

Developing a global standard of practice supported by the science of information protection

2014-09-24
Keynote Address
Beijing, China

Dr. Fred Cohen



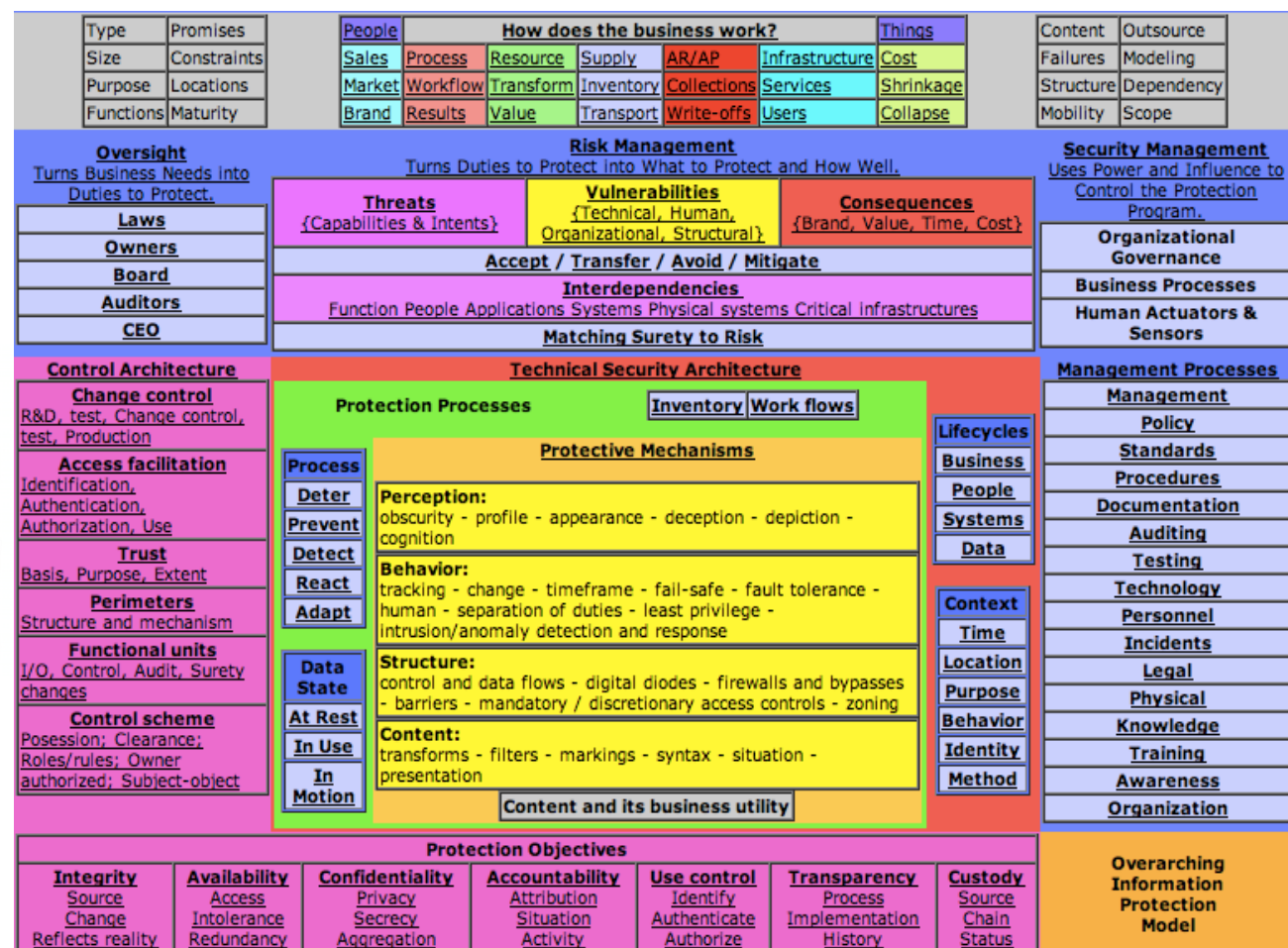
Insurance Solutions Company

Abstract

- The information world has changed over the 70 years since computers became a vital component of the modern world, and yet the science of information protection has remained largely stagnant since the 1980s.
- Governments largely chose offense over defense, feeling that the need for intelligence outweighed the need for secure operations. But at the same time, societies and the critical infrastructures supporting them became increasingly dependent on and connected to information systems and networks.
- Today, there is a global and dire need to advance both the science and the practice of information protection. Building a science takes a long time, but a standard of practice for reasonable and prudent protection decision-making exists today
- This talk outlines the process by which a standard of practice can support the development of a science and a science can support the development of a standard of practice, discusses how that process is being undertaken today, and asks for your participation in the effort.

Outline

- **Background and history**
 - Fear, Uncertainty, and Doubt vs. Facts
 - The art (not science) of information protection
 - Rationalizing decisions (alternatives, decisions, bases)
- A Standard of Practice
- Building a basis in science
- SoP updates
- Discussion



Fear, Uncertainty, and Doubt

- “Computer Security” as a business

- The goal is to make money
- If it works **too well**, you don't need any more of it
- If it doesn't work well enough, you won't buy it
- How do we sell it?

