Fearless Security – The Basics
2013-11-11
You have nothing to fear but fear itself

Dr. Fred Cohen

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Fear and relief vs. Reason

- Fear and relief sell security:
  - Basic psychology supports this approach
  - And it works well – but it leads to poor decisions
- The fear cycle:
  - 1: Propose more protection, not funded by management
  - 2: Bad things happen – blame placed on unfunded stuff
  - 3: Proposed protection is applied regardless of events
  - 4: Goto 1
- Breaking the fear cycle:
  - Make rational decisions before, during, and after events
  - But how do we do this?

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Fear / reason / rationalization

- Fear:
  - "A trio of researchers have uncovered 25 security vulnerabilities in various supervisory control and data acquisition (SCADA) and industrial control system (ICS) protocols." - threatpost.com
  - Followed by names of the "hunters", slow release, etc.
- Reason:
  - All systems and software have vulnerabilities
  - If we are architecturally protected, it won't matter
- Or is it rationalization?
  - It might matter. Our systematic approach needs to adapt to changing conditions. But we should not be in a race over vulnerabilities.

Copyright(c) Fred Cohen 2013 – All Rights Reserved

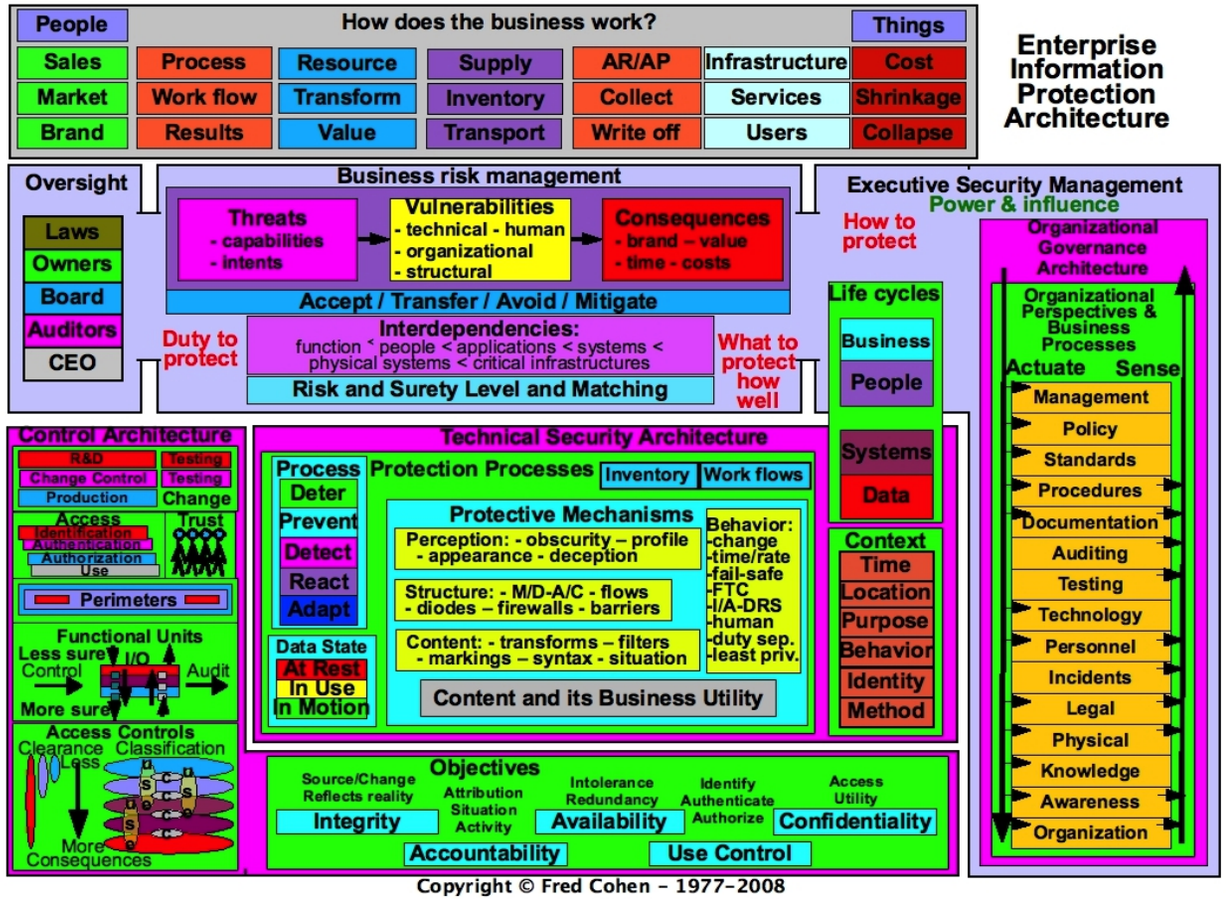
The resolution comes from science

- The difference between rationalization and reason
  - Rationalization is a theory.
    - We hypothesize that
      - All systems and software have vulnerabilities
      - If we are architecturally protected, it won't matter
  - Reason tests theories before adopting them.
    - Do ALL systems and software have vulnerabilities?
      - So far they do – and no horizon exists for this to end
      - But not all vulnerabilities produce negative consequences
    - Will architectural protection save us?
      - It might. Some architectural structures are demonstrably effective against large classes of attack mechanisms.
      - Depending in the specifics of the vulnerabilities and the architecture and its method of operation.
      - We need to analyze against the science to find out.

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Outline

- How do we make rational security decisions
  - Basics of decision-making
  - A standard of practice
  - Specify & review – separation of duties – independence
