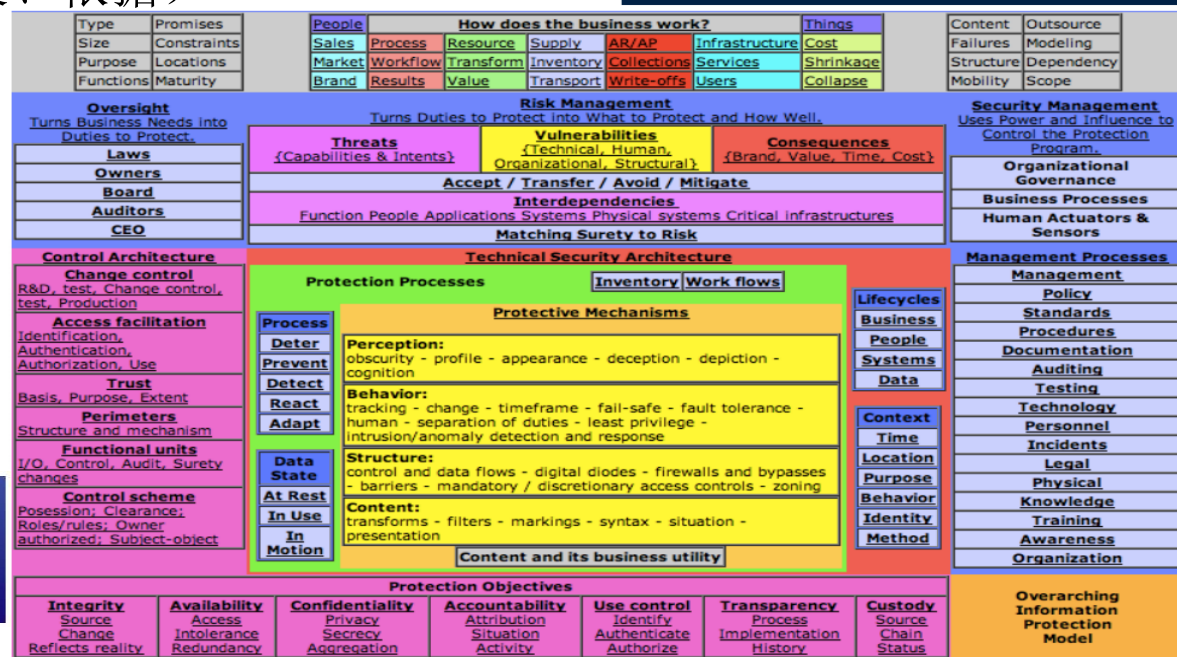
- 理论
- 实验
- 反馈

## SoP的更新

## 思考与探讨



Insurance Solutions Corp



- 如今，在信息保护领域并不存在成熟的理论。
  - 一些例外
    - 密码学元素
    - 信息流控制元素（Shannon，等等）
    - 病毒和恶意软件元素（Cohen, 等等）
    - 其他例外
- ✓ 但所有这些元素的作用都很有限
  - 密码学理论在很大程度上忽略了现实状况
  - 信息流控制的方法几乎没有被使用
  - 病毒和恶意软件理论在很大程度上只是规定了哪些事情不可以做
  - 其他因素的局限性
- 我们还有很多的问题需要研究
  - SoP恰好为探索提供了出发点

- 因果，测试，验错，调整
  - 通过一定的机制施加影响
    - $C \rightarrow E$  — 因果关系是所有科学的基础
  - 科学理论需要实验的验证
    - 实验能够证明一个理论是错误的
    - 但对于普遍规律，实验并不能证明理论的正确性
    - 为了“验证”需要“衡量”某些事物---什么事物？
  - 当一个理论被推翻时，我们就会对理论做出调整
    - 或尝试其他方法
- 地平论即是一项科学理论
  - 实验证实地平论是错误的（环球）
  - 科学发展了一项新理论



