Web Application Security Strategies -- OWASP Taiwan 2008

Yen-Ming Chen
Director of Consulting, Northwest
Foundstone, A Division of McAfee

Yen-Ming.Chen@Foundstone.Com

OWASP

Agenda

- Security Problems and Statistics
- Analysis
- Strategic Planning
- Conclusion

Yen-Ming Chen

- Director of Consulting, Northwest.
- Joined Foundstone in 2000
- 4 Contributing authorships: HE 3rd edition, HE of Web App, Win XP professional Security and HackNote Web security
- Dozens of articles in SecurityFocus, DevX, SysAdmin, PCWeek, CNET Taiwan, ITHome and other medias
- Invited speaker for world wide security conferences
- MSIN from C.M.U. Information Networking Institute (1999)

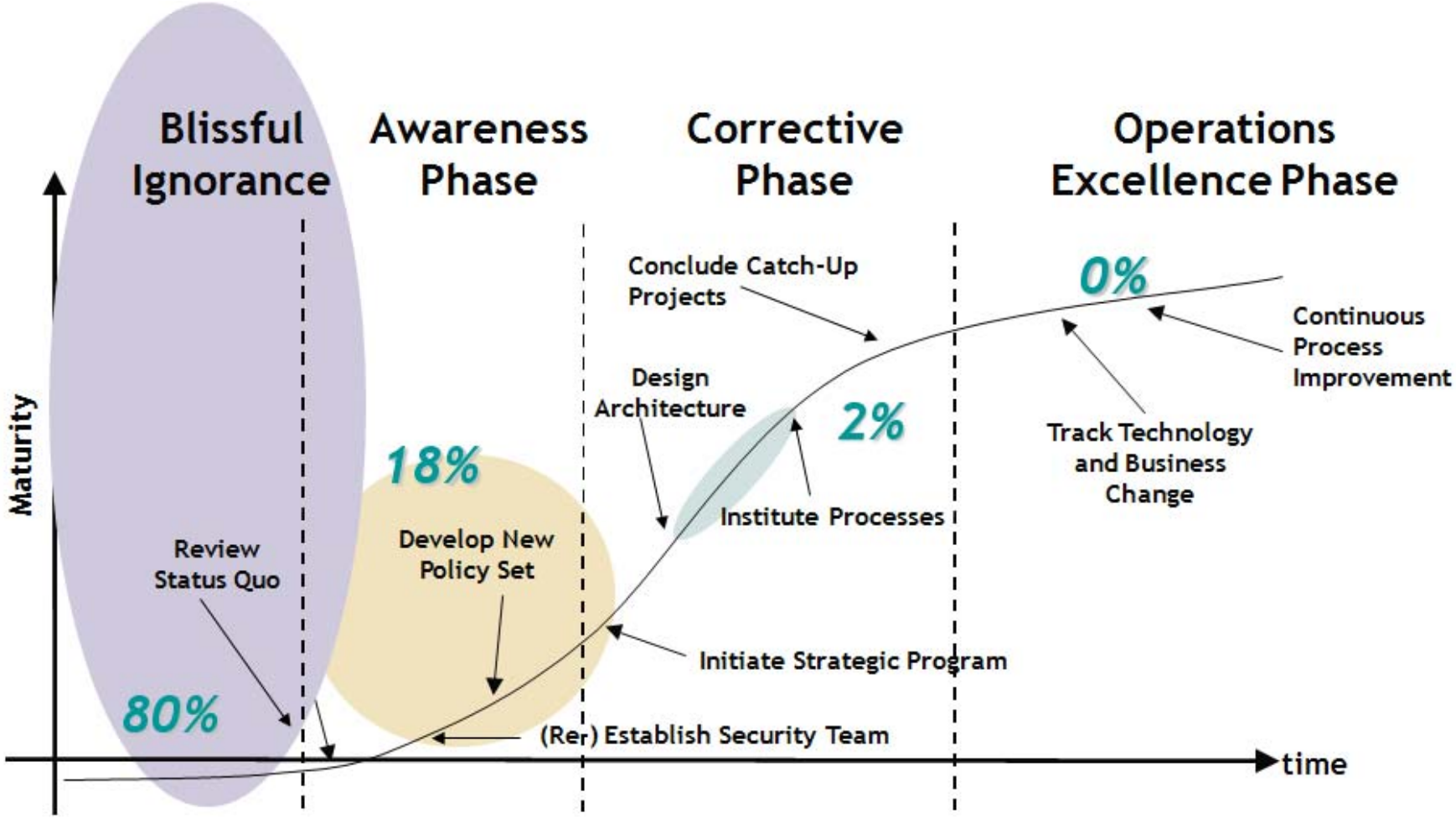
Thus do many calculations lead to victory, and few calculations to defeat

SECURITY PROBLEMS

Current Status

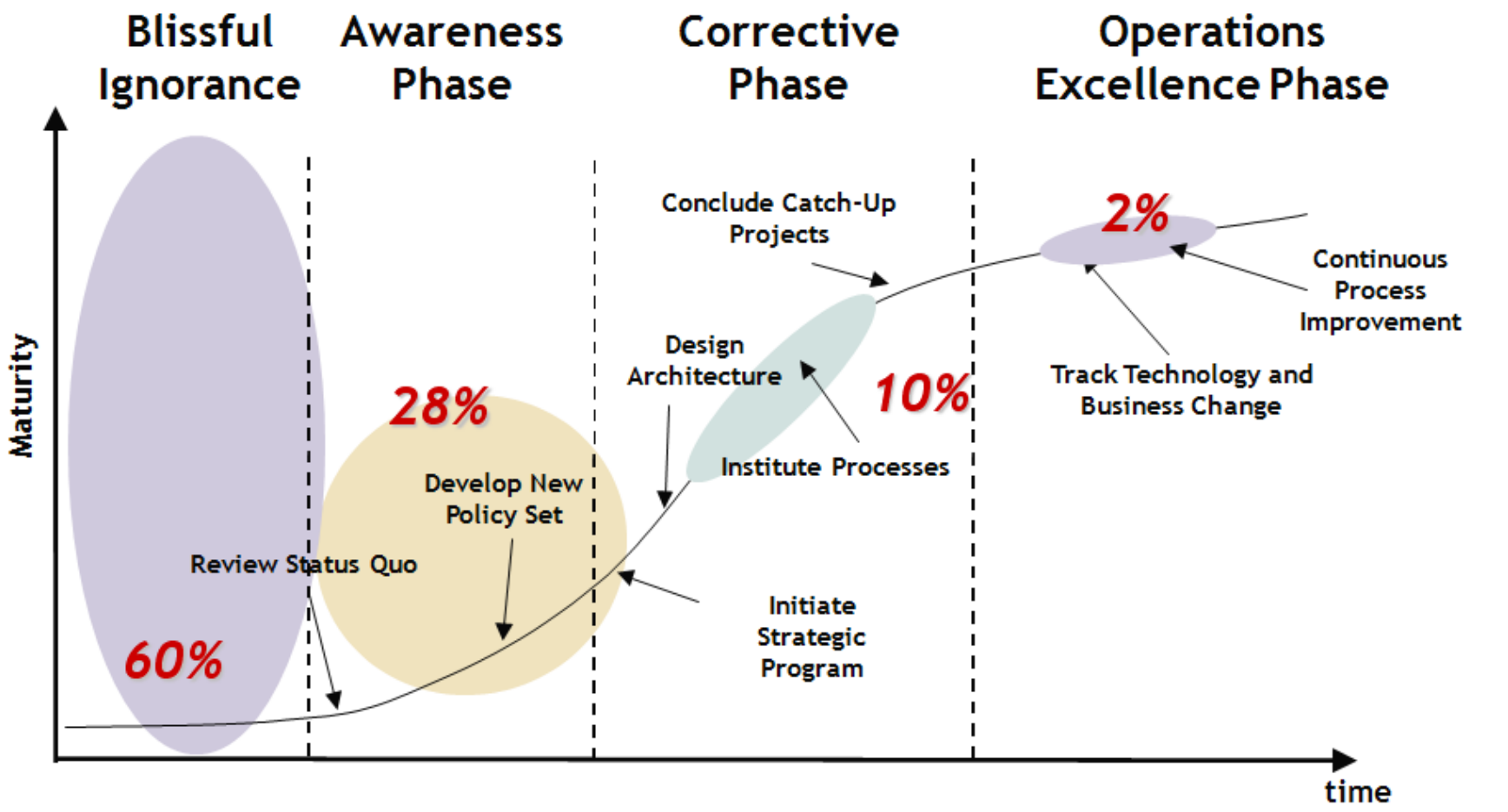
- Security Maturity
- Attack Target Shift
- Security Ecosystem
- SQL Injection
- Why You Still Can't Rely on Automated Tools

Information Security Maturity: 1996



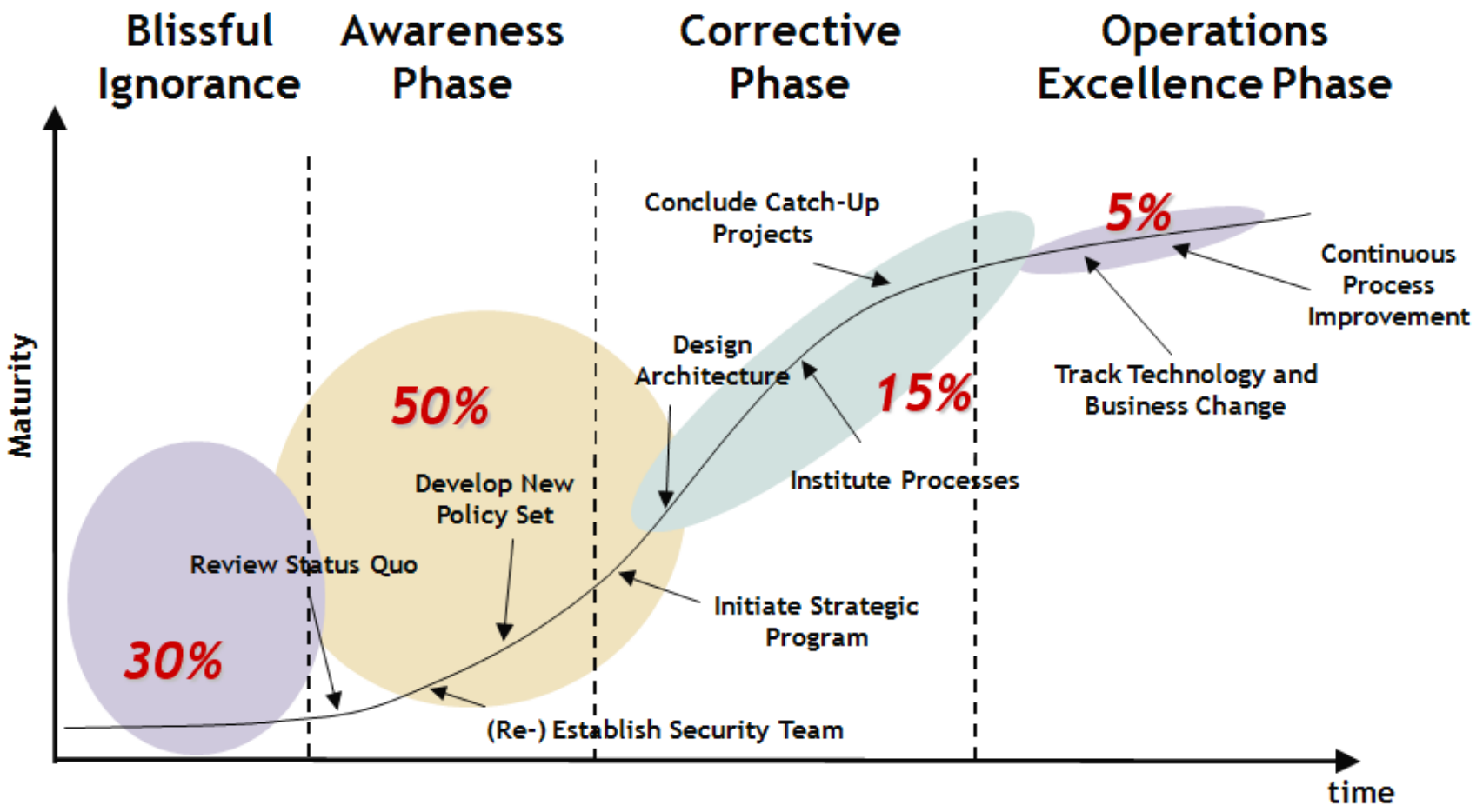
NOTE: Population distributions represent typical, large G2000-type organizations