- How does Fearless do it?
  - Scientific research
  - Independent expertise
  - Working as a team
  - Outreach
  - Tools and techniques
- Discussion



Copyright © Fred Cohen - 1977-2008

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Basics of decision-making

- There are many different facets of decision-making
- But most strategic protection-related decisions have (or should have) specific characteristics:
  - Objective, Qualitative, Nominal, Flat, Complex, Predictive, Group, Formal (well-defined), Satisficing, Architecture, Ad-hoc, Work, Enterprise process decisions made using Text for Strategic purposes driven by Models- and/or Knowledge-based Internally defined evaluation criteria at Group consideration speed tempo by decision-makers with Group expertise in a Static decision space with Mixed competitive, cooperative objectives.
- While tactical decisions have (or should have) quite different characteristics...

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Strategic protection decisions

- Typically 100 or so key strategic decisions
  - Decisions are between a limited set of alternatives
    - Usually only a few choices and factors
  - The information needed to make them is limited
    - Collecting the information is often fast and simple
  - The decisions require high-level situational knowledge
    - Typically 3-5 people are adequate for preliminaries
  - Every organization is different
    - There is no perfect generic solution or right checklist
  - There are reasons for choices
    - Science is preferred - but sometimes rationalization is the only thing available
    - But rationalization must be tested for refutation!

Copyright(c) Fred Cohen 2013 – All Rights Reserved

A Standard of Practice

- Our practice is helping others make good decisions
- Our standard of practice is the approach we follow
  - Why do we do this?
    - Why do airline pilots use checklists?
    - What happened when doctors applied this?
    - We find it to be better / faster / cheaper – all three
  - How do we do this?
    - We use people with knowledge, skills, experience, etc.
    - We use tools that facilitate and support those people
    - We peer review heavily and try to stay knowledgeable
    - We adapt to the client reality and update when needed
  - We publish the details for public comment
    - http://all.net/ → Protection → Standards of practice