- 资源枯竭造成拒绝服务

- C: 使用大量资源  $\text{Resources } R = (k_1r_1 + k_2r_2 + \dots k_nr_n)$

$\text{Usage } U = (u_1r_1 + u_2r_2 + \dots u_nr_n)$

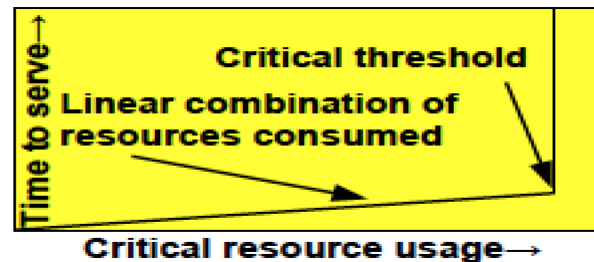
- 特别地，性能尺度，线性地直到.....

- m: 可用资源耗尽

- 关键资源耗尽  $(k_1r_1 + k_2r_2 + \dots k_nr_n) - (u_1r_1 + u_2r_2 + \dots u_nr_n)$

- E: 拒绝服务  $\forall_{i < n}, \text{ if } u_i > k_i \rightarrow \text{DoS}$

- 不再提供服务



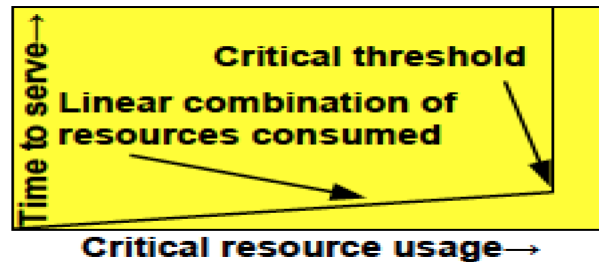
- 关键资源的示例:

- CPU时间，文件句柄，磁盘空间，内存空间，进程中条目，连入端口，网络带宽，内部总线带宽，等等

- 问题：我们如何检验理论？



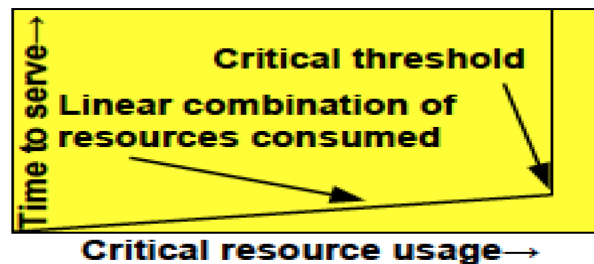
- 对理论进行测试  $R=(k_1r_1+k_2r_2+... k_nr_n)$ 
  - 隔离一种特定的资源
  - 给资源设定一个上限  $k_2=100$
  - 利用大规模的消耗戏院来衡量系统性能
    - 不断增加对资源的消耗，并实时评估系统性能
  - 将有限的资源耗尽  $u_2=(1, 2, ..., 99, 100, \textcolor{red}{101}, ...)$ 
    - 消耗到临界值，达到拐点
    - 超过拐点便会拒绝服务  $u_2 > k_2 \rightarrow \text{DoS}$
  - 增加可利用资源
    - 在原有的资源上限之上进行测试
    - 确保服务线能够先行增长
  - 一个混杂因素（非线性） $\rightarrow$ 其他资源？



- 韦伯斯特大学网络实验室
  - 全球性大学
    - 在五大洲有课程，在中国有3个地方有课程
- 网络实验室的科学实验条件
  - 基于虚拟机的可重复的实验环境
    - 同时并发的多个实验或单个的大型实验
  - 全球能力
    - 任何地方的课堂均可访问实验资源
    - 多个实验场地，具备容灾条件
    - 可供科学实验使用
  - 可以安全地从事危险性实验