FUD

- Fear
 - Bad things will happen to you – they have happened to others
- Uncertainty
 - How do you know you're safe? Who's watching the watchers?
- Doubt

- Even the NSA couldn't keep their secrets safe

Note: Consistency is not the hallmark of computer security sales

- To sell, you need to relieve the fear

- If you buy from us, you will be safe – trust us, the NSA does

Fear, Uncertainty, and Doubt

- Facts bring clarity – ignorance is not bliss
- Governments largely chose offense over defense
 - How much is spent on attack weapons vs. defensive shields?
 - “The best defense is a good offense”
 - How much is spent on “intelligence” vs. “counterintelligence”?
 - Need for intelligence outweighs the need for secure operations
- However, as the information age has dawned
 - Societies depend on critical infrastructures
 - Water, food, fuel, power, air, financial systems, record-keeping, medical and health systems, police and fire, governance, communications, and ultimately, education, environment, etc.
 - These are increasingly dependent on and connected to information systems and networks
- Critical infrastructures increasingly depend on computers
 - Can / will we unwind these dependencies? Likely NO

Fearless

The art of information protection

- Like alchemy – information protection is an art, not a science
 - A set of “mystical” notions with rules of thumb
 - Change your passwords every XX months
 - More protective measures makes for more effective protection
 - Many/most of the rules of thumb have little basis
 - The password basis stems from WW2 cryptographic systems
 - The basis for “more is better” doesn't really exist
 - Many/most of the notions are not provided with a real basis
 - Probabilistic risk assessment (largely refuted for this area)
 - Following standards improves protection posture
 - Most of the basis provided is without any science applied
 - None of the PRA elements can actually be determined
 - Most standards can be perfectly followed with little benefit

Rationalizing decisions

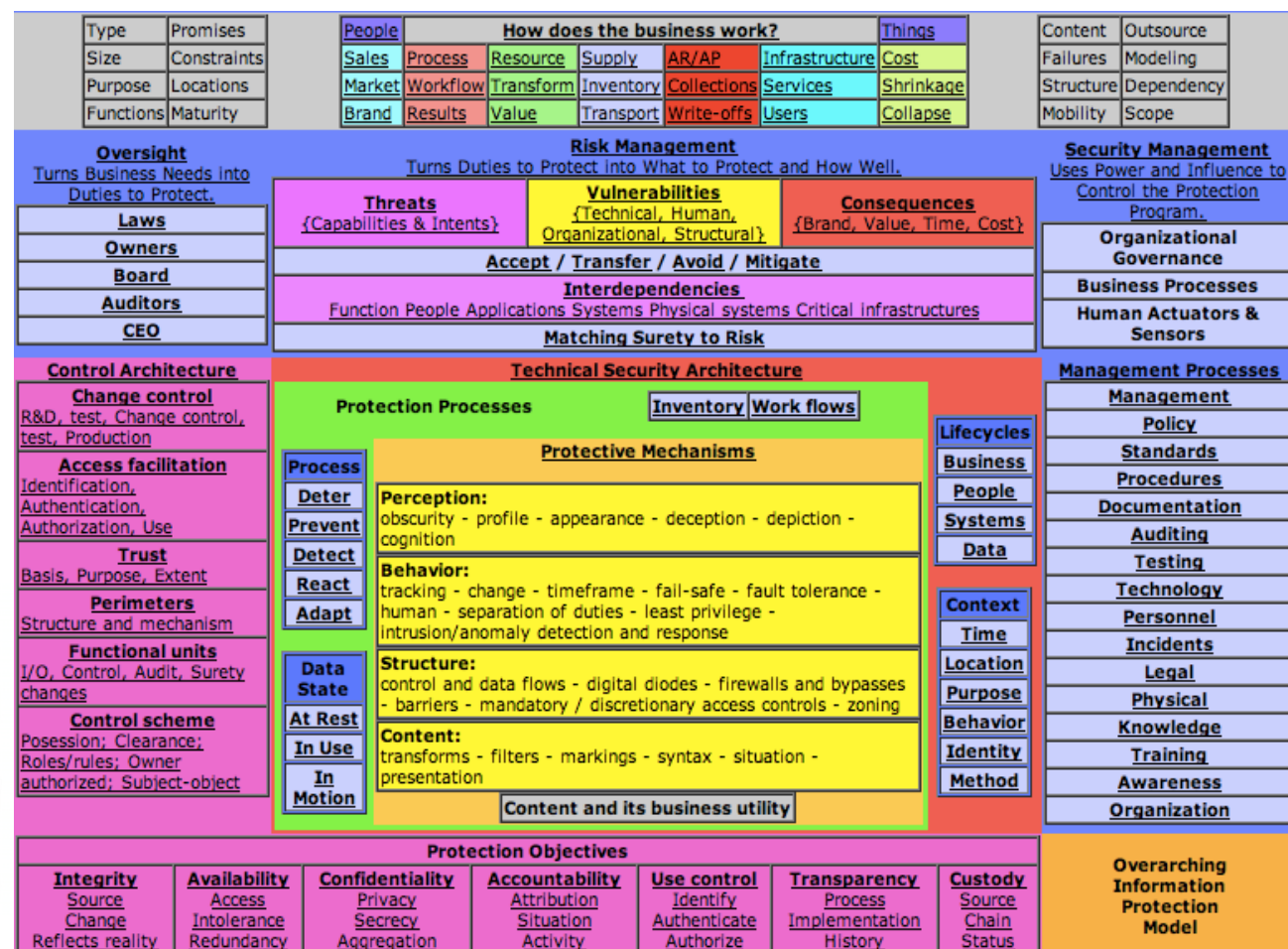
- Alternatives
 - A finite set of alternatives to choose from (the reality today)
 - Example: Duties to protect in what form?
 - Written / Verbal / Email / Web site / Database w/workflows /etc.
- Decisions
 - Conditionals based on finite numbers of facts
 - Example: If maturity > “managed” → Database w/workflows
- Basis
 - How and why these conditionals are sensible
 - This maturity level requires systematic approaches to process and this (typically today) works via a workflow system
 - Why the particular conditional applies – or why not in this case
 - But we may have a paper workflow system → no database

But why is this scientifically valid?

