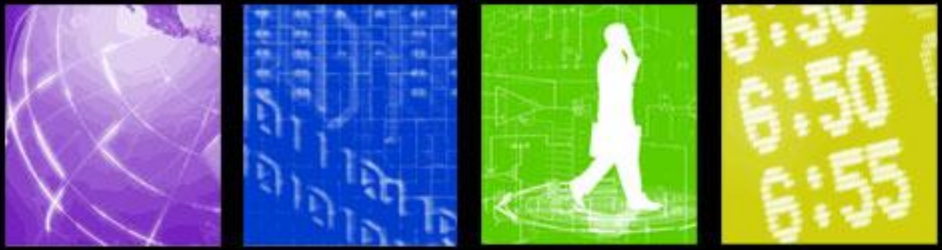


LAYER one

May 28-29, 2011

Security Prioritization in Large Organizations

Kevin Nassery
http://kevn.org
kevin@nassery.org
Twitter: @knassery

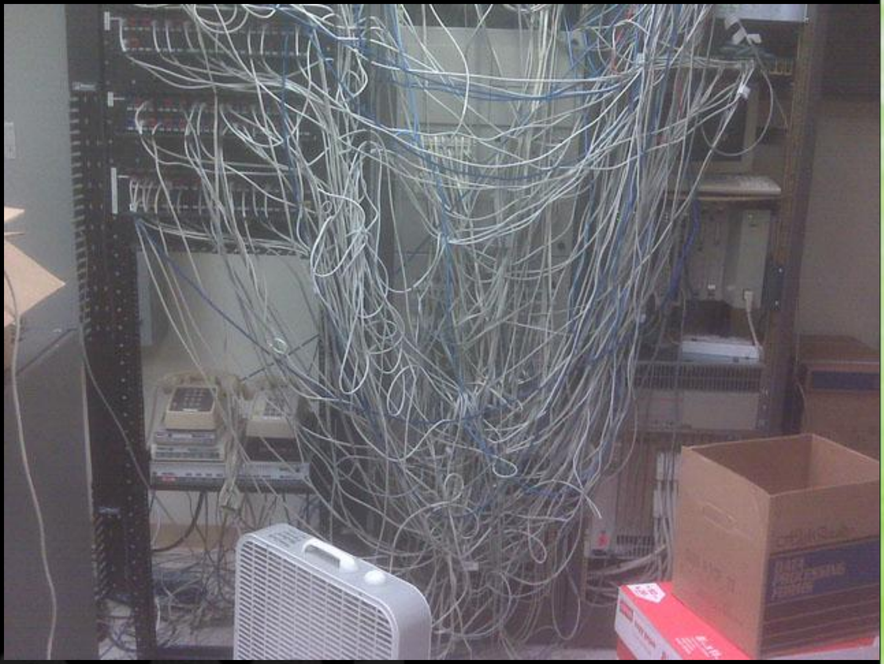
My Background

- Spent 10 years focused on infrastructure architecture and engineering.
- Chief Infrastructure Architect for large online marketing firm for ~4 years.
- Former principal security consultant, doing work at enterprises large and small.
- Now running internal penetration testing and security research group for a large bank.