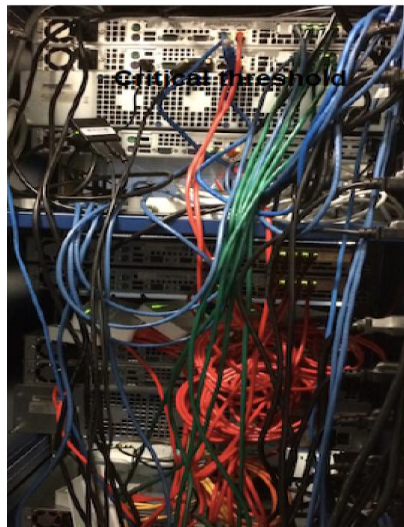
- 被度量的实验现象
  - 等到正确的响应所花费的时间
- 受控的变量
  - 可供使用的资源以及消耗率
- 实验结果
  - 正常操作的受限资源
  - 对一台或两天计算机做Ddos攻击
  - 更多的资源
  - 减去实验开销
  - 通过增加关键资源的“防卫”有效么？





- 在度和测试上做得更好
  - 对多种资源的参数做测量
    - 线性关系  $R=(k_1r_1+k_2r_2+... k_nr_n)$
    - 拐点  $U=(u_1r_1+u_2r_2+... u_nr_n)$ ?
  - 识别是度量令人迷惑的因素
    - 组合度量
      - 这些资源是相互独立的么?
      - 哪些资源是相关联的, 如何关联?
- 创建一个预测方程  $(k_1r_1+k_2r_2+... k_nr_n)$   
 $- (u_1r_1+u_2r_2+... u_nr_n)$ 
  - 设计一个之前没有尝试过的实验
  - 用函数来预测性能  $f(\text{Designed Parameters})$
  - 通过测试来证实/证伪一个方程
  - 报告结果

$\forall_{i < n}, \text{ if } u_i > k_i \rightarrow \text{DoS?}$



- 当得到结果后
  - 更新方程式，以更接近事实
  - 尝试用更大范围的取值来探索实验空间
  - 识别会影响实验的环境参数
    - 保持更新，以控制更多的环境因素
  - 识别可观测性和精度/准确率的限制
    - 保持更新，以估计传感器的极限
    - 制造更好的传感器，同时更新实验方法
  - 更新理论，如果它已经被证伪的话
    - 限制它的适用范围
  - 公布结果，使其他人可以从中获益
    - 同时关注他人的实验结果