- It's not – but it could be
 - The reason for higher maturity levels is that higher maturity tends to reduce errors and omissions
 - e.g., Airplane safety improved by checklists etc. (lots of studies)
 - e.g., Medical care improved by checklists etc. (a few studies)
 - Higher maturity forces more well-controlled and verified process
 - But we haven't done studies on this for information protection
- We need to do scientific studies to bring clarity to this
 - Systematic presence and absence of maturity elements
 - Blind studies of errors and omissions in protection
 - Measurements and analysis to test hypotheses
 - Is higher maturity actually better? Always? How high to go?
 - When is what level of maturity called for?

Outline

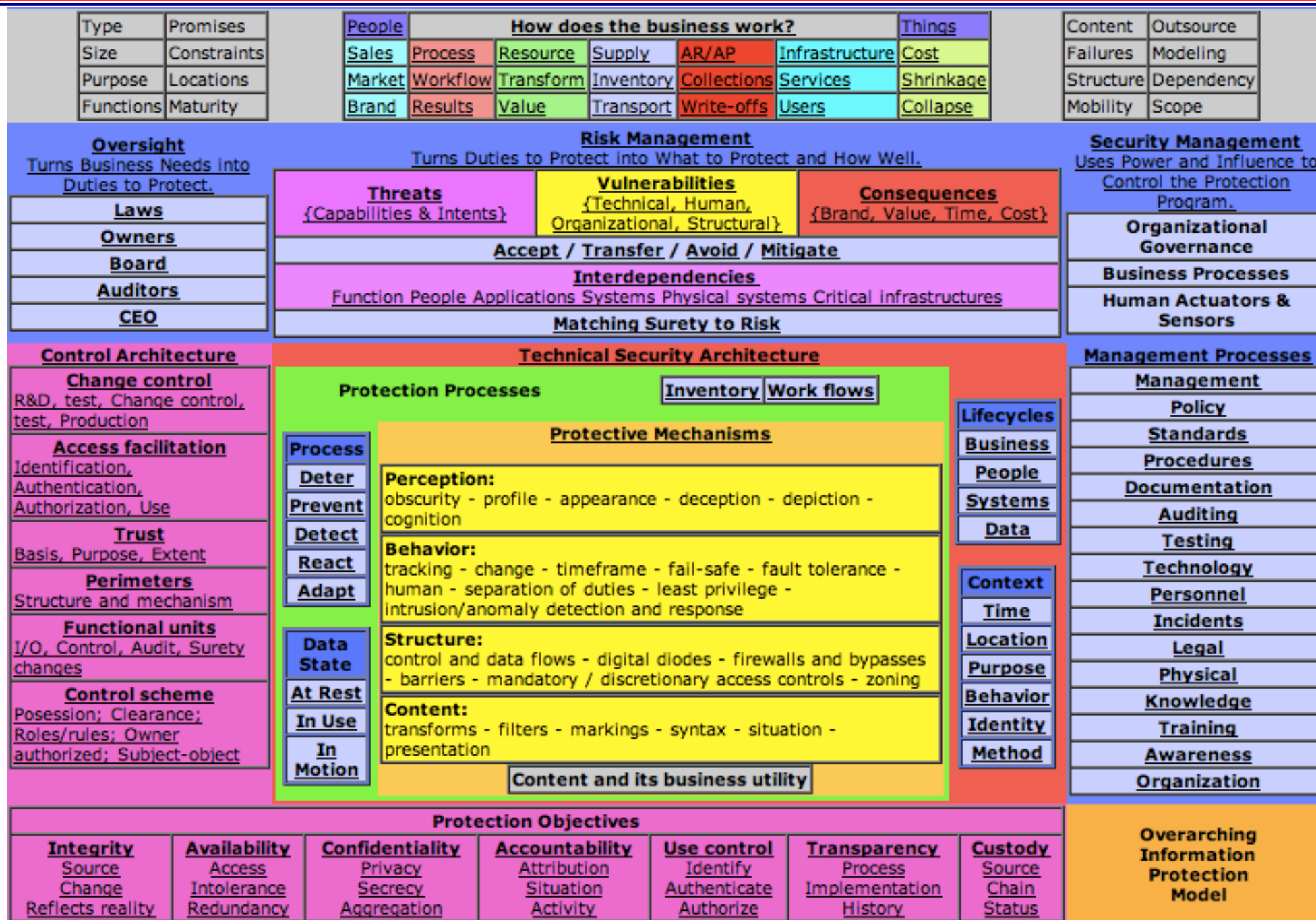
- Background and history
 - Fear, Uncertainty, and Doubt vs. Facts
 - The art (not science) of information protection
 - Rationalizing decisions (alternatives, decisions, bases)
- A Standard of Practice
 - All.Net → Protection
- Building a basis in science
- SoP updates
- Discussion



We apply our Standard of Practice

- What is a (our) Standard of Practice (SoP)
 - An SoP is **not** a “Standard” (something you follow)
 - “Reasonable and Prudent” practices (diligent vs. negligent)
 - **Not the ONLY such practices** – not always applicable
 - Open source / reviewed: <http://all.net/> → Protection → SoP ...
- We use the standard of practice to help our experts
 - Ask a reasonably comprehensive set of questions
 - Codify responses consistently in a defined language
 - Guide decisions using pre-defined bases
 - Identify variances from baselines for consideration
- When the standard practice works, we use it
 - When it doesn't, we adapt, and update if/as appropriate

The SoP



An example SoP element

- Depending on consequence, skill, and maturity
 - Some regions are identified as unsafe and not to be operated
 - Some regions have fewer process elements identified
 - As risk, skill, maturity increase, so do the “things to do”