Information Security Maturity: 2000



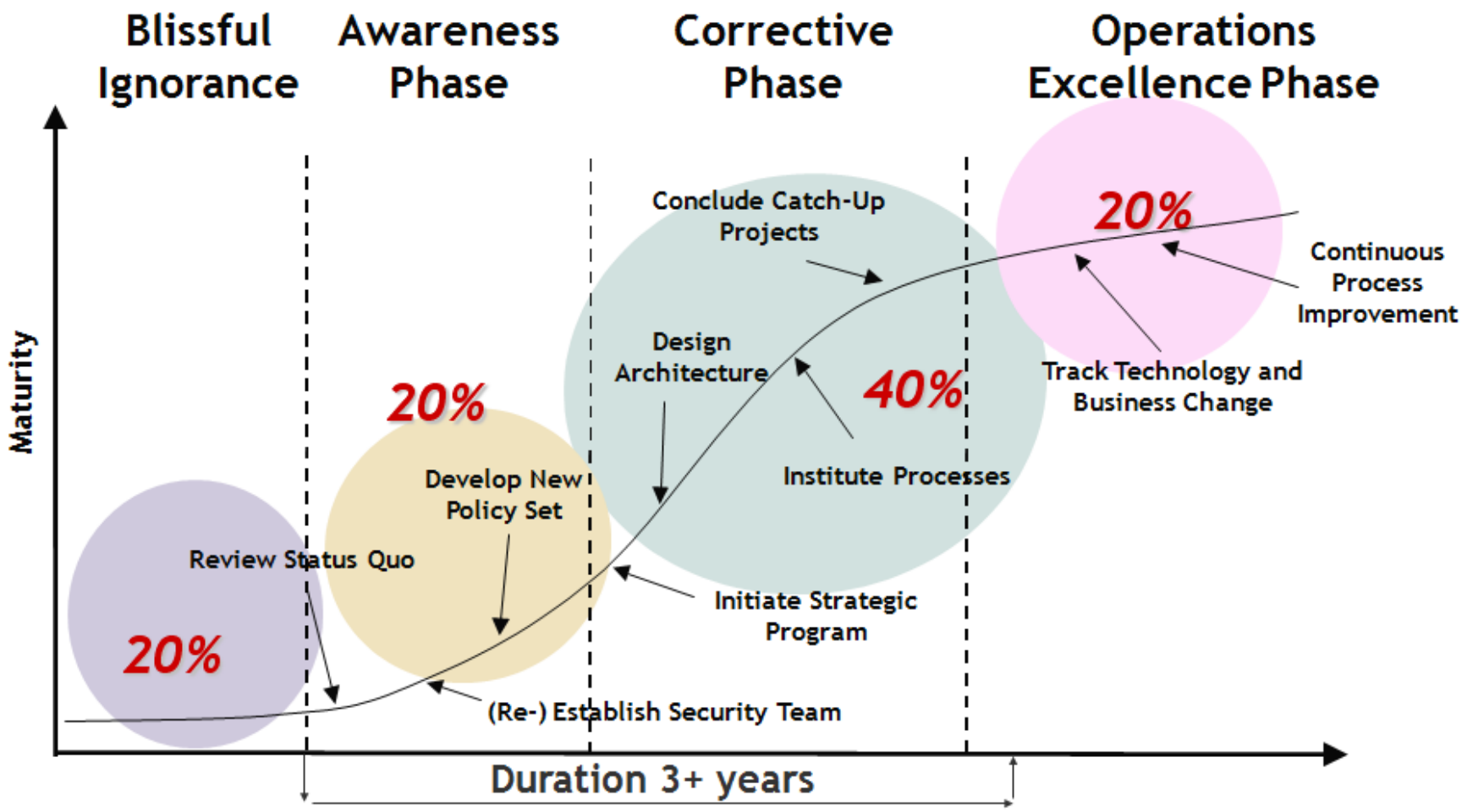
NOTE: Population distributions represent typical, large G2000-type organizations

Information Security Maturity: 2004



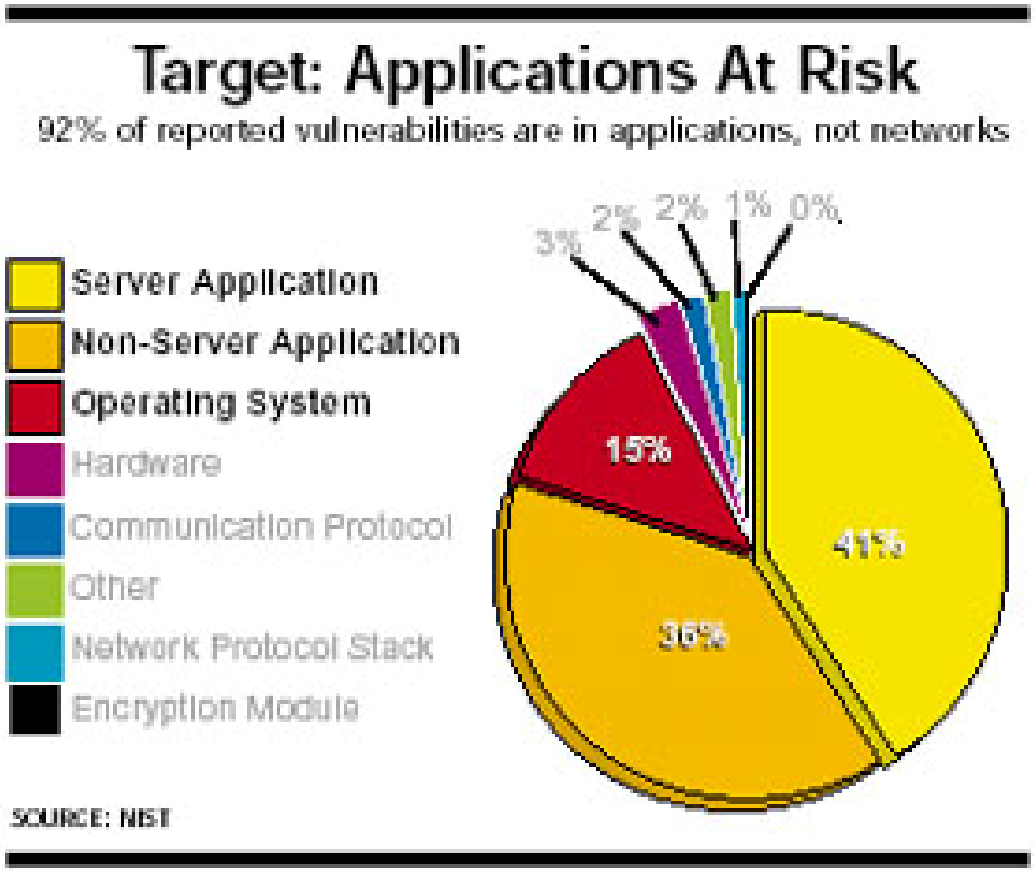
NOTE: Population distributions represent typical, large G2000-type organizations

Information Security Maturity: 2008

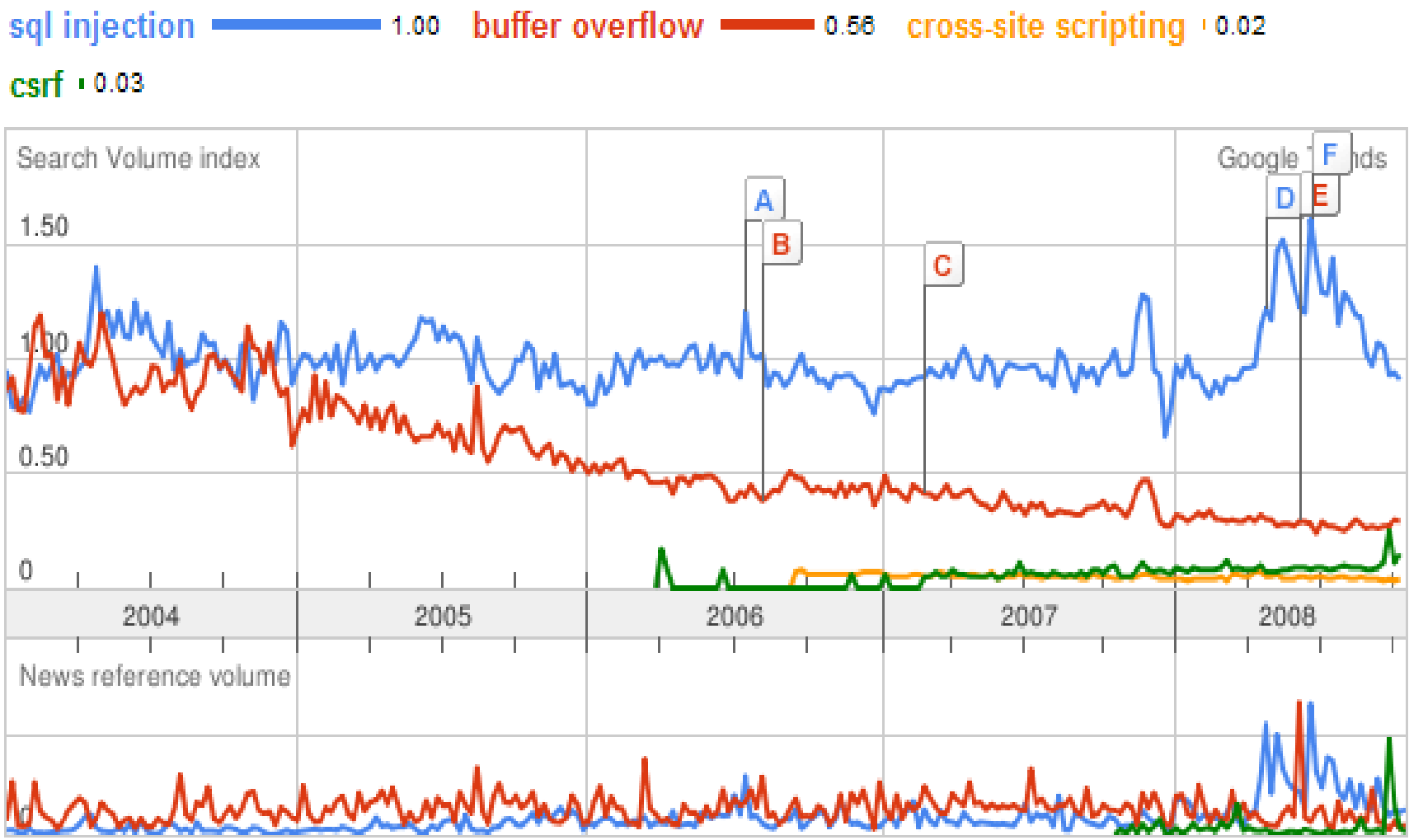


Attack Target Shift

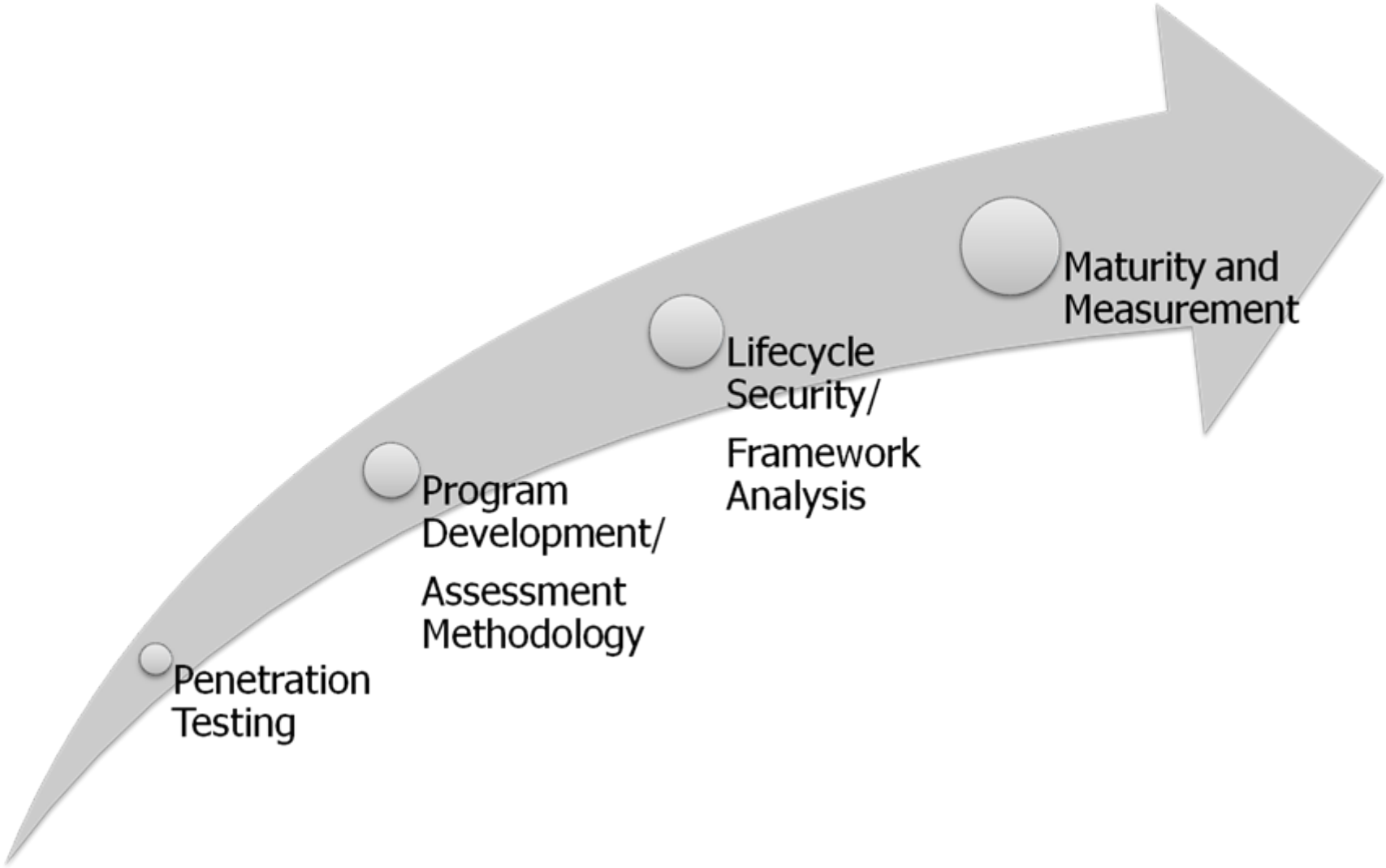
- From server to application; from corporate network to every user.