## 历史与背景

- 恐惧、不确定、怀疑 与事实
- 信息保护的艺术（非科学）
- 合理化决策（选择、决策、依据）

## 实践标准SoP

## 理论体系的构筑

- 理论
- 实验
- 反馈



## SoP的更新

## 思考与探讨

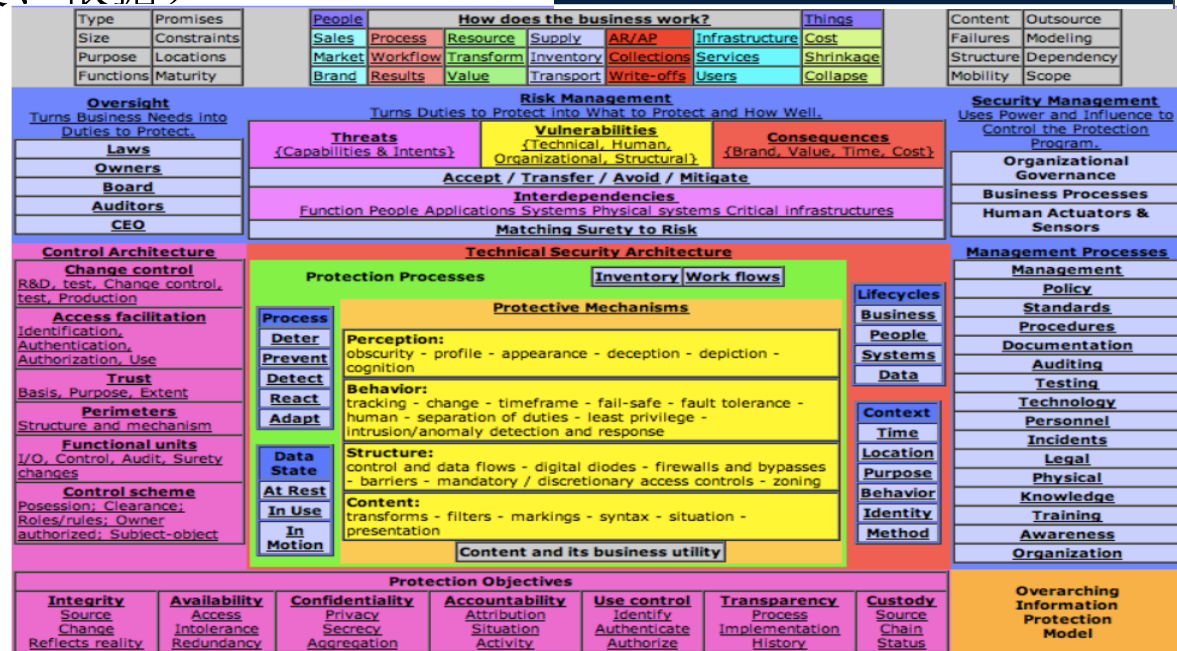



Insurance Solution



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA



- 科学告诉我们DDos是怎么回事儿以及如何减轻影响
    - 除非被适用，科学结果是没有用的
    - 我们如何适用这些实验结果？
  - 更新SoP来反映最新的科学成果
    - 用科学结果来改进SoP
    - 重复使用SoP来适应保护
  - SoP提出问题
    - 科学回答问题
      - SoP适应科学
  - 发生某事件
    - SoP提出更多问题
- 



- InterRES Trust (UBC 的贡献)
  - 从企业SoP开始
  - 审阅管理和档案管理 (ARM) 文献
  - 更新SoP
  - 创建专用于ARM的SoP ( ARM-SoP )
  - 对等社区的相互评审(security / ARM)
  - 应用SoP到全球已经存在的ARM实体中 (10月2日作为开始时间)
  - 对比目前的实践和ARM-SoP的机械作法
  - 评价ARM-SoP是否是合理的、谨慎的
  - 根据评论改写SoP
  - 出版结论
- 测试更新并通知SoP, 反之亦然





- Ridge 保险服务公司(RISCO)和Fearless(FS)
  - RISCO以提供信息技术保险作为主要业务
    - 由Lloyds集团成员和其他公司共同担保
  - FS为潜在投保客户提供SoP评估
    - 实际做法vs. SoP，辅以专家判断的结合（现状）
    - 对利率/免赔额/限额的风险有更好的理解（理论）
  - 保险要求报告损失/事件/变更
    - 报告（测试）和SoP相关的结果（理论）
  - FS支持客户防护立场的改进
    - 实践中变化的跟踪和反馈(实效vs. 理论)
    - 向RISCO报告改进和风险的变化
  - RISCO对更佳的防护环境提供费率折扣
    - 精准数据使更优的保护的费率降低
  - 通过反馈我们一起建立科学的基础



我们一直期待  
反馈

- 决策者需要一个好的理由来花钱
  - 内部有什么理由?
    - 无论什么原因其实都很有限
    - 你对内部的了解程度实际不足以支撑正做出确的风险管理
- 保险业通过建立风险准备金而改变了这个现状
  - 许多组织有独具自己特色的防护方法、环境和变更细节
  - 对事故和后果的掌握
    - 最终结果表现为风险准备金的支出
    - 不可抗力事件免赔并被报告
- 最终的效果取决于防护和支出的关系
  - 决策者支付已知的保险或防护成本
  - 市场驱动产品/服务的单位产出价值