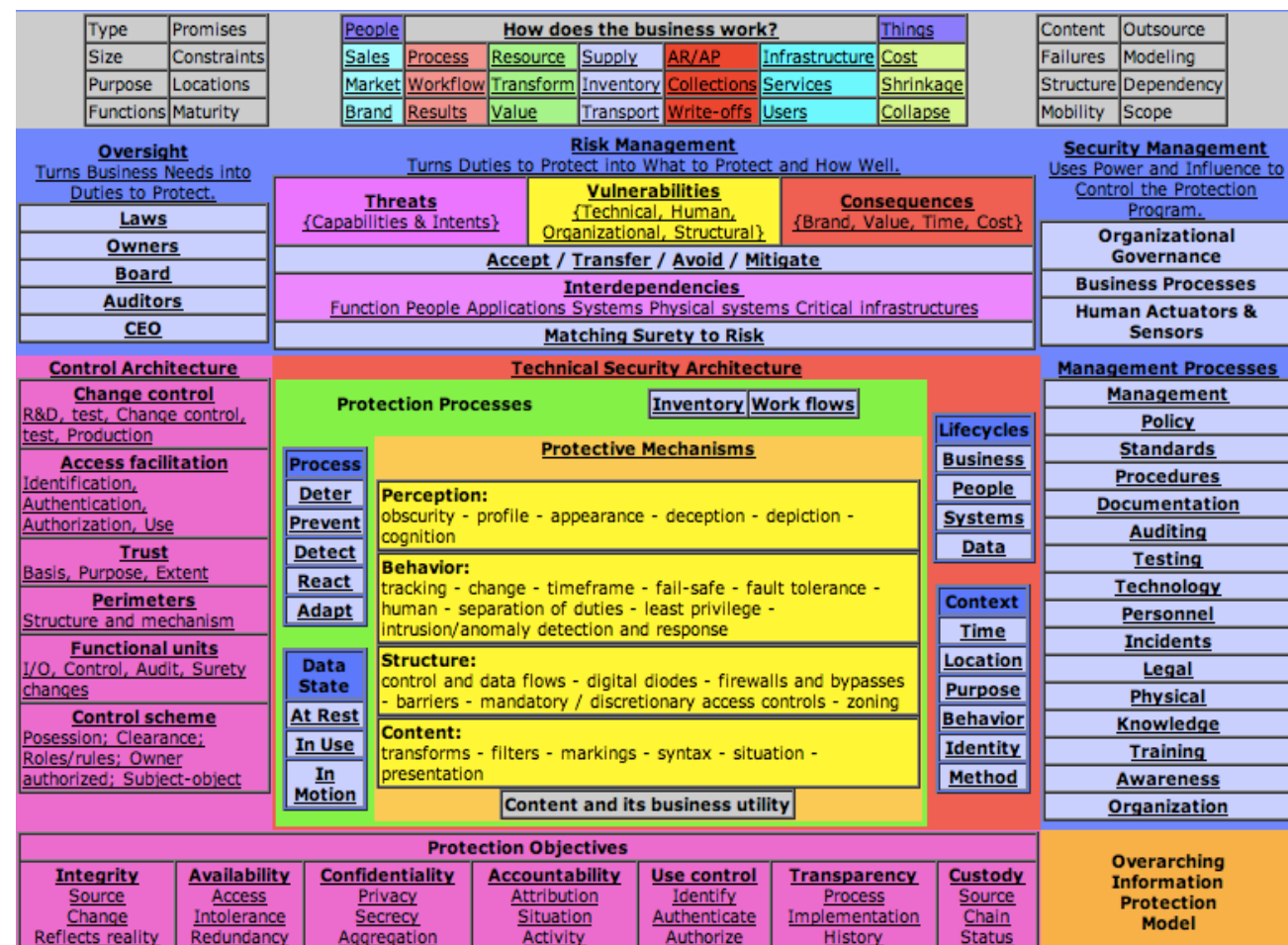
The suggested approach to real-time interdependency risk management is as follows:

Risk Level	Skill	Maturity	Alternatives
High	High	Optimizing	Real-time interdependencies should be identified in advance as far as they reasonably extend. AND 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. AND Interdependent failures should be mitigated in advance by adding redundancy and/or hardening interdependent systems. AND Interdependent failures should be mitigated in advance through failsafes and alternative operating modes. AND 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. AND Interdependent failures should be mitigated in real-time as part of the incident response process. AND 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. AND 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

Outline

- Background and history
 - Fear, Uncertainty, and Doubt vs. Facts
 - The art (not science) of information protection
 - Rationalizing decisions (alternatives, decisions, bases)
- A Standard of Practice
 - All.net → protection
- Building a basis in science
 - Theory
 - Experiments
 - Feedback
- SoP updates
- Discussion



Theory

- Theory is largely non-existent in information protection today
 - Some exceptions:
 - Some elements of cryptography
 - Some elements of information flow control (Shannon, etc.)
 - Some elements of viruses and malicious software (Cohen, etc.)
 - Some other things here and there
 - All very limited
 - Cryptography largely ignores real-world realities
 - Information flow controls are rarely used
 - Viruses and malware theory is largely on what cannot be done
 - Some other things are very limited
- We need to develop theory for hundreds of subfields
 - The SoP offers a starting point for where to explore

The science of cyber security

- Causality, Testability, Refutation, and Adaptation
 - Cause works via mechanisms to produce effects
 - $C \rightarrow^m E$ – Causality is the foundation of all science
 - A scientific theory must be testable by experiment
 - The experiment can show the theory to be wrong
 - For a universal theory, it cannot prove the theory right
 - To “test” we need to “measure” something – what?
 - When a theory is refuted, we adapt the theory
 - Or try another
- The flat earth was a scientific theory
 - An experiment proved it wrong (circumnavigation)
 - Science developed a new theory



A theory of DoS

- Resource exhaustion causes denial of services

$$\text{Resources } R = (k_1 r_1 + k_2 r_2 + \dots + k_n r_n)$$

- **C: Using lots of resources**

$$\text{Usage } U = (u_1 r_1 + u_2 r_2 + \dots + u_n r_n)$$

- Specifically, performance scales ~linearly until...