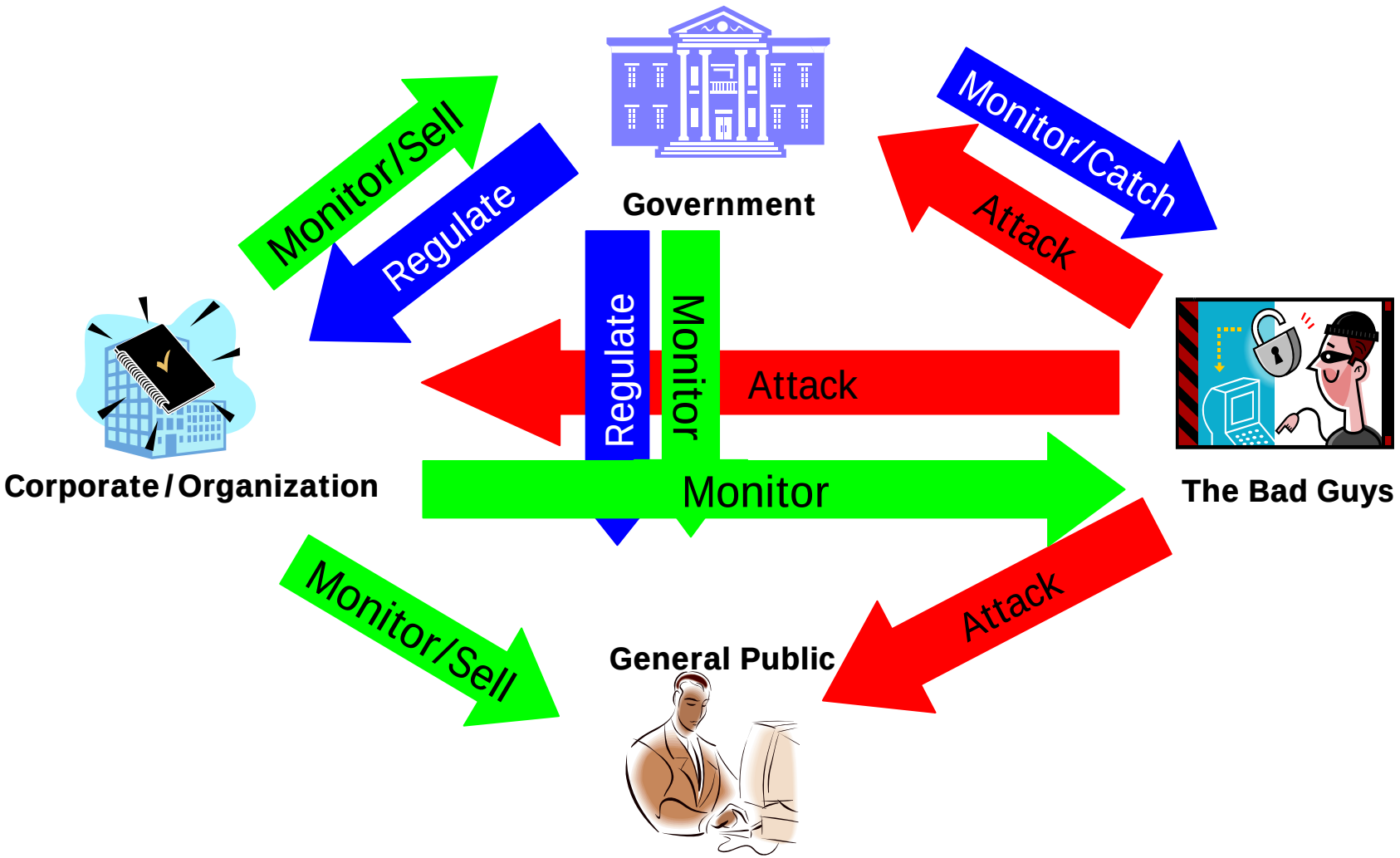
Google Search Trend



Hacking Evolved

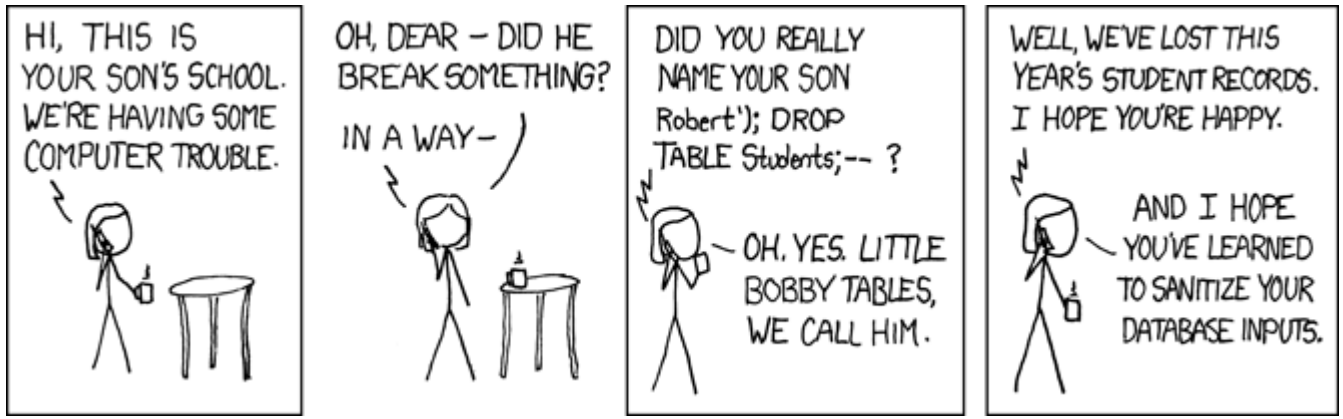


Security EcoSystem



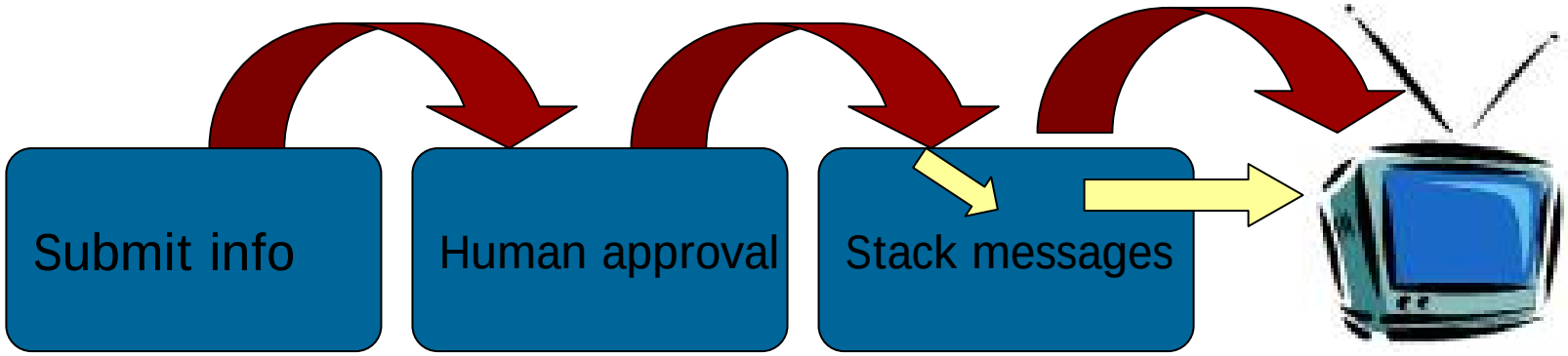
SQL Injection

- RFP (Rain Forest Puppy) identified the problem in Phrack 54 (December 1998)
  - http://www.phrack.org/issues.html?issue=54&id=8#article
- In 2005, Cardsystem lost 40 million credit card info
- In 2008, an automated mass attack of 500,000 (estimated) web servers
  - Yes, using SQL Injection!
- Exploits of a mom (http://xkcd.com/327/):



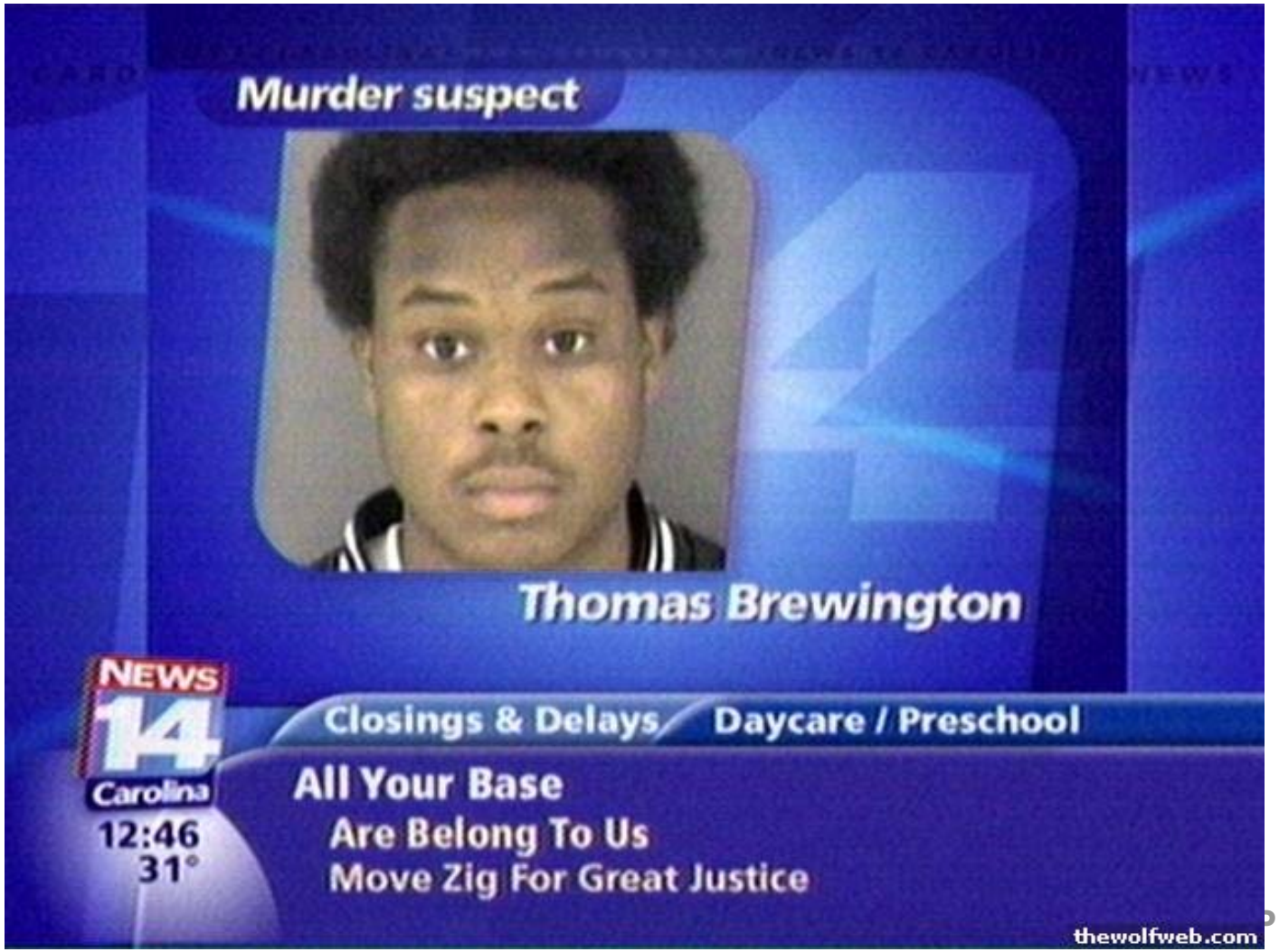
Why You Still Can't Rely on Automated Tools?

- North Carolina News 13
- Web-based "closings" ticker for schools/businesses

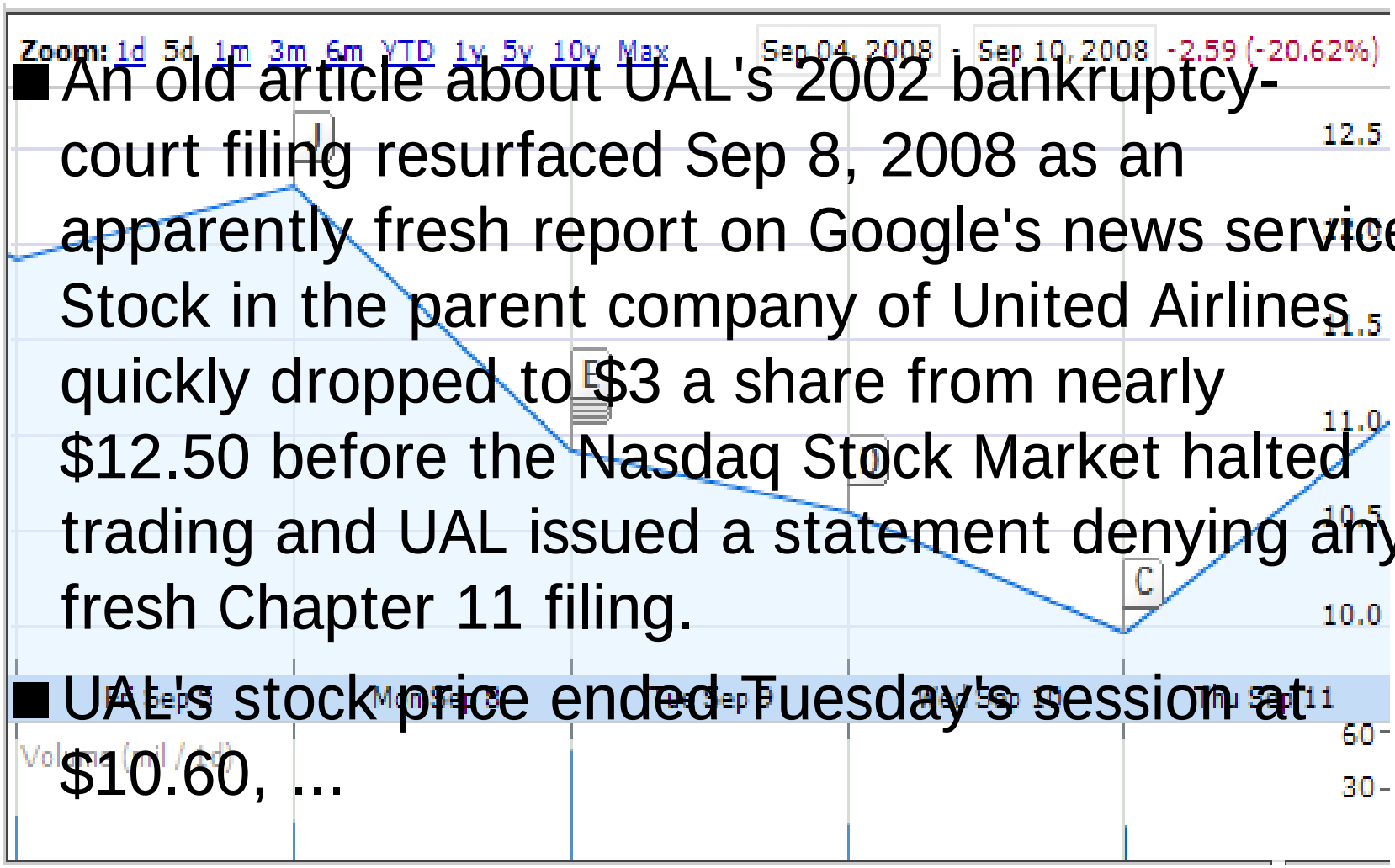


http://tinyurl.com/pwpec

This is What You See...



