

The logo features the word "FORRESTER" in a white, serif, all-caps font, centered within a dark green oval. The oval is set against a dark blue background with subtle, curved, lighter blue lines radiating from the left side.

FORRESTER®

# Web 2.0, Consumerization, and Application Security

**Chenxi Wang, Ph.D.**

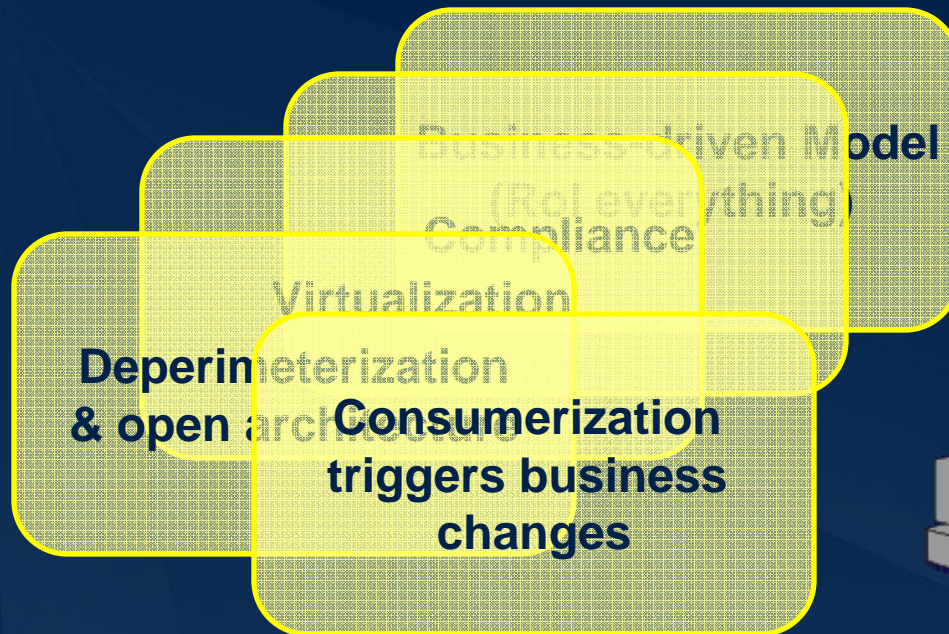
Principal Analyst

Forrester Research

OWASP, New York City

September 25, 2008

# Today's enterprises face multitude of challenges

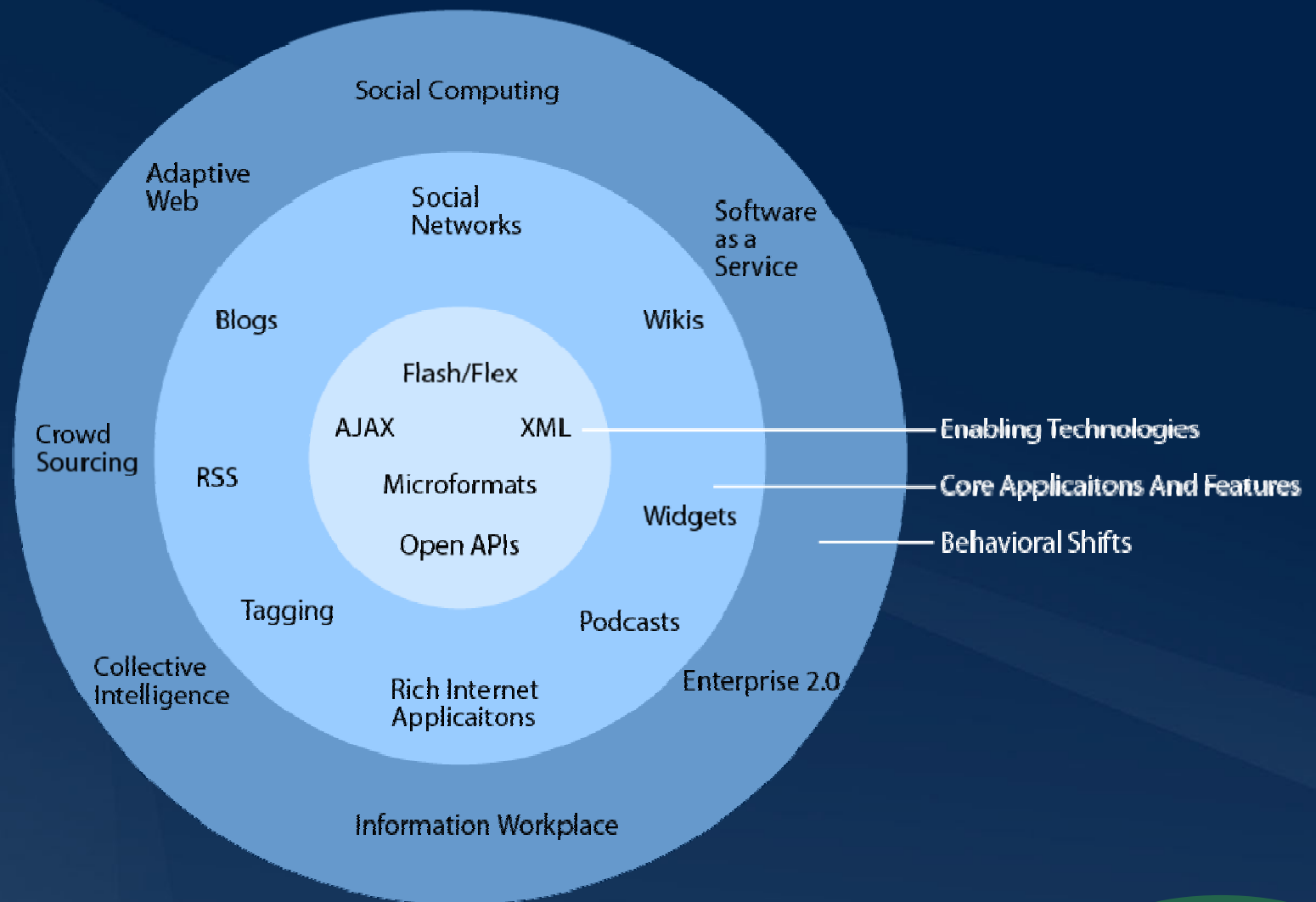


# Consumerization

- Is at the forefront of innovation
- Fosters new business models
- Promotes new social structures
- have become part of enterprise fabric



# Three Lenses to View Consumerization



# Consumer technologies foster new business

## Example: Random House book widget

- Provides top-selling books in your ZIP code
- New viral distribution channel
- Creates new business opportunities