- **m: Exhaustion of available resources**

$$(k_1 r_1 + k_2 r_2 + \dots + k_n r_n) - (u_1 r_1 + u_2 r_2 + \dots + u_n r_n)$$

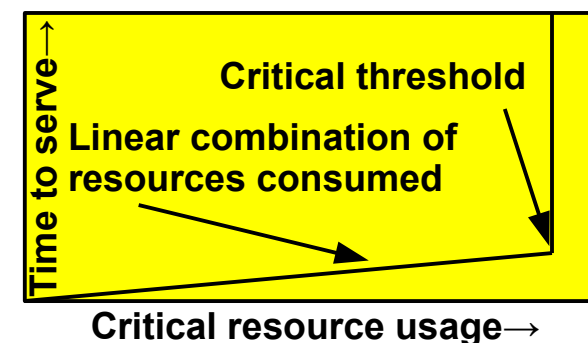
- A critical resource is exhausted \rightarrow

- **E: Denial of services** $\forall_{i < n}, \text{ if } u_i > k_i \rightarrow \text{DoS}$

- Services are no longer provided

- Examples of critical resources:

- CPU time, file handles, disk space, memory space, process table entries, TCP incoming ports, network bandwidth, internal bus bandwidth, etc.
- Problem: How do we test this theory?

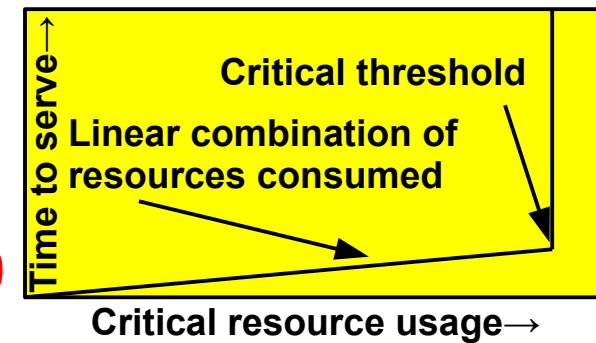


A theory of DoS

• Testing the theory:

$$R = (k_1 r_1 + k_2 r_2 + \dots + k_n r_n)$$

- Isolate a specific resource, one at a time
- Limit resource to a finite known value $k_2 = 100$
- Measure performance with consumption scale



- Consume more and more and measure performance

- Use up the limited resources

$$u_2 = (1, 2, \dots, 99, 100, 101, \dots)$$

- Consume to a threshold and it should hit a knee point
- Should deny services past the knee point

- Increase available resources

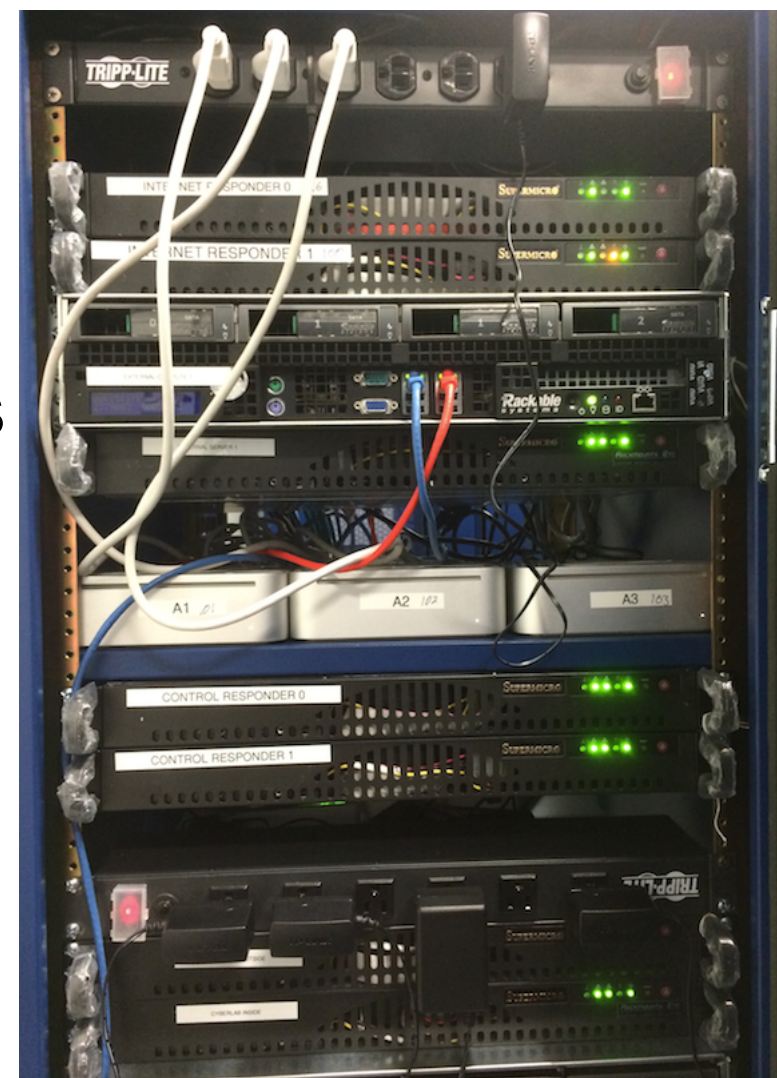
- Test over the range of resources
- Should allow services to go linear longer

- A confounding factor (non-linearity) → other resource?