UAL vs. Google



- An old article about UAL's 2002 bankruptcy-court filing resurfaced Sep 8, 2008 as an apparently fresh report on Google's news service. Stock in the parent company of United Airlines quickly dropped to $3 a share from nearly $12.50 before the Nasdaq Stock Market halted trading and UAL issued a statement denying any fresh Chapter 11 filing.
- UAL's stock price ended Tuesday's session at $10.60, ...

UAL vs. Google

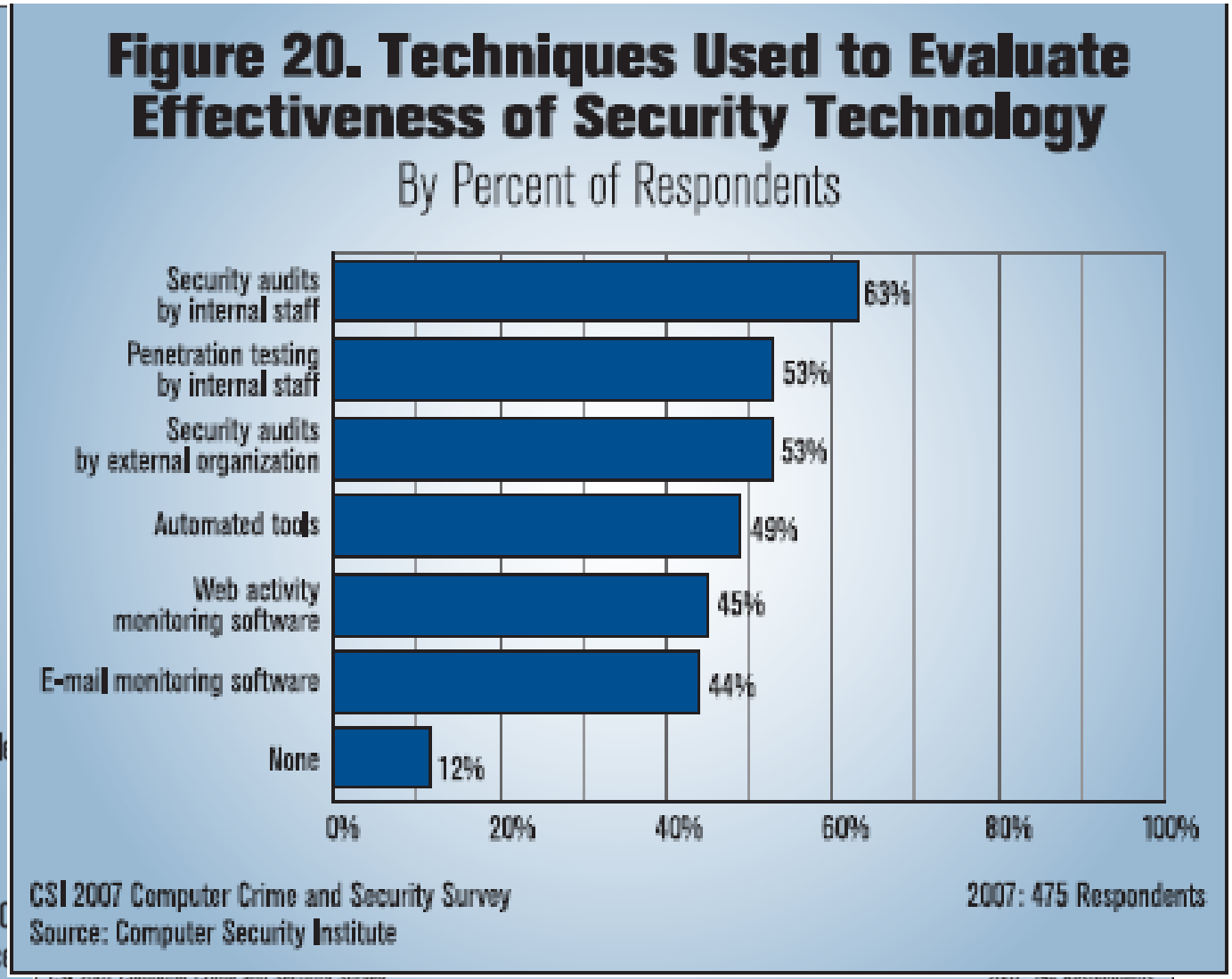
Sep 6, 2008
10:36pm PDT,
A new link to
the UAL story
was found

Sep 8, 2008
UAL stocks
dropped from
$12 to $3

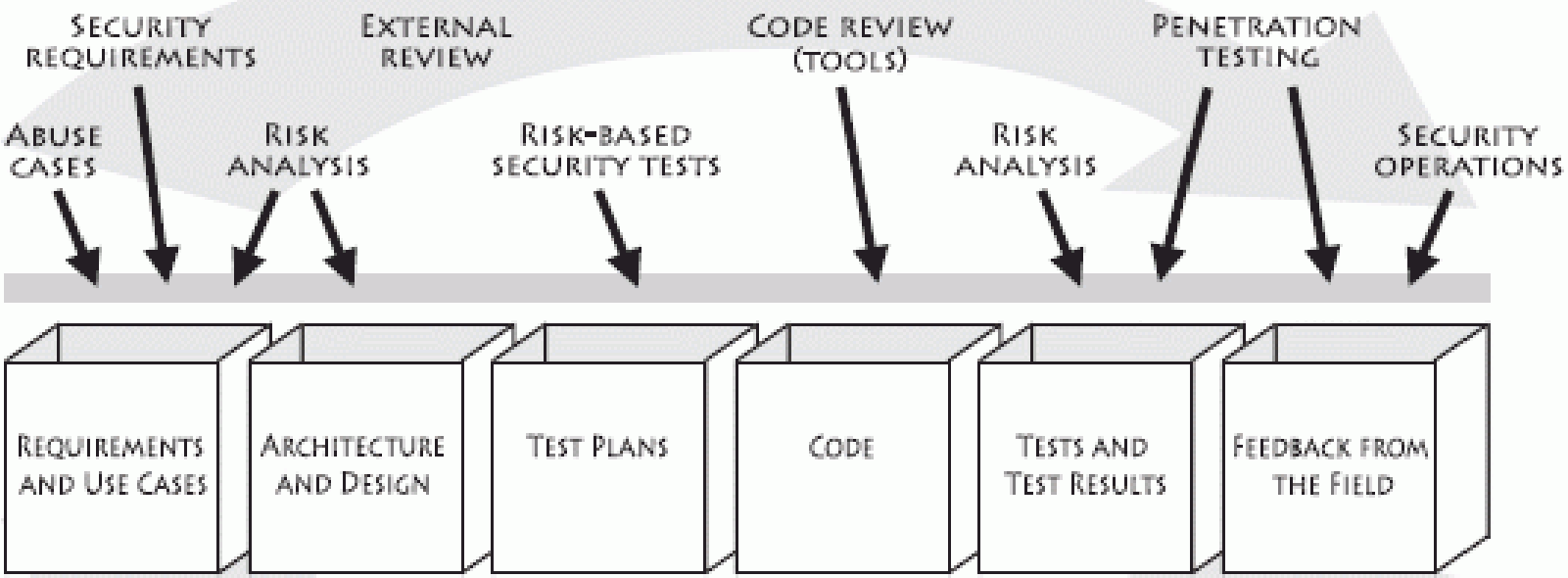
$1.1 Billion market value disappeared in a few hours!!!

Google news
took and
indexed the link

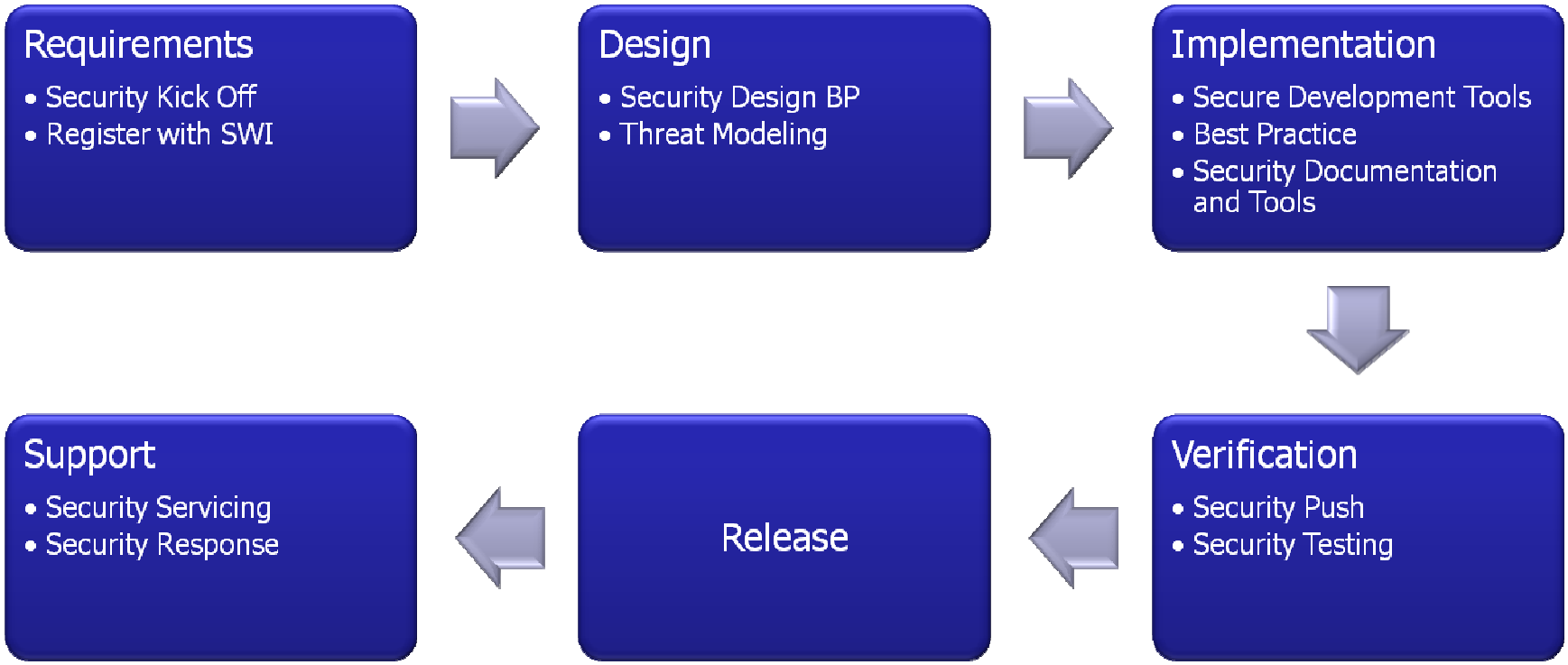
Some Survey Data



McGraw Touchpoint Secure SDLC



Microsoft SDL



Where are things going?

- Penetration testing is still how a lot of companies are going to assess their security
- Frameworks/libraries/etc are going to make shooting yourself in the foot harder (xss, SQLi, etc)
- “Silver Bullet” devices/technologies are always going to be around
- SDL is starting to show proven results


Spongecell
Jyla
kiko
Trumba
eskobo
mayomi
Pageflakes
vimeo
skobee
shadows
groovee
YouTube
Zimbra
LookSmart FURL | Your Personal Web File
smugmug
newsgator
Blogniscient
TiNFINGER
shutterfly
meefeedia
PodDater
Feedster
favoor
Planzo.com
ZAZZLE
Tailrank
TagWorld
nuvvo
dogear
yakalike
grouper
ODDPOST
QOOP
iNods
Lulu
BR
blish
flagr
FireAnt
simplyhired
Veoh
theadcloud
rbloc.com
gather
Agatra
browsr
oyogi
cafepress
Renkoo
pixagogo
standpoint
meebo
EXTRA TASTY!
last-fm
Jotspot
Frappr!
jeteye
dabble
YEDDA
Writeboard
SHOUTWIRE
iKarma
RANOODLE
AirSet
tech.memeorandum
CalendarHub
Suprglu
PIECING YOUR WEB TOGETHER
pando
zigtag
Findory
backfence
clipmarks
wayfaring
gOFFICE
AllPeers
orb
Rallypoint
Zoozio
blogbeat
Ziggs
zoto
vSocial
Boltfolio
wink
riya
Audible Wordcast
Opinity
reddit
measuremap
gumshoo
bluepulse
STREAMLOAD
Ta-da Lists
FeedSky
jellyBam.INC
nativetext
CONGOO
PODZINGER
RSS MAD
FeedTier
phanfare
WIKIPEDIA
Fruitcast
PubSub
dPolls
flickr
Ning
Ookles
Strongspace
zoominfo
CASTPOST
yubnub
AC
BLOOP
ProjectSpaces
FeedBurner
Bloglines
purevolume.com
FOTOLOG
ourmedia
gabbr.com
Gcast
blinkx
openomy
riffs
ajchat
Yub.com
Spot Runner
myspace
NewsAlloy
Allmydata.com
chatsum
PANDORA
looklater
jambo
ROLLYO
ClipShack
PROTOPAGE
squishr
WebJay
PLAZES
Noodly
30 BETA
wondir
diigo
box
Jots
Xdrive
vizu
digg
del.icio.us
omni drive
AlmondRocks
Tagyu
30GIGS
writely
Simpy
Gtalkr
TRUVEO
egoSurf
mozy
Quimble
pegasus
remember the milk
SQUIDOO
picturecloud
newsvine
Clipfire
Basecamp
Netvibes
gooey
My Videokaraoke
Lexxe alpha
powered by advanced natural language technology
OOKSTER
PXN8
measuremap
facebook
43 Things
Technorati
Platial
Backpack
Gmail
yelp
Smarkets
inform
filangy
magnolia
ShoZu
wrichr.com
feedmarker
mercora MusicSearch
Meet With Approval.com
HOMEPORTALS
Spin spy (beta)

What's Next?