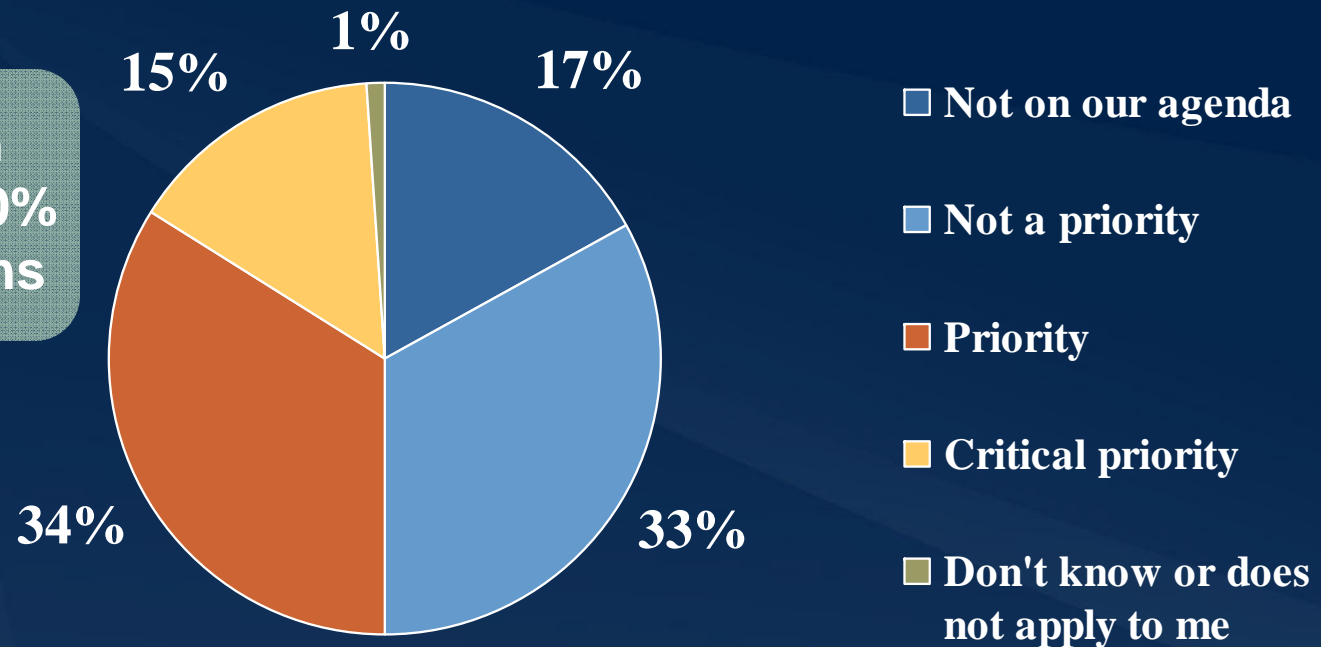


# Collaboration is part of enterprise strategy

“Which of the following are likely to be one of your IT organization’s major software technology initiatives for the next 12 months?”

Implement an enterprise collaboration strategy

Collaboration  
Is priority for 50%  
of organizations



Near 50% of businesses view it as a priority

Base: 2,252 Software IT decision-makers at North American and European companies  
Source: Forrester Enterprise And SMB Software Survey, Q3, 2007