$$u_2 > k_2 \rightarrow \text{DoS}$$

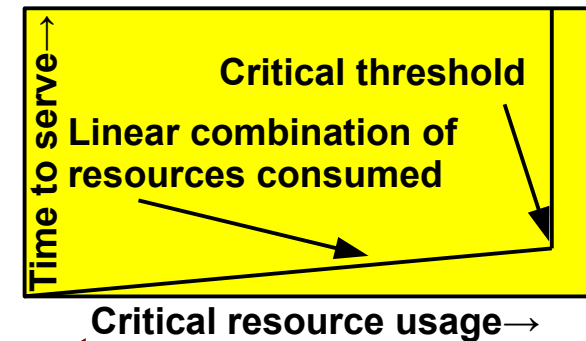
Experiments

- Webster University CyberLab
 - **Global University**
 - Classes on 5 continents
 - Including 3 locations in China
- CyberLab supports scientific experiments
 - **Repeatability using stored VMs**
 - Multiple experiments OR
 - Single larger scale experiments
 - **Global capability**
 - Access for classes anywhere
 - Multiple/redundant locations
 - Available to support scientific experiments
 - **Safe place to do otherwise dangerous things**



Interpreting the experiment

- Measured phenomena:
 - Time till correct response
- Controlled variables:
 - Available resource and consumption rate
- Experimental outcomes:
 - Normal operation limited resources
 - DDoS one computer / two computer
 - More resources
 - Subtracting out the experimental overhead
 - Is “defense” of increasing critical resource effective?



Lab assignment

- Do a better job of measuring and testing
 - Determine the parameters for various resources



- Linear relationship (all the r's and k's) $R = (k_1 r_1 + k_2 r_2 + \dots + k_n r_n)$

- Knee point (s)? (cache vs. RAM vs. page vs. ???)

- Identify and measure confounding factors

- Measure in combination \rightarrow

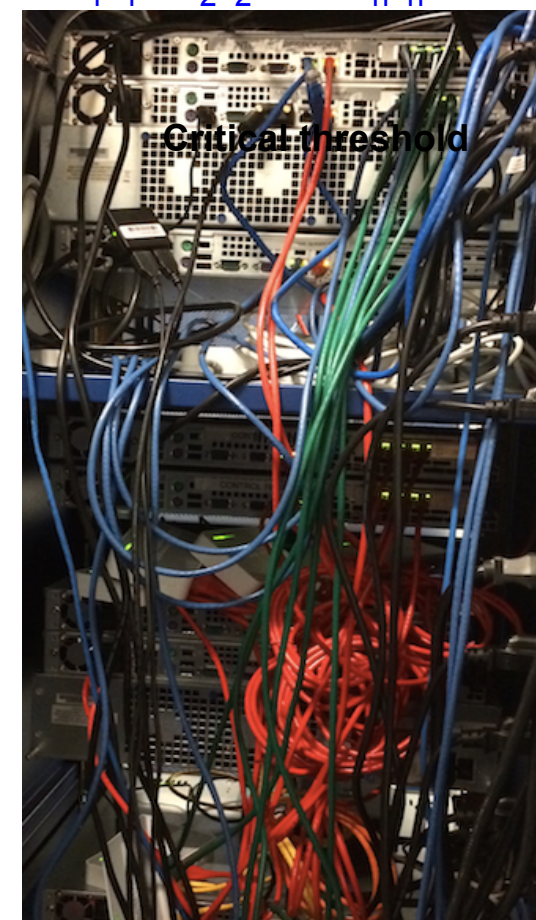
$\forall_{i < n}, \text{ if } u_i > k_i \rightarrow \text{DoS?}$

- Are the resources independent?
- Which are interrelated and how?

- Create a predictive equation $(k_1 r_1 + k_2 r_2 + \dots + k_n r_n)$
 $- (u_1 r_1 + u_2 r_2 + \dots + u_n r_n)?$

- Design a previously untried experiment
- Predict performance as $f(\text{design parameters})$
- Test to confirm / refute validity of equations
- Report results