- Security research is chasing after new technologies
  - New vulns on different products will happen daily
  - Better accuracies from security products
  - Slower to see new paradigm shift
- Integrate security into your daily life
  - Corporate M&A
  - Need better management on execution
  - New technologies to make it harder to make unsecure web applications
- Learn from other fields
  - Knowledge Discovery, Data Mining & Information Retrieval
  - Biology, Physics, Social Science and others

Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight

WEB APPLICATION SECURITY

2007-2008 Analysis

- Collected 77 Applications in 5 industries
- Picked 27 out of them and did further study
- Arranged findings based on
  - Foundstone Security Framework,
  - Overall risk level and
  - Root cause in SDLC phases

Foundstone Security Framework

Configuration Management

- Secure deployment and hardening. Issues will include default deployment settings and administrative access

Data Protection

- Handling of sensitive data as it is at rest in files and databases or as it is transmitted across the network

Authentication & Authorization

- Access to protected resources and kinds of controls on such access. How identities are verified.

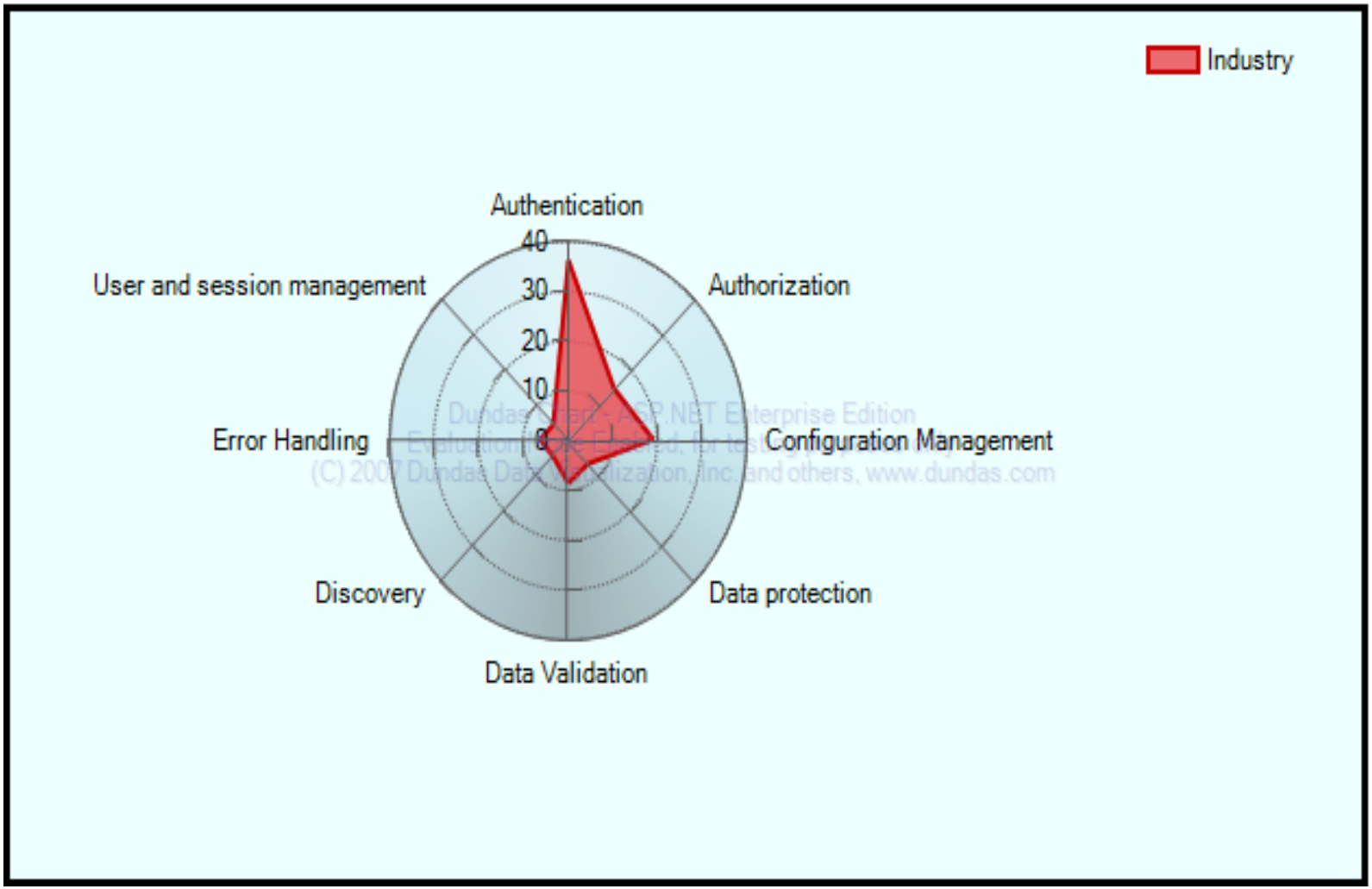
Logging & Auditing

- What information is logged and where it is logged. Can information act as audit trail?

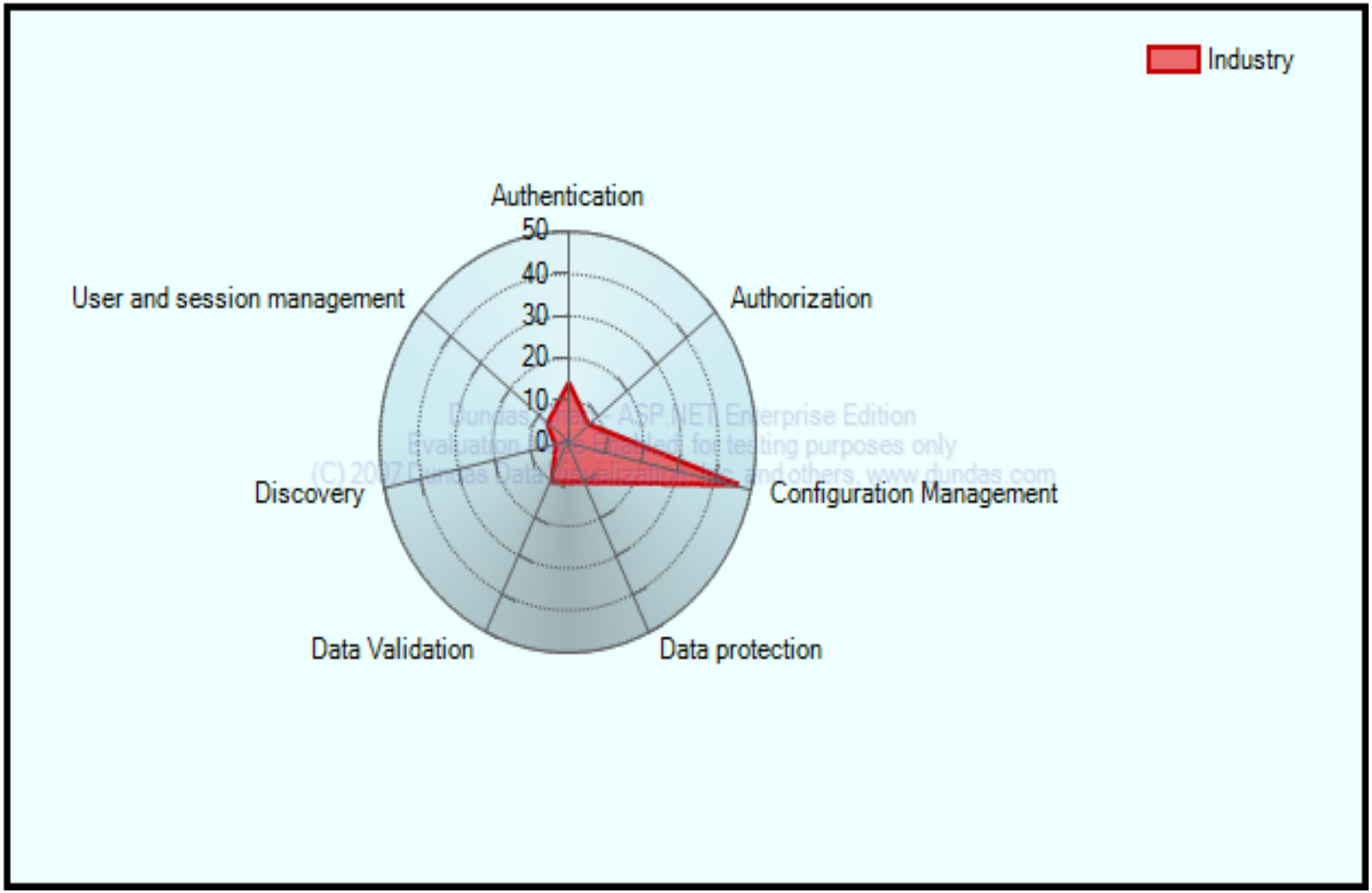
Data Validation and Exception Management

- How the application performed data validation on both input and output and how exceptions are being handled without information leakage