# Many are building serious applications on top of consumer technologies



- Crew portal (mission-critical app)
- Compliance documentation management



- AMD Central intranet
- Global partner sites (mission-critical)



- “Trusted workplace” for multi-company collaboration
- Sharing of critical design documents (airplane design docs, CAD drawings)



# This is how a distributed team could work . . .



# This is how a distributed team could work . . .



# Perhaps this is what happens . . .

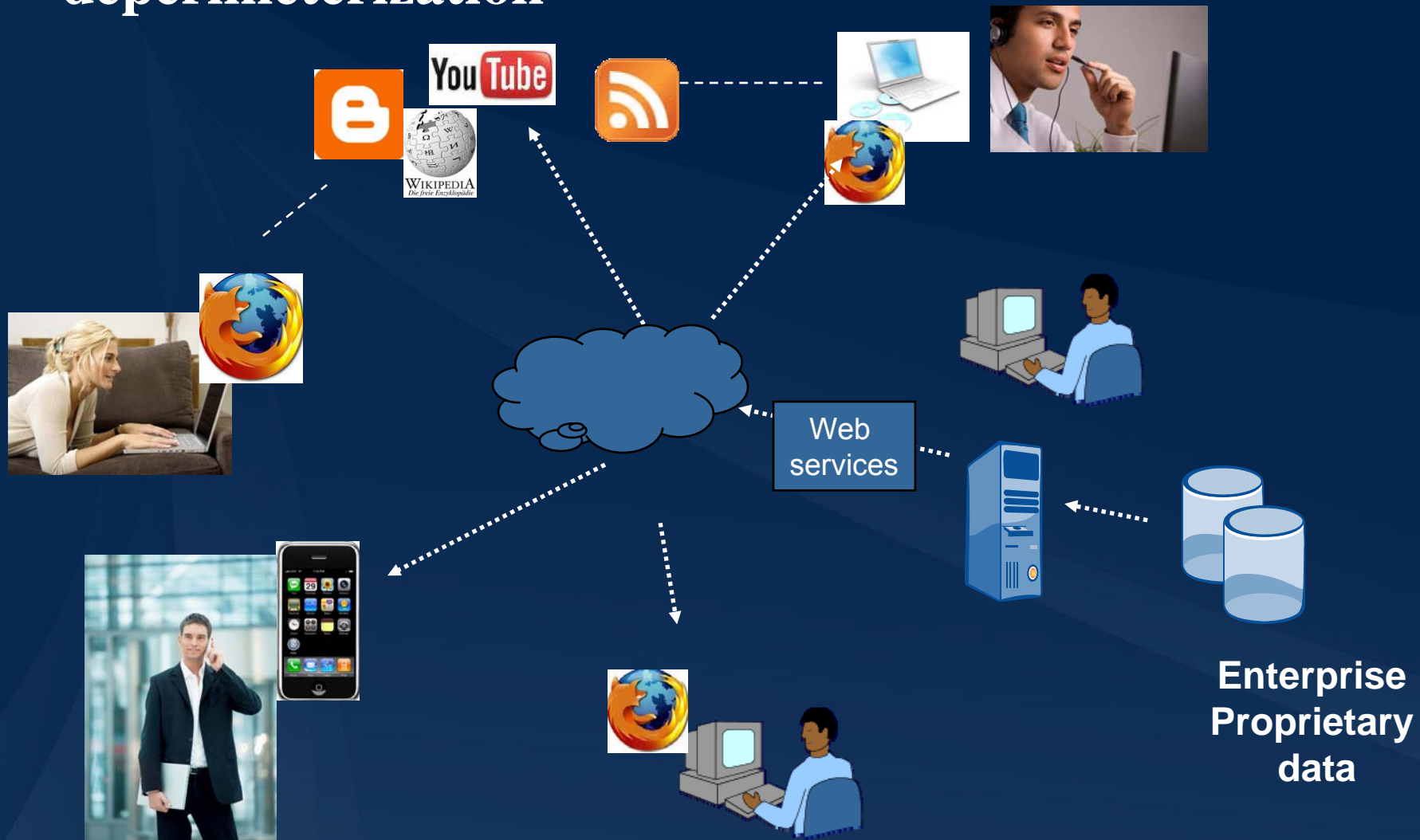
The screenshot shows the iGoogle homepage with the following elements:

- Top Bar:** iGoogle logo, search bar, "Google Search" and "I'm Feeling Lucky" buttons, and links for "Advanced Search", "Search Preferences", and "Language Tools".
- Navigation:** "Make iGoogle your homepage? [Yes, please](#) | [Not now](#)" and "Add a tab" button.
- Left Sidebar:**
  - Wikipedia:** Search bar with "Wen" entered, "Go" and "Search" buttons.
  - Mountain View Voice:** Links to "Google hotel falls through", "Gabby drivers take note", and "Strikers at BMW returning to the table".
  - My calendar** (button)
  - Team blog RSS reader** (button)
  - Corporate Siebel** (button)
- Center:** **Mountain View Map** widget showing a map of Mountain View, CA, with street names like "Central Expy" and "Cuesta Dr".
- Right Sidebar:**
  - Weather:** "Mountain View, CA", 60°F, "Current: Clear", "Wind: N at 0 mph", "Humidity: 62%". Forecast for Today (72° | 52°), Wed (74° | 54°), Thu (77° | 56°), and Fri (86° | 66°).
  - Movies:** "Showtimes for 94043 »", "Get Smart" (1hr 50min, Rated PG-13, 2 reviews), "The Love Guru" (1hr 28min, Rated PG-13, 2 reviews), "The Happening" (1hr 31min, Rated R, 18 reviews).
  - Gmail:** "Inbox (2310)", "Hide preview", "Compose Mail".

# Consumerization accentuates every aspect of deperimeterization



# Consumerization accentuates every aspect of deperimeterization





# But, organizations are wary of consumer technologies

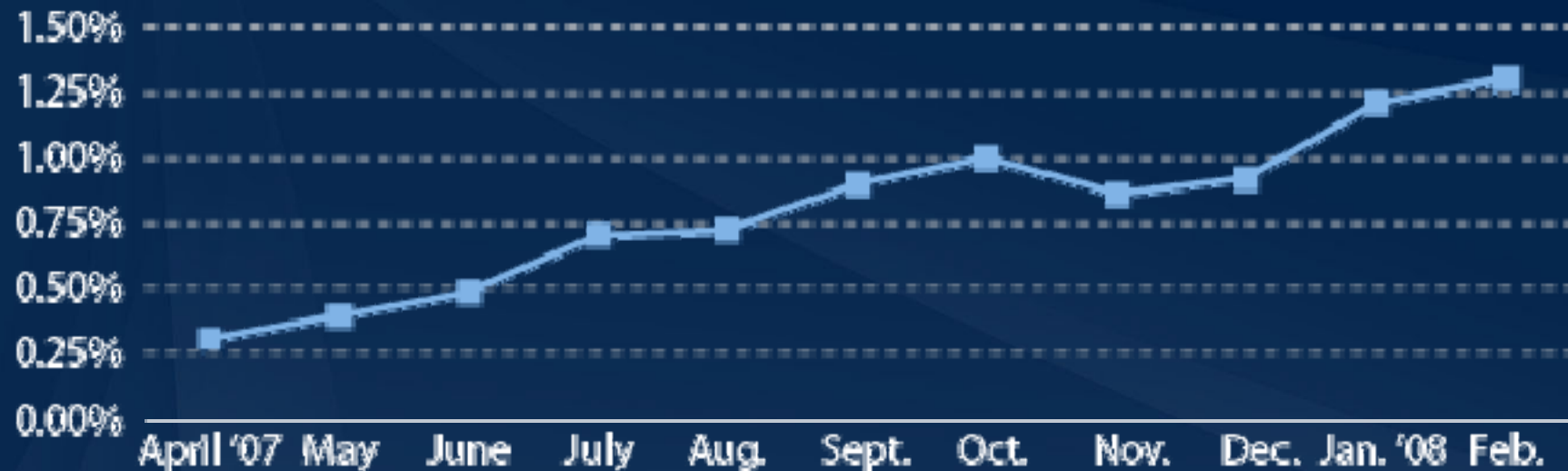
- Greater number of security risks
  - » Attackers are targeting collaboration and Web 2.0 applications.
  - » Staying ahead of all the issues is difficult.
- Increased complexity of IT operations and management
- Further dilution of the enterprise boundary