$$U = (u_1 r_1 + u_2 r_2 + \dots + u_n r_n)?$$



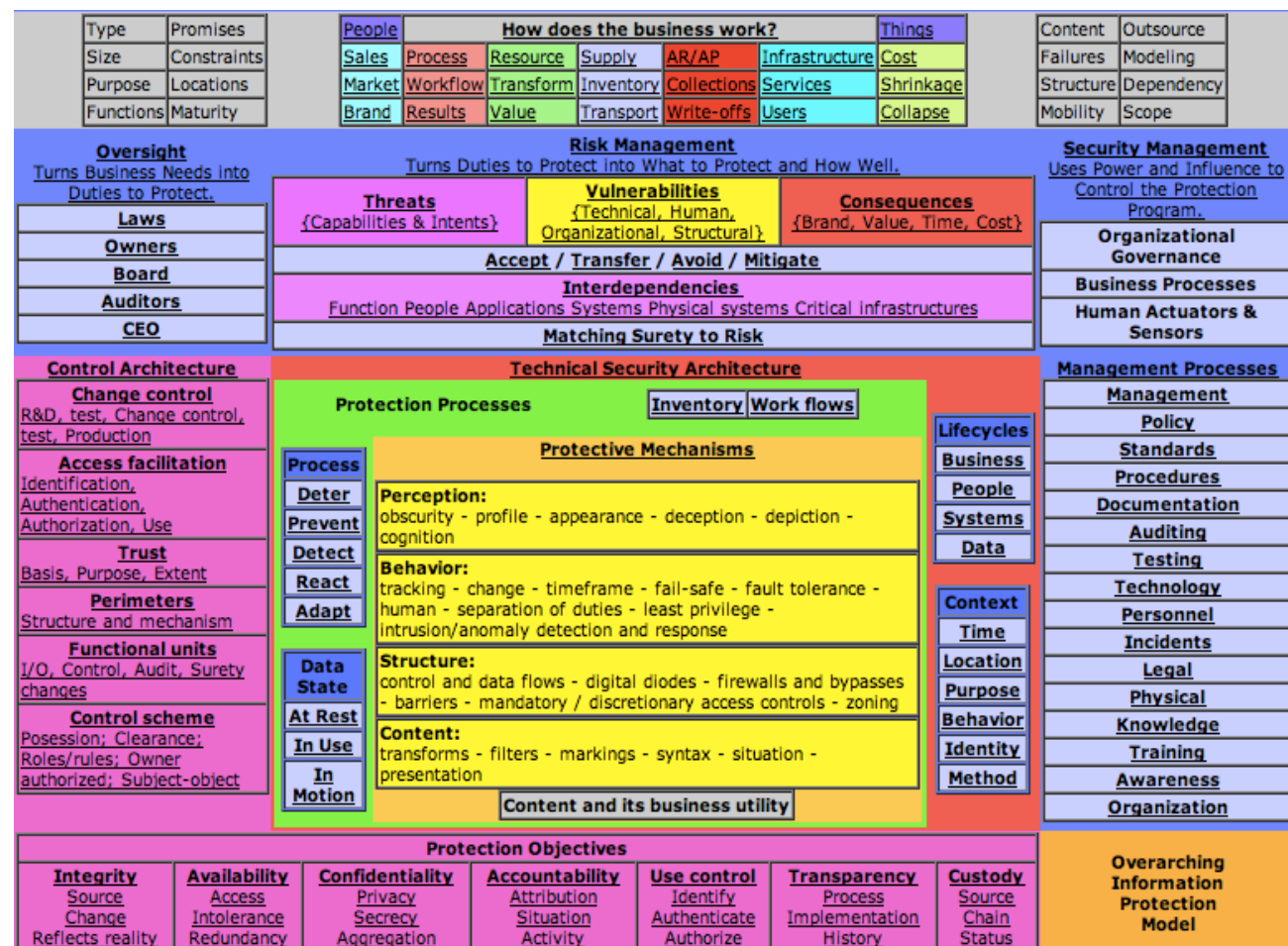
Feedback

- As results come back
 - Update the equations to more closely reflect reality
 - Try over wider ranges of parameters to explore the space
 - Identify environmental factors effecting experiments
 - Update to control for more environmental factors
 - Identify limits of observability and precision/accuracy
 - Update to account for sensor limits
 - Build better sensors and update approach
 - Update the theory as and if it is refuted
 - Limit its applicable range of uses
 - Publish results so others can benefit
 - And keep reviewing their results to update yours

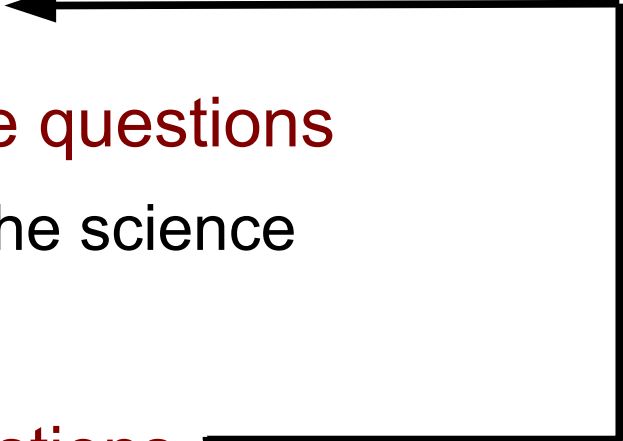


Outline

- Background and history
 - Fear, Uncertainty, and Doubt vs. Facts
 - The art (not science) of information protection
 - Rationalizing decisions (alternatives, decisions, bases)
- A Standard of Practice
 - All.Net → Protection
- Building a basis in science
 - Theory
 - Experiments
 - Feedback
- SoP updates
- Discussion



Informing the SoP with the Results

- Science tells us about DDoS and mitigations
 - The scientific results are not useful unless/until applied
 - How do we apply those results?
- Update the SoP to reflect the updated science
 - Use feedback from science to improve the SoP
 - Apply the SoP repeatedly over time to adapt protection
- The SoP asks the questions 
 - The science answers the questions
 - The SoP adapts to the science
- Things happen
 - The SoP asks more questions
- ...

ARM as a broader example

- InterPARES Trust (UBC effort)
 - *Start with the Enterprise SoP
 - *Review literature in Archives and Records Management (ARM)
 - *Update SoP for commonalities
 - *Create ARM-specific SoP (ARM-SoP)
 - *Peer review by both communities (security / ARM)
 - +Apply SoP to existing ARM entities worldwide (Oct 2 start date)
 - Compare current practices to “rote” ARM-SoP
 - Take comments on whether ARM-SoP is “reasonable & prudent”
 - Adapt SoP per comments
 - Publish results
- Experiments update and inform the SoP – and vice versa



Insurance as a further example

- Ridge Insurance Services Company (RISCO) and Fearless (FS)
 - RISCO offers cyber-insurance as a master broker
 - Underwritten by Corporation of Lloyds members and others
 - FS provides SoP reviews for potential insured clients
 - Metrics on actual practices vs. SoP with expert judgement (situation)
 - Better risk understanding for rates / deductibles / limits (theory)
 - Insurance requires reporting on losses / incidents / changes
 - Reporting (measurement) correlated to SoP results (theory)
 - FS supports improvements in protection posture by clients
 - Changes in practice tracked to feedback (measurements v. theory)
 - Report on improvements and risk changes to RISCO
 - RISCO offers rate reduction for better protection environments
 - Actuarial data produced rate reduction for better protection
 - Together we build the scientific basis through feedback



How does insurance help society?