Copyright(c) Fred Cohen 2013 – All Rights Reserved

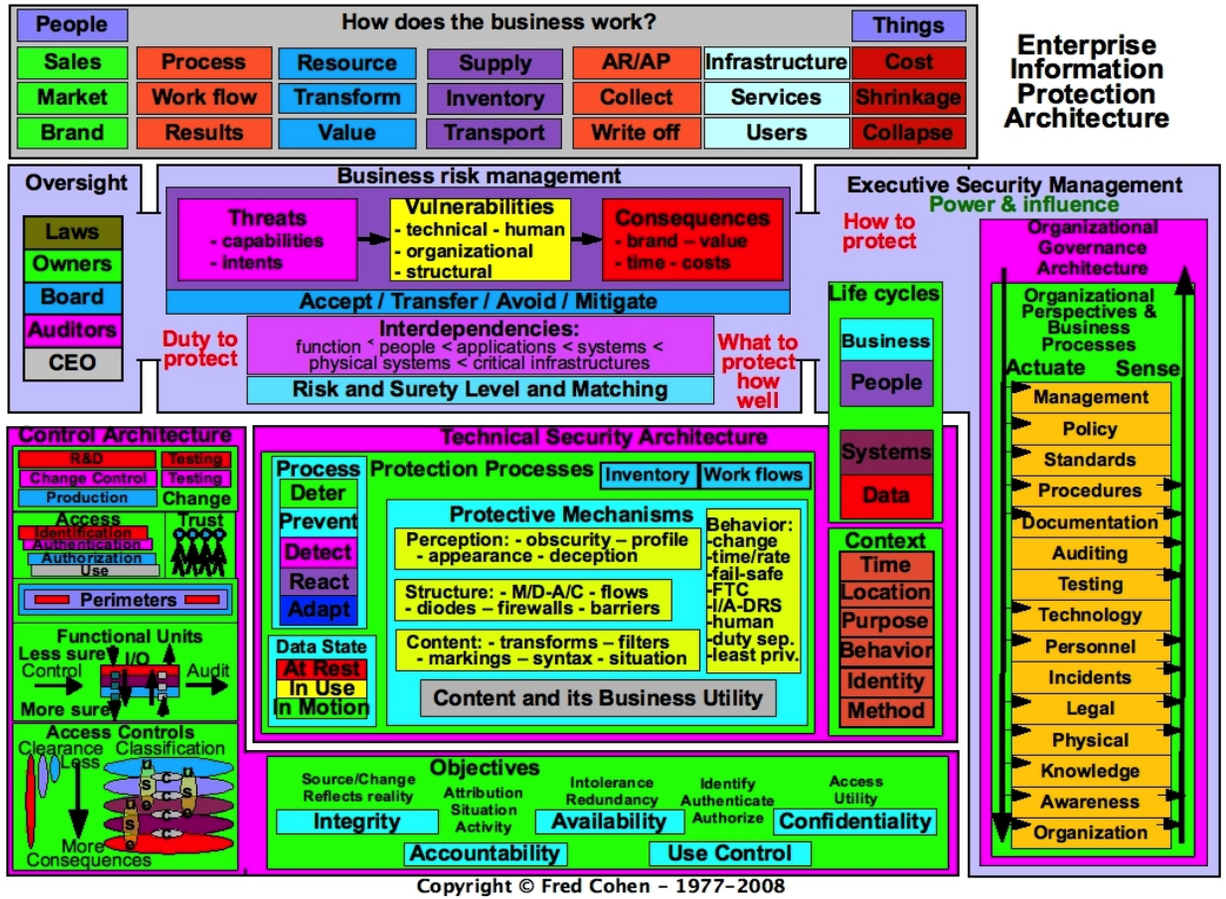
Separation of duties issues

- There is a fundamental issue
  - Separation of duties between specify, perform, verify
    - If you do all three, you can subvert any system
  - Our standard of practice identifies requirements to separate specification, performance, and verification
- The standard of practice is fundamentally a specify and review (verify) process
  - The standard of practice is clear
    - Those who **Specify** and **Verify** **MUST NOT** **Perform**
- We **Specify and Verify** – We do **NOT** **Perform**
  - NOTE: Those who **Perform** **MUST NOT** **Specify or Verify**
  - **Of course we do perform for our own protection…**

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Outline

- How do we make rational security decisions
  - Basics of decision-making
  - A standard of practice
  - Specify & review – separation of duties – independence
- How does Fearless do it?
  - Scientific research
  - Independent expertise
  - Working as a team
  - Outreach
  - Tools and techniques
- Discussion



Copyright © Fred Cohen - 1977-2008

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Scientific research

- Fearless is a division of Management Analytics
  - Management Analytics does research & development
    - For clients as part of our forensics and related work
    - As part of technology licensing and related work
    - As part of our expert witness work
    - Operation of All.Net and affiliated companies
  - Team members keep up with and perform research
    - With and for government organizations
    - With and for private enterprises of all sizes and sorts
    - With and for universities and educational institutions
    - In peer reviews for research journals and conferences
    - As part of community participation

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Techniques

- Independent expertise
  - Not affiliated with vendors / don't do vendor selection
  - Industry press / analysts members
- Working as a team
  - Strong internal peer review process
  - External review of standard of practice
- Outreach
  - Participation in NIST, ICS-ISAC, Conferences, Journals, …
  - Active response to fear-based security in social media
  - All.Net, FearlessSecurity.com, this Webinar, etc.