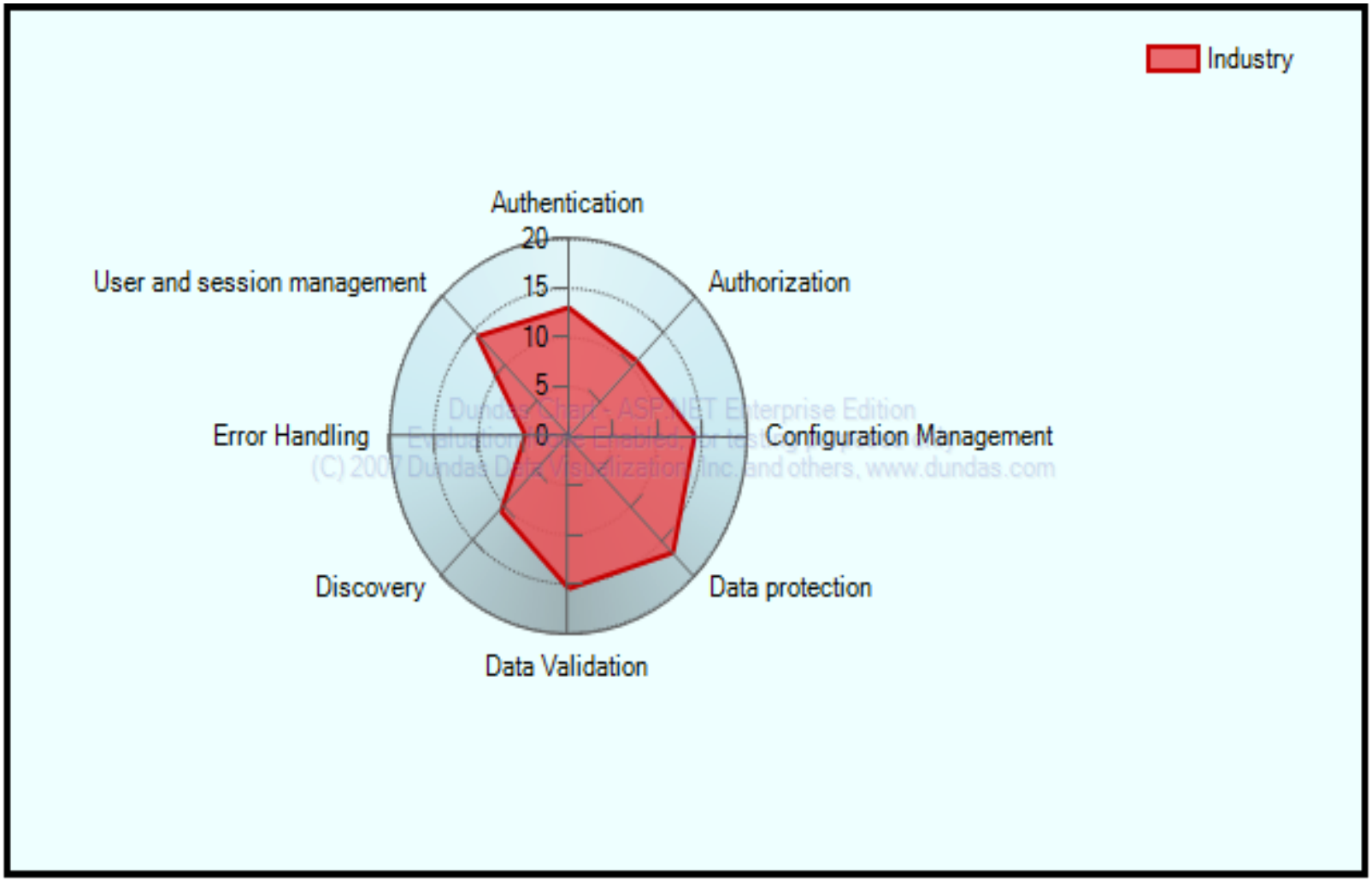
Financial Services – 15 Apps



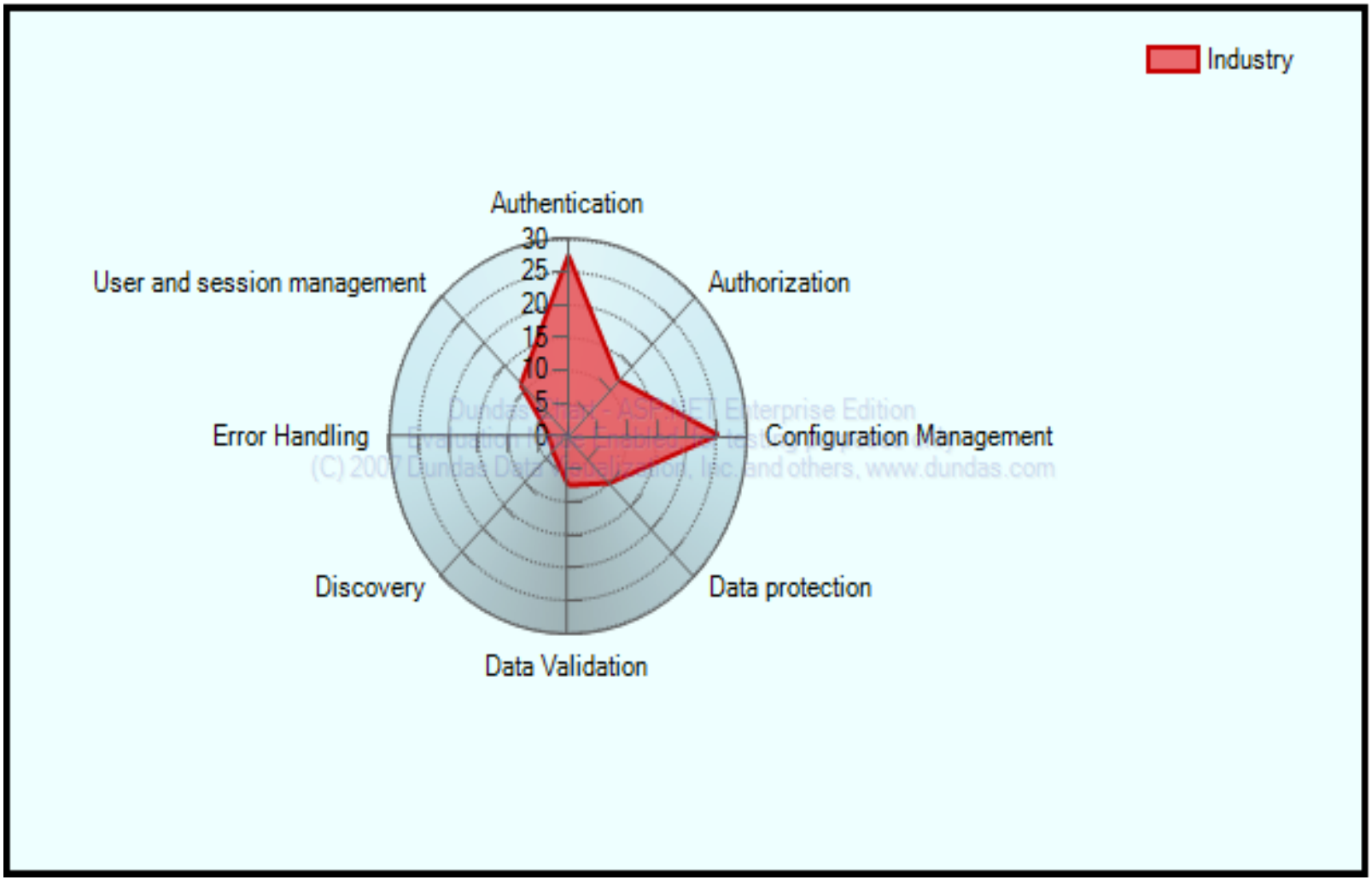
Healthcare – 12 Apps



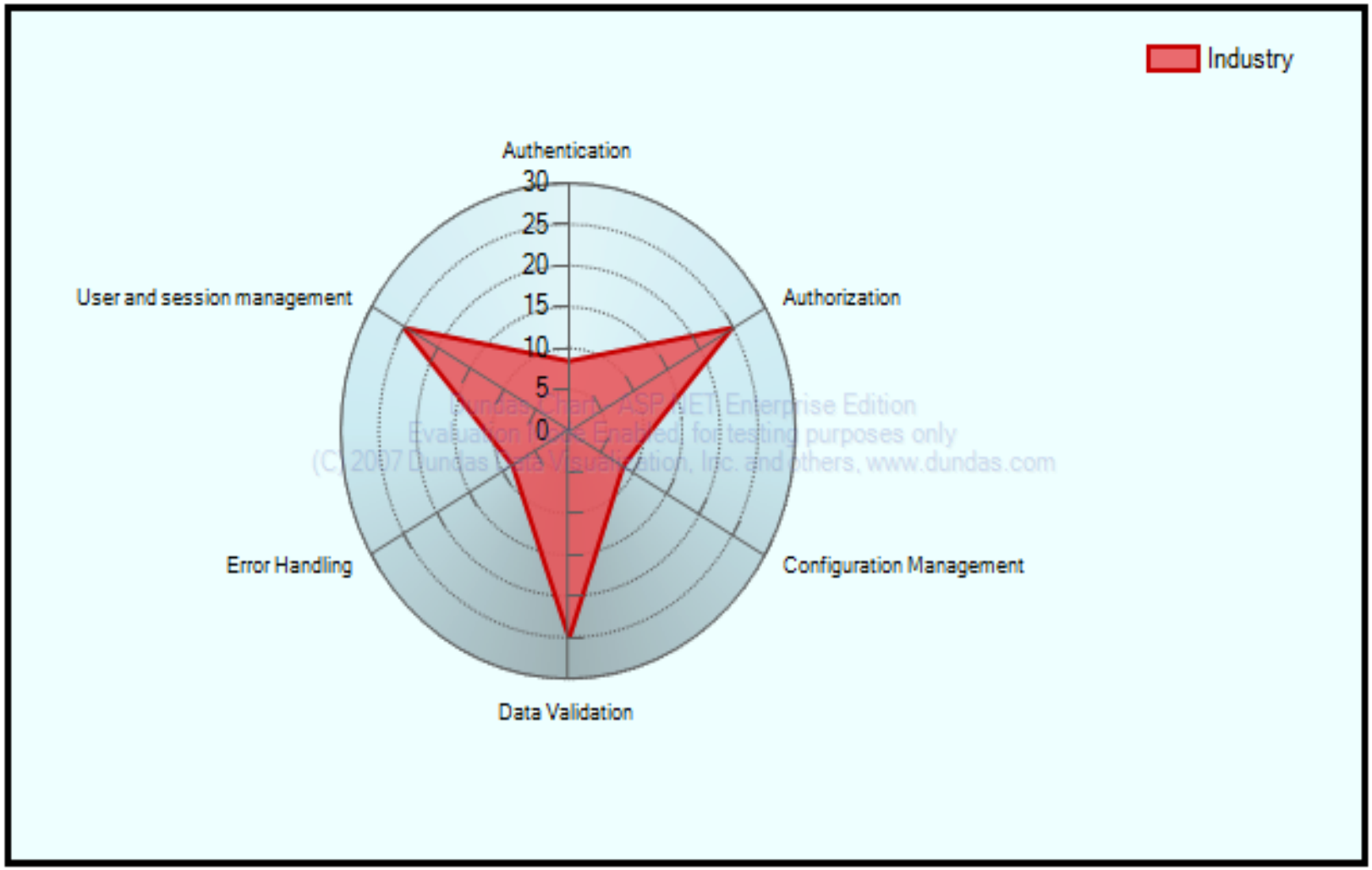
Insurance – 27 Apps



Retail – 17 Apps



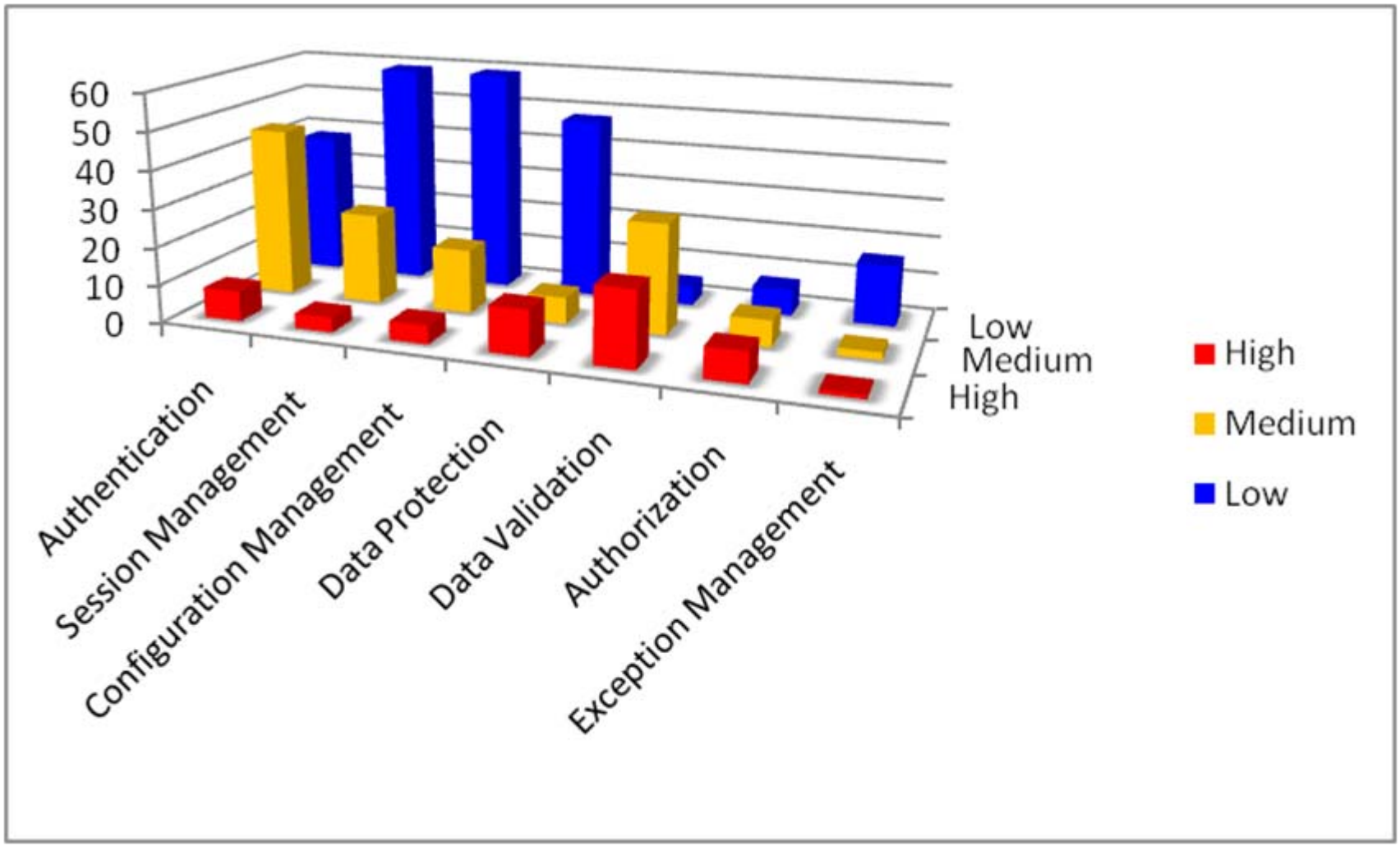
Utility – 6 Apps



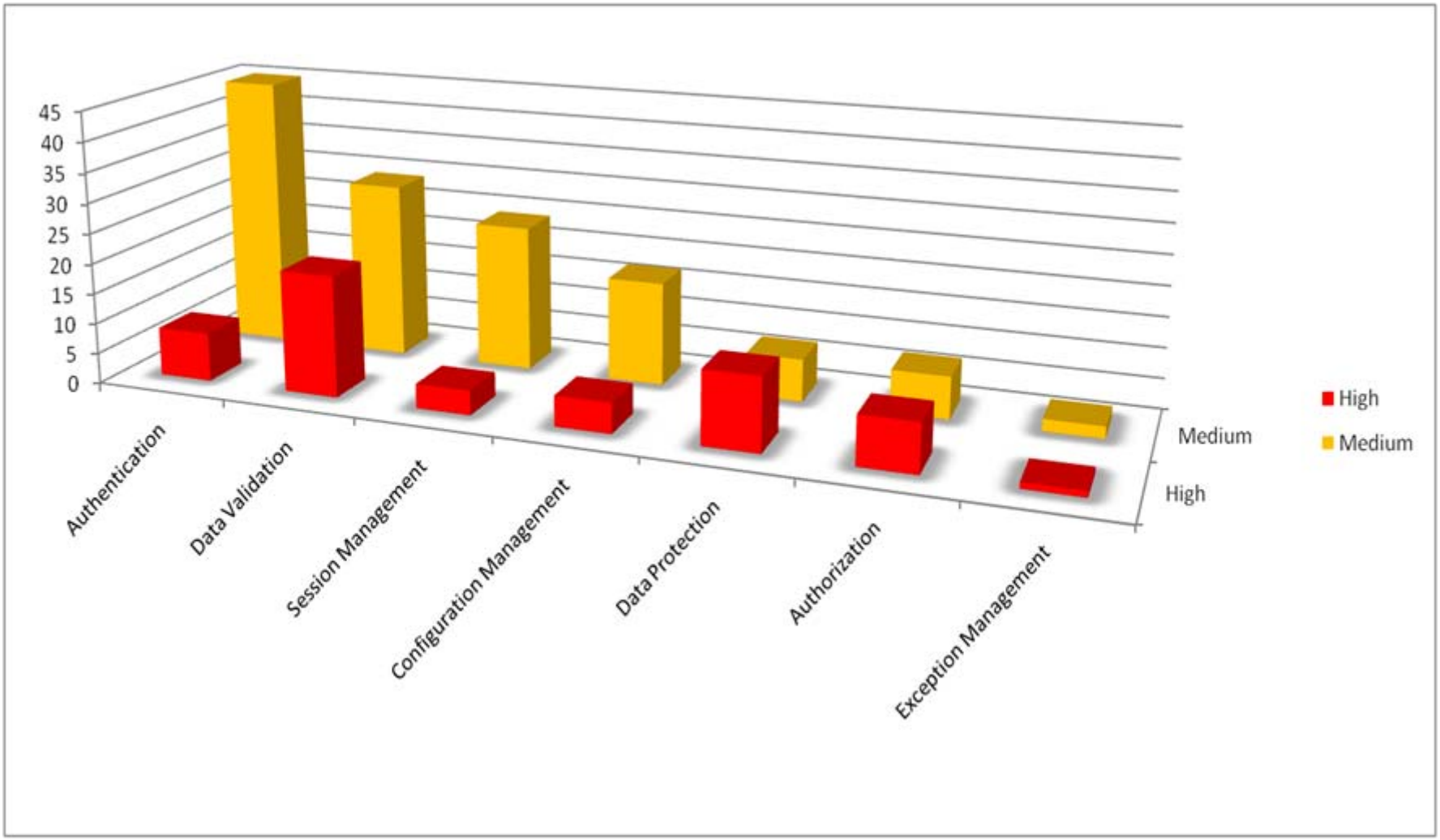
27 Applications

- 13 on Unix; 13 on Windows; 1 on Novell
- Total 421 findings

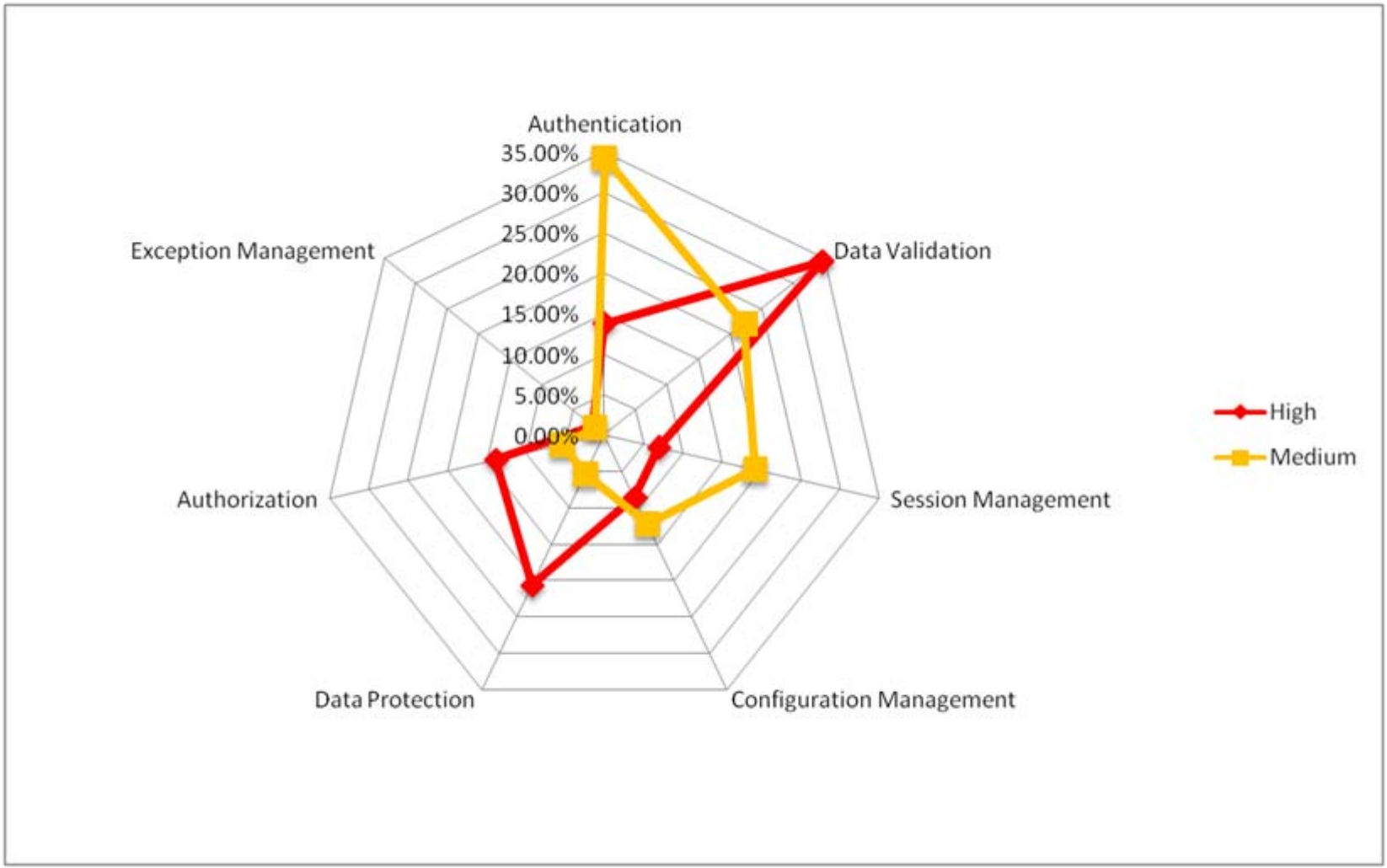
Findings by Framework and Risk Level



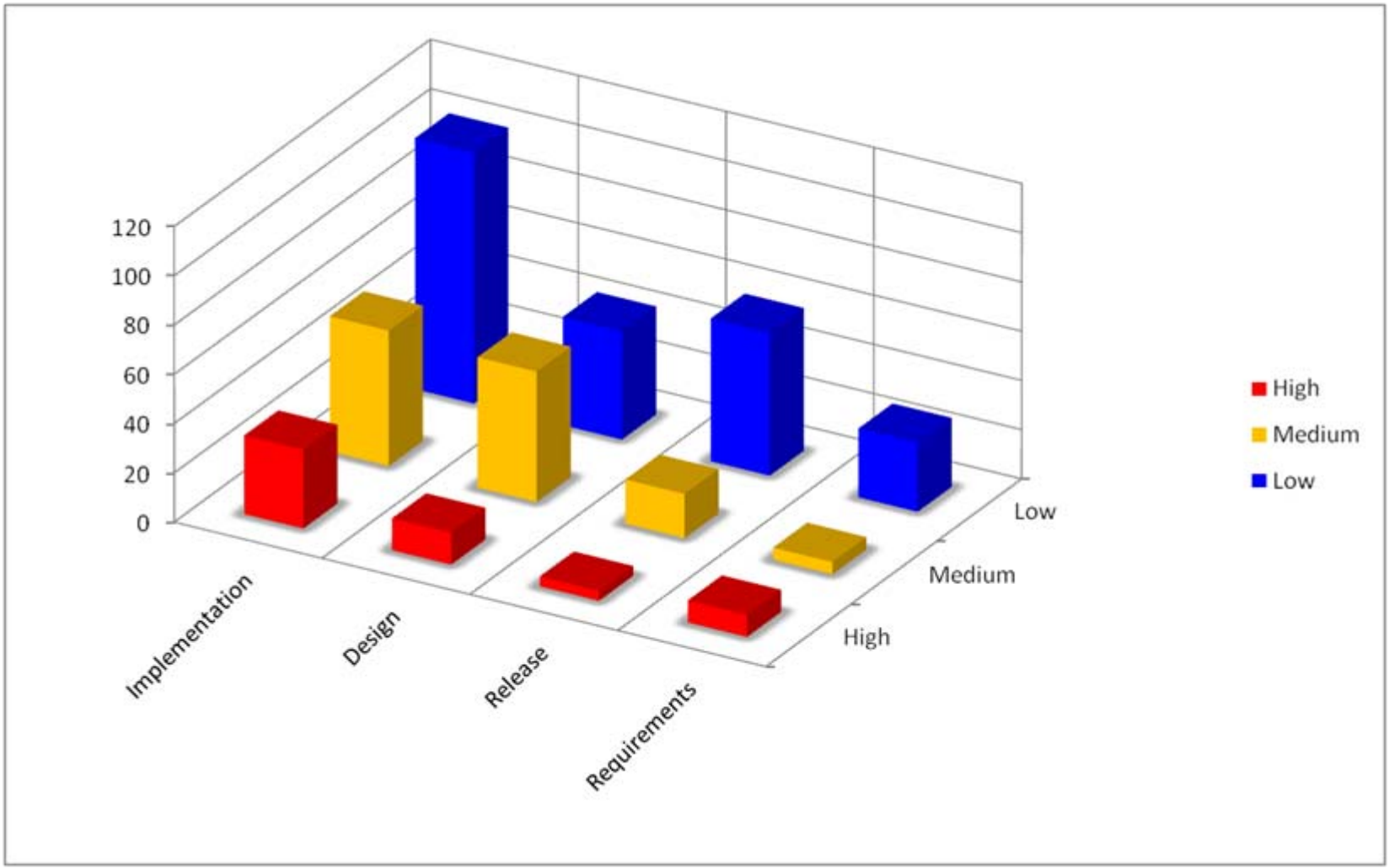
High and Medium Risk Findings



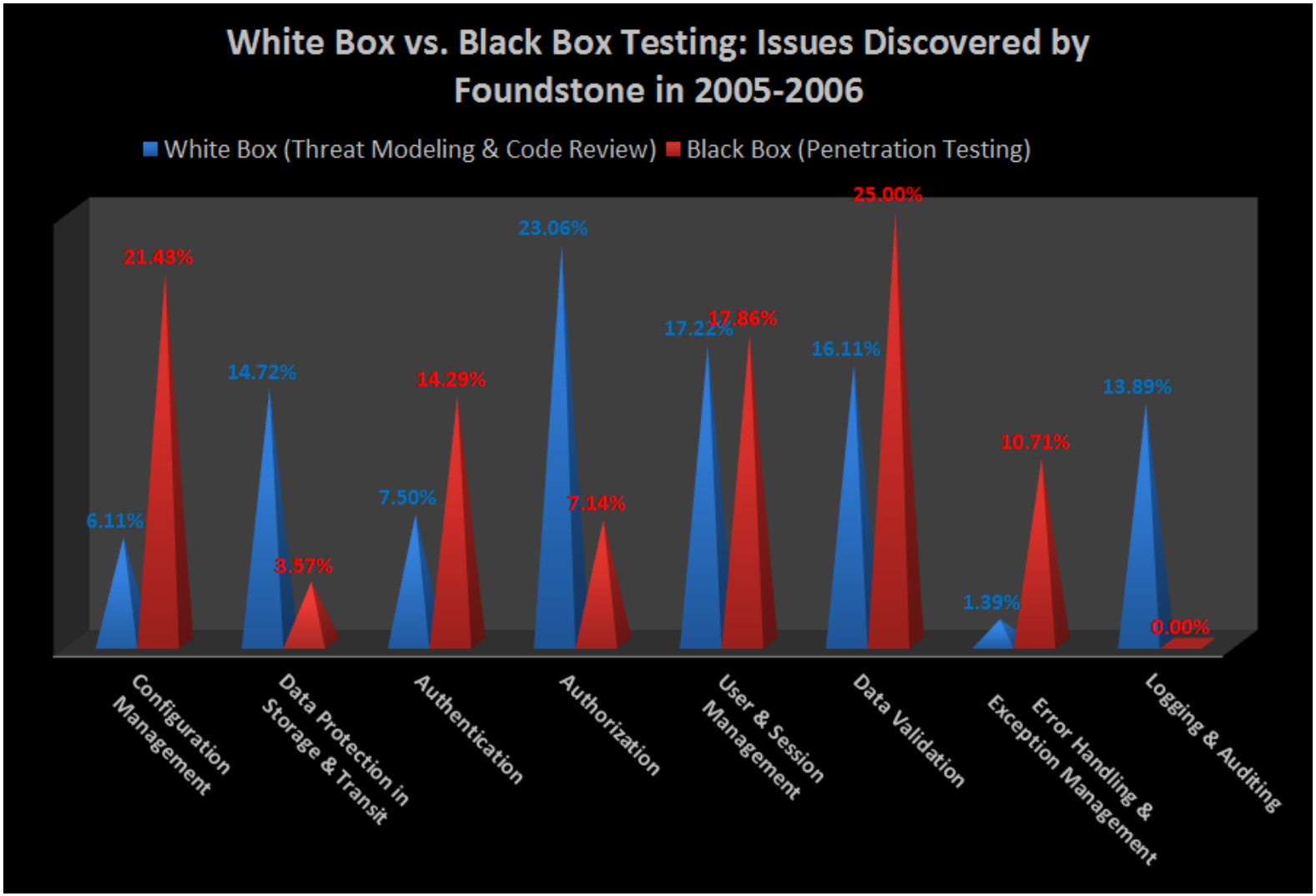
Findings by Percentage



Findings by SDLC Phases



White Box vs. Black Box



10 Things To Secure Your Web App

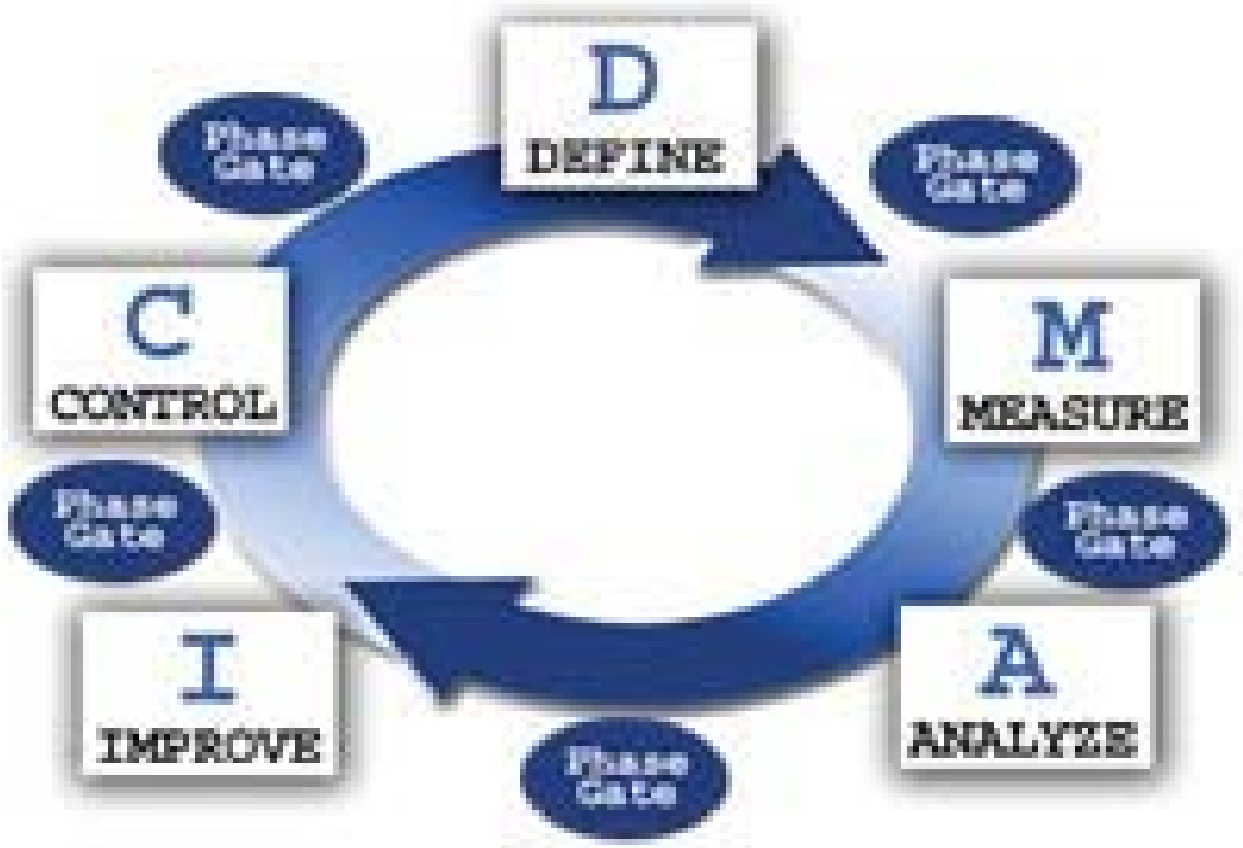
- Authentication
  - Password policy
    - Reset password function, history, complexity and account lockout
- Authorization
  - Role/privilege mapping and enforcement
  - Workflow/business logic authorization enforcement
- Data Validation
  - Do your validation on the server-side both on output and input!
- Session Management
  - Use random session ID and maintain the state on server-side. Do not depend on any state information on the client
- Data Protection
  - Protect your important data in storage and transit
  - Choose your data protection solution wisely
- Configuration Management
  - Secure server configuration and patch it well!
- Exception Management