- Decision-makers need a good reason to spend money
 - What reasons can you provide internally?
 - Whatever those reasons are, they are limited
 - You don't know enough internally to do risk management right!
- Insurance changes this by looking at risk pools
 - Many organizations with characterized protection approaches, environments, and details of changes
 - Knowledge of incidents and outcomes
 - Final outcomes result in payouts from insurance pools
 - Incidents are used against deductibles and are reported
- The net effect will be correlation between protection and outcome
 - Decision makers pay known insurance or protection costs
 - Markets drive value of goods / services per outcomes

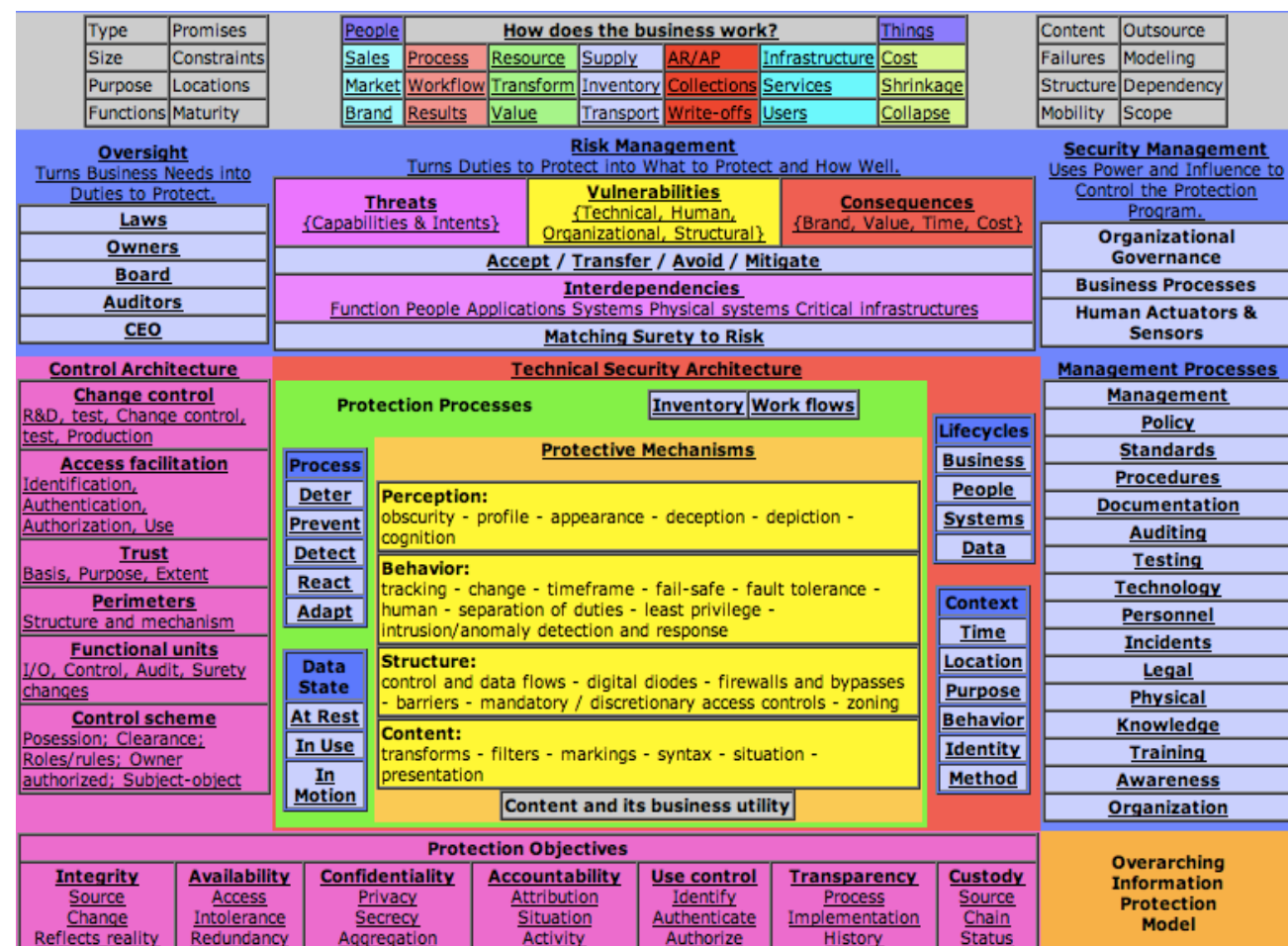
**The feedback
we have been
looking for**



Fearless Security
You have nothing to fear but fear itself

Outline

- Background and history
 - Fear, Uncertainty, and Doubt vs. Facts
 - The art (not science) of information protection
 - Rationalizing decisions (alternatives, decisions, bases)
- A Standard of Practice
 - All.Net → Protection
- Building a basis in science
 - Theory
 - Experiments
 - Feedback
- SoP updates
- Discussion



How can you participate?

- Learn what the SoPs say today
 - Review versions at <http://all.net/> → Protection
- Devise new experiments to better inform decisions
 - Take an SoP element with alternatives
 - Develop scientific experiments to differentiate conditions
 - Test to see what actually works better in what regions and why
- Publish results of the tests and inform the SoP
 - Bring clarity to the decision-making process through results
 - Let us know and we will update the basis in the SoP
 - As the basis changes, so will the decisions
- We update the SoP to meet the science and ask new questions
 - And we will seek to repeat experiments for scientific validity

Other ways to participate

- Join us!



- Work with us at UBC on the InterPARES Trust (ITrust) project

- Bring your Archives and Records Management Systems
- Work with and through the Chinese delegates to ITrust

- Support research with and at Webster University



- Get graduate degrees in cyber security
- Engage with the Webster CyberLab and Cyber Explorers
- Propose experiments to be performed in the CyberLab

- Advance the state of practice through the insurance process

- Work with Ridge Global to bring Cyber Insurance to China
- Engage Chinese underwriters with RISCO

- Bring the SoP into your enterprises as an approach

- Help translate the SoP into Chinese
- Help apply the SoP in China and globally



Thank You



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