Copyright(c) Fred Cohen 2013 – All Rights Reserved

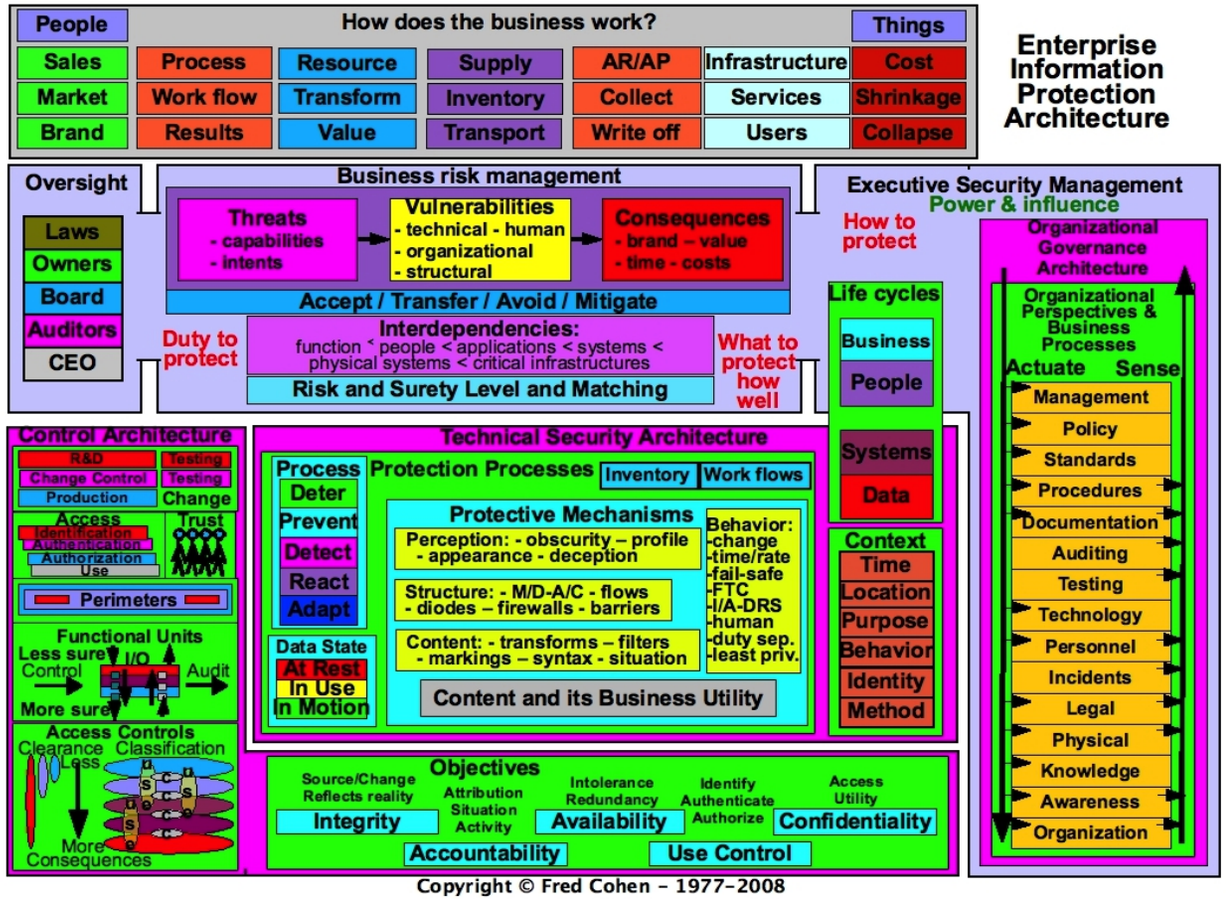
Tools

- JDM
  - A data collection and analysis support tool
  - Used for real-time remote desktop review and specify
  - Supports as-is, future state, gaps, transition planning
  - Draft reports instantly available – no surprises
- Decider
  - Multi-factor group decision-making process with justification, report generation, libraries, sharing, …
- People
  - Tools are just tools. People are needed for judgement.

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Outline

- How do we make rational security decisions
  - Basics of decision-making
  - A standard of practice
  - Specify & review – separation of duties – independence
- How does Fearless do it?
  - Scientific research
  - Independent expertise
  - Working as a team
  - Outreach
  - Tools and techniques
- Discussion



Copyright © Fred Cohen - 1977-2008

Copyright(c) Fred Cohen 2013 – All Rights Reserved

Thank You

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

Copyright(c) Fred Cohen 2013 – All Rights Reserved