  - Handle all exception and return generic error messages
- Logging and Auditing
  - What to log and how/when to audit?

If you know the enemy and know yourself, you need not fear the result of a hundred battles

STRATEGIC PLANNING

Six Sigma Tactical Steps

- Define
- Measure
- Analyze
- Improve
- Control

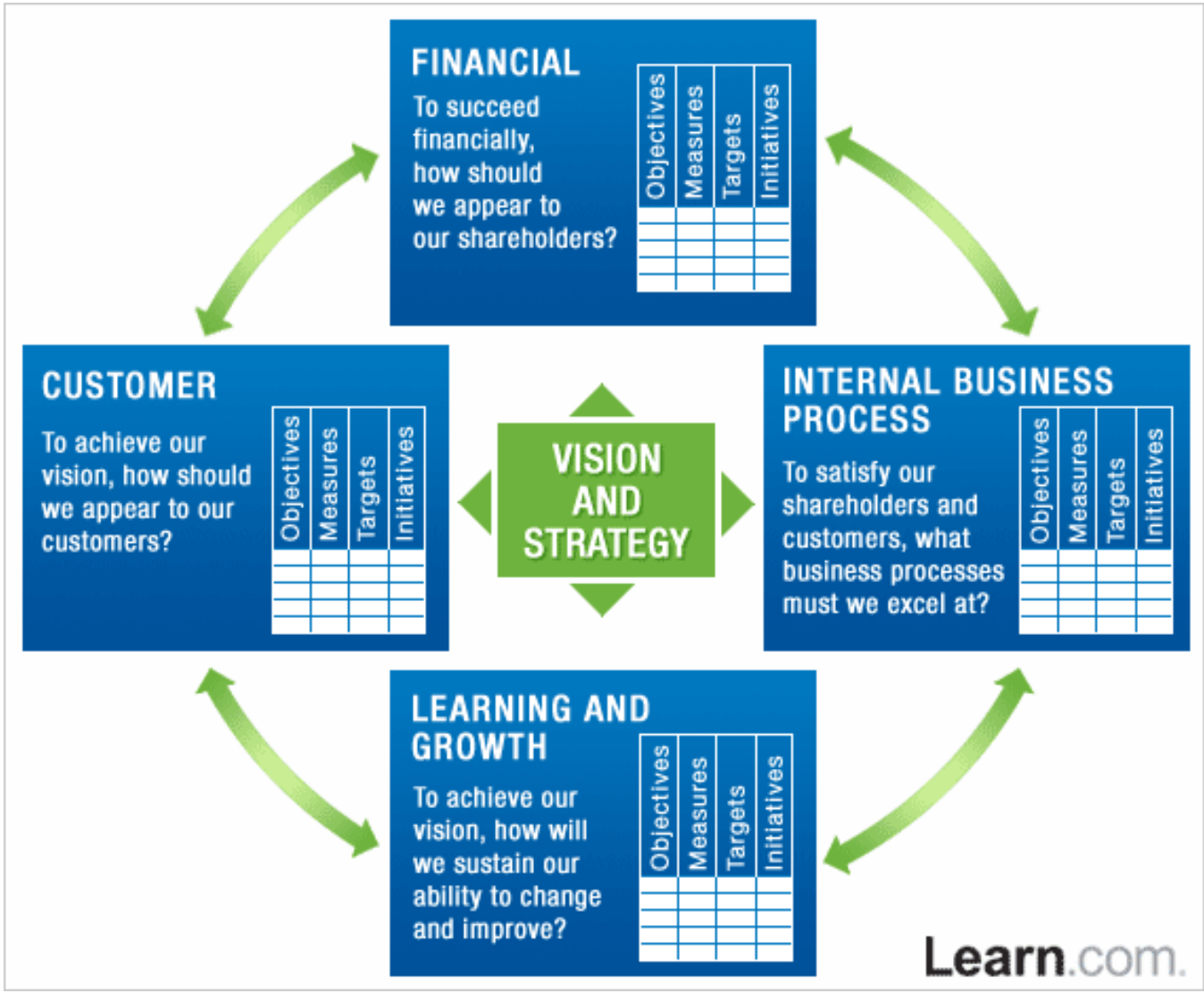


What is Process Sigma?

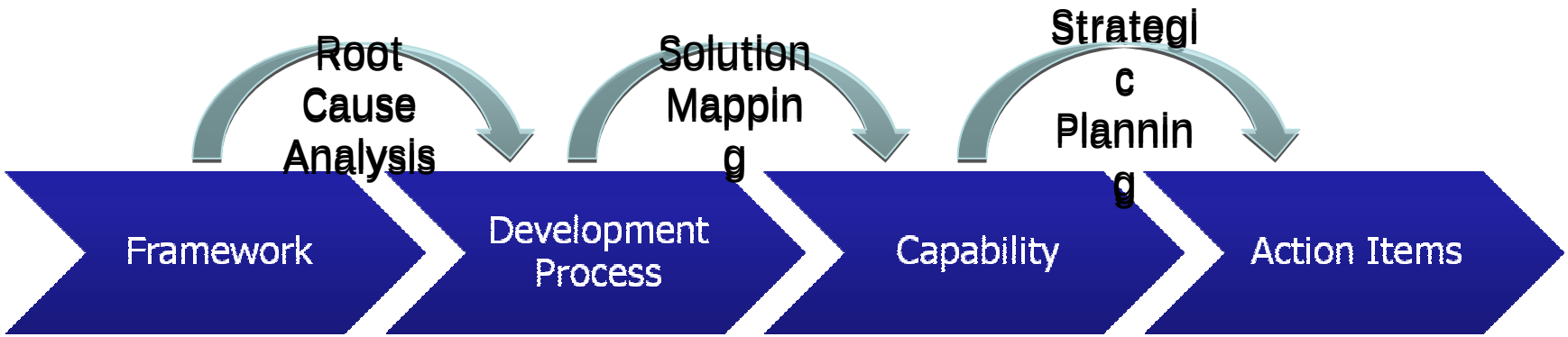
- Defects per Unit and Opportunities
- 3.4 defects per 1 million opportunities is Six Sigma

$$\frac{\text{Number of Defects}}{\text{Number of units} \times \text{Number of opps.}} \times 1{,}000{,}000$$

Balanced Scorecard



Methodology



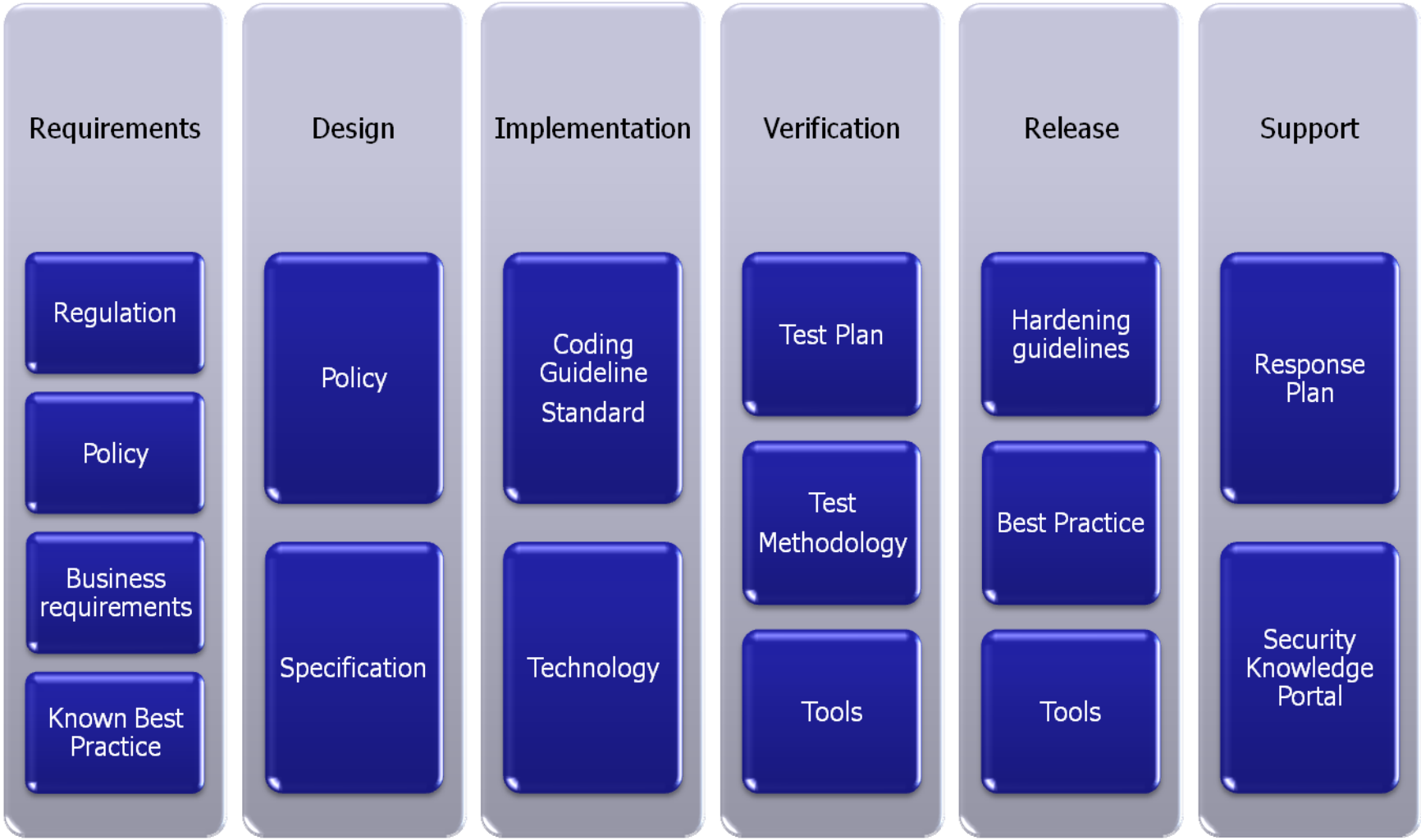
- Authentication & Authorization
- Data Validation & Exception Management
- Data Protection
- Logging and Auditing

- Requirements
- Design
- Implementation
- Verification
- Release
- Support

- People
- Process
- Technology

- Objectives
- Measurements
- Targets
- Initiatives

Solution


Requirements
Regulation
Policy
Business requirements
Known Best Practice
Design
Policy
Specification
Implementation
Coding Guideline
Standard
Technology
Verification
Test Plan
Test Methodology
Tools
Release
Hardening guidelines
Best Practice
Tools
Support
Response Plan
Security Knowledge Portal

Capability

People	Process	Technology
• Organization • Training • Budget	• Policy • Guidelines • Standards • Best Practices • Methodology • Response	• Tools • Knowledge Repository

Action Items

- Create/enhance secure coding standard
- Train developers to do threat modeling
- Improve security quality from customer's perspective

- Number of implementation bugs
- Number of threats identified
- Number of maintenance patches per month

- Maintain six sigma
- Every developer should be able to perform 1 TM/year
- Reduce to 2 per month

- Improve current coding guideline/standard
- Computer based training
- Security knowledge management

In order to carry out an attack, we must have means available

CONCLUSION

Summary

- We reviewed:
  - Current security status
  - Web application security statistics
  - Strategic planning to keep your web application secure
- Security is an on-going process that also requires people and technology to play important roles.

No Silver Bullets or Easy Button!

If Toyota Builds Your Web Applications…

- Modularization, Automation and Just-In-Time
- Reduce cost, maintain highest customer satisfaction
- Implementation phase will be automated and modularized
- Developers won't be able to use any insecure implementation techniques
- Web applications will be stick to the known best practice with high quality in security. When there is a serious flaw there will be a recall.

Thank You

Yen-Ming Chen
Director of Consulting,
Foundstone, A Division of McAfee
Yen-ming.chen@foundstone.com

OWASP