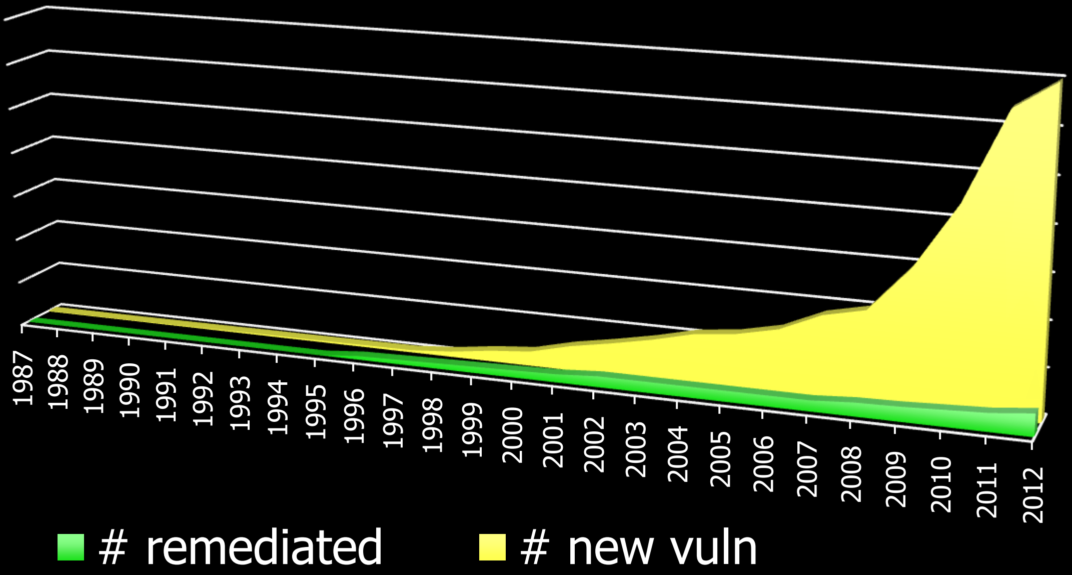
The Problem

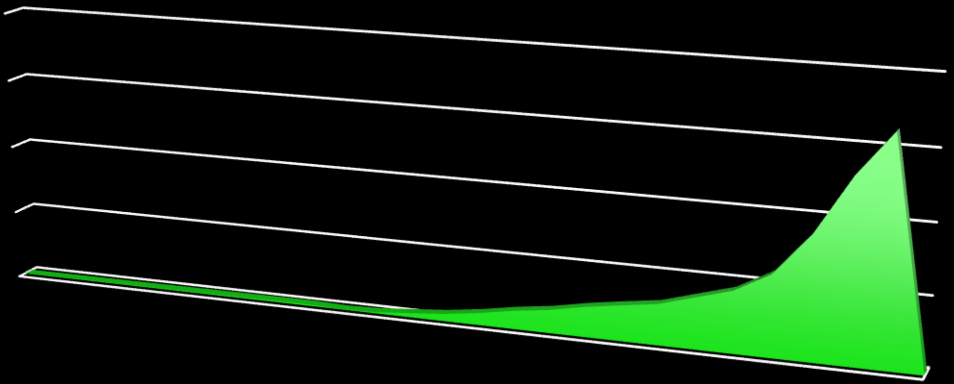
How can we make the biggest impact on the security of an organization with the resources we have?

- Organizations have decades of “security debt.”
- Generally we create new problems faster than we solve any problems, (debt grows).



New Vulnerability vs Remediation Velocity





Active Vulnerabilities

Common Problems

#1 We stop thinking critically about problems and their root cause.

- We operationalize the wrong solution.
- Very poor return on investment in remediating individual issues.
- We underestimate the complexity of systems and the attack surface.
- Distributed problems are harder to solve than central problems.
- Marginalizes our most precious resource, talented people.

Common Problems

#2 We focus on "known" security issues.

- Very little internal security research to identify new security issues.
- We purposely limit our visibility into security issues, based on limited ability to react.
- Direction of security generally comes from external sources.

Common Problems

#3 False hope in policy over technical controls.

- We know people are the weakest link, how is any control based on their behavior helpful?
- Policy should be developed in harmony with detective and resistive controls.

In March 2007, the D.A.R.E. program was placed on a list of treatments that have the potential to cause harm in clients in the APS journal, *Perspectives on Psychological Science*.

D.A.R.E.
TO RESIST DRUGS AND VIOLENCE.
DRUG ABUSE RESISTANCE EDUCATION
D.A.R.E.
ESTABLISHED 1983

Common Problems

#4 Security metrics are being abused.

..the metric we are looking for is 76%
YEAH!
SURE.
RIGHT ON!
.. we know the answer, how do we match that to the actual data?

http:///www.curphey.com

- Lack of transparency.
- Lack of utility in the decision making process.
- Being used to justify security spend, not measure security performance.
- Work effort on metrics can often overwhelm security action efforts.

Common Problems

#5 Team charters are often not conducive to security insight.

- Very little cross-over knowledge sharing in most organizations.
- Defense in depth is error prone in layering/division of security responsibility.
- Security is almost always reactive or external to technology deployment.

Common Problems

#6 Culture of process.

- Applying the same process different issues generally leads to ineffective and inefficient work efforts.
- By design limit creative people.
- Inflexible, and painful.

Moving Forward

#1 Transition investment from security operations to internal security research and automation development.

- Enable culture of critical thinking and creative problem solving.
- Improve understanding through root cause and failure analysis.
- Move security operations closer to technology operations.

Moving Forward

#2 Where resistant controls are difficult, develop detective controls.

- Often more effective.
- Very few obstacles of security debt.
- Can be very cost effective given investment in good security data centralization (flow data, log data, interrogative capability into devices).

Moving Forward

#3 Analyze defense in depth strategy against organizational charter to find responsibility gaps.

- Identify more effective organizational structures.
- Increase cross-team collaboration.
- Increase inter-domain technology knowledge.

Moving Forward

#4 Move towards creative culture:

- Use processes to increase efficiency and consistency, not to control creativity.
- Facilitate individual research efforts.
- Avoid falling into a culture of rigid process.
- Use penetration testing and vulnerability data to identify systemic problems.

Moving Forward

#5 Increase visibility regardless of remediation capability.

- Gain better understanding of security posture.
- Quantify the systemic issues (good security metrics).
- Understand security interaction between cohabitated systems and the combined attack surface.

Moving Forward

#6 Hire fewer, and better people.

- Enthusiasm for technology and security.
- Understand importance of finding the origination of issues.
- Can facilitate remediation strategy.
- Good problem solvers.

Then what?

How do we prioritize effort?

- Understanding and modeling threat perspectives large to small.
- Don’t run from uncertainty, include it in your scoring and reduce it through research.
- Find statistically significant issues, identify systemic failures, triage major risks, work to facilitate remediation at origination level.

More prescriptive commentary.

Common, big wins I’ve seen.

- Controlling the user-population network access control (network admission control).
- Isolate and insulate legacy infrastructure.
- Turn things off more aggressively.
- Identify which assets are “under control.”
- Rely principally on “empirical” data.
- Model system security lifecycle in your organization.

Discussion/Questions?

kevin@nassery.org

@knassery on Twitter

http://kevn.org