## • 历史与背景

- 恐惧、不确定、怀疑 与事实
- 信息保护的艺术（非科学）
- 合理化决策（选择、决策、依据）

## • 实践标准SoP

## • 理论体系的构筑

- 理论
- 实验
- 反馈



## • SoP的更新

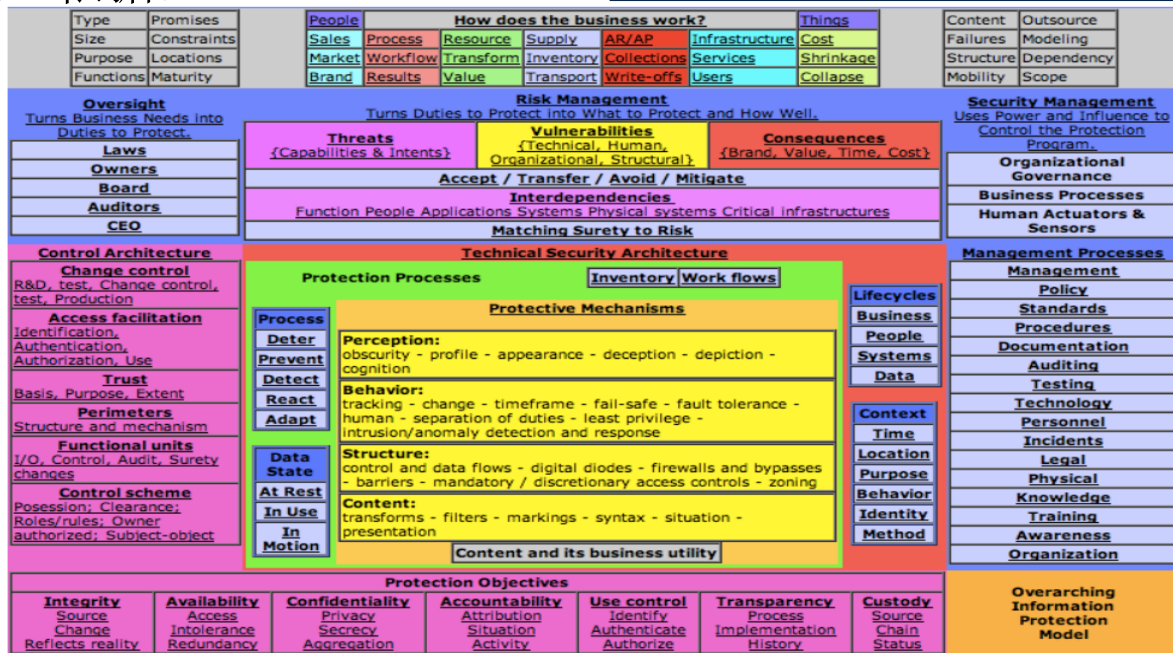
## • 思考与探讨



Insurance Solutions Co.



a place of mind  
THE UNIVERSITY OF BRITISH COLUMBIA



- 了解SoPs的最近进展
  - 参考<http://all.net/> → Protection
- 新的尝试以改善信息决策
  - 变更某些 SoP元素
  - 开发科学的测试以适应不同的场景
  - 验证实际谁在何种场景更有效以及为什么
- 公布测试结果并告知SoP
  - 通过测试结果使决策过程更清晰
  - 让我们知道，并更新 SoP原则
  - 随着原则的改变结论也将改变
- 我们更新SoP 以适应科学发展并提出新的问题
  - 我们将做验证测试以保证科学有效

- 加入我们!
  - 和我们一起在UBC 工作, 参与 InterPARES Trust (ITrust) 项目
    - 拿出你的档案管理系统
    - 通过Itrust中国代表一起工作
  - 支持和Webster University的共同研究
    - 获得计算机安全的学位
    - 参与Webster信息技术实验室和信息技术探险者相关活动
    - 对信息技术实验室将进行的实验提出建议
  - 通过信息保险流程推进实践
    - 和Ridge Global一起将信息保险带到中国
    - 吸引中国的保险公司和RISCO的合作
  - 将SoP 作为一种方法带入您的企业
    - 将SoP翻译成中文
    - 促进SoP在中国和世界的应用



# Thank you

**Fearless Security**  
You have nothing to fear but fear itself



<http://all.net/> - fc at all.net