Resilience via Measurement

Mike Lloyd, CTO
Presentation at 9th Workshop on Internet Economics

REDSEAL

Problem to Address: Lack of Digital Resilience

- Breaches are all too common
  - Marriott is just the latest
    - 500 million customers affected
  - Open Question: are breaches getting worse?
    - Some signs say “not really”
    - Measure them like earthquakes?
      - Log scale, annual hazard rate

Root Cause: Complexity

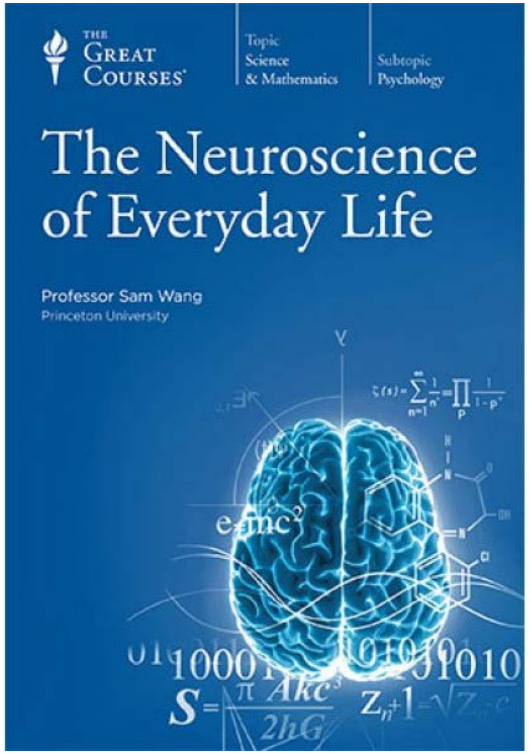
- We know a great deal about making elements secure
  - Checklists, frameworks, hardening guides
- We know people do not follow all this advice
  - Cost? Time? Attention? Scale?
- Every network has an error rate
- Networks cause complex interactions
- Creates fragile systems

Everyday Hard Decisions

- Defenders can’t tell where to focus:
  1. Hardening elements
  2. Understanding networked dependencies
  3. Launching new control or tech
  4. Improving process or training
  5. Connecting security to other objectives

- Need better ways to prioritize
- Could we ever tell we’ve done enough?

Where Resilience Gets Lost



- Central Nervous System
- Systems
- Maps
- Networks
- Neurons
- Synapses
- Molecules

- Business
- Business Units
- Zones
- Networks
- Applications
- Software
- Hardware

- GRC
- Qualitative Assessments

- Hardening Rules
- Checklists

Policy Goals, worst to best

Regulation is here

Vendors (like me) are here

Open space for:
Research
Insurance

A Simple Three-Step Plan

1. Measure defensive posture
2. Gather breach records
3. Correlate

How hard can it be?

Insurance – on a Parallel Track

- Insurers have one massive asset
  - Claims data, as a proxy for breach data
- Similar goals, but:
  - Not keen on disclosure
  - Focused on insurable events
- Two major measurement problems
  - Resilience of one organization
    - “Non-smokers discount”
  - Portfolio correlation risk
    - Monoculture, group-think, systemic risk
    - Open space for research?

Measurement Problem: Easy vs Good

- Outside measurement is easy, but …
  - No visibility of internal processes or readiness
  - Often looks at “proxies” of security
    - e.g., expired certs, not actual attack pathways
    - Does it drive the wrong behavior?
  - Imagine insuring a building against fire, based on a photo across the street
- Inside measurement is great, but …
  - Invasive; requires permission
  - Not easily shared/compared
  - Vendors (like me) do this in proprietary ways

WIE Goals

1. Policy goal
   - Improving digital resilience
2. Data needed to measure progress:
   - How well secured are real networks?
   - What is the hazard rate?
3. Methods:
   - Compare inside vs outside measurements
   - Establish hazard rates from public sources
4. Who/how
   - Good question …

Discussion Areas

- Context for sharing of risk measurements
  - Anonymized? But how would we correlate against breach reports?
  - Every company wants comparison to peer groups
    - Can we extract “group X commonly does Y, hazard rate R”?
- Establish true hazard rates
  - Are breaches getting more/less common?
  - More disclosure, more better
- How to correlate
  - Indicator variables: “I bought tech X” or “adopted framework Y”
  - Don’t we need to study whether it was used sensibly/effectively?
    - Does shelfware indicate anything?

REDSEAL

Thank you.