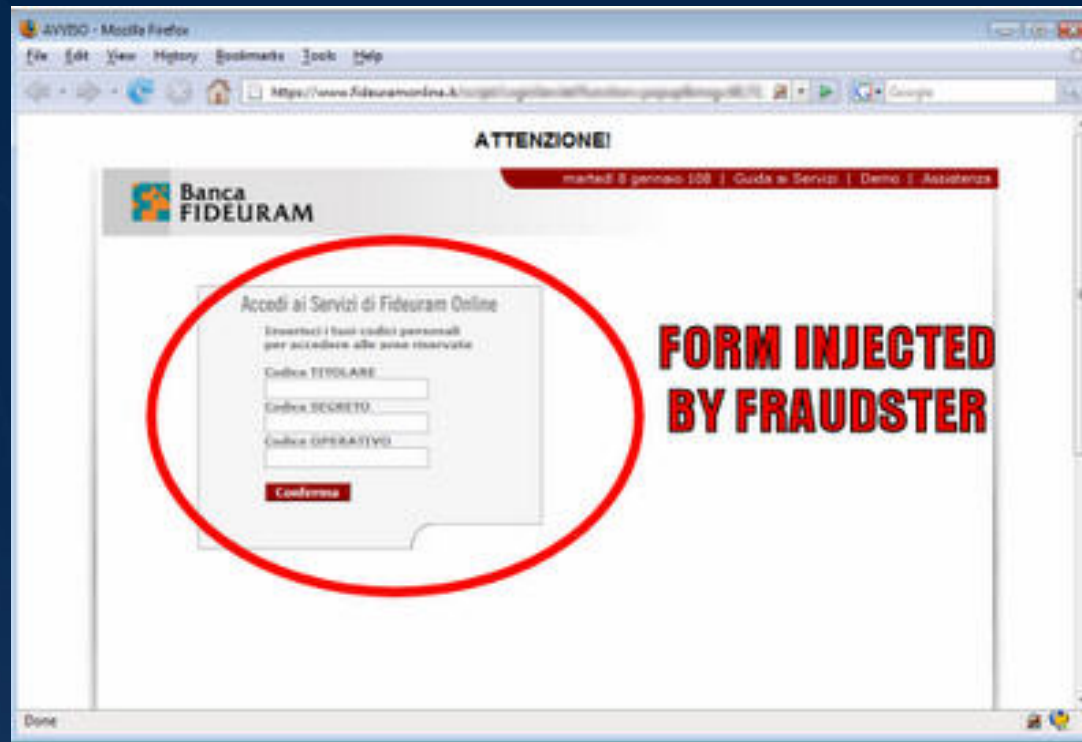
# Web 2.0 Security risks

# Internet is becoming more dangerous . . .



Source: "All Your iFRAMES Point to Us," Google, February 4, 2008

# Innocent participants in malware infection chain



- Fraudsters exploited a XSS vulnerability to inject a modified login form onto Banca Fideuram's Web page
- User's account info is sent to a server in Taiwan

# Data theft is rampant ...

**Low**      **High**

\$2	\$5
\$25	\$35
\$200	\$300
\$25,000	\$40,000

Payment card

Magnetic stripe data

Full account information

Zero-day malware

eBay, PayPal  
accounts

Driver's licenses

Birth certificates

Other items for sale

Source: The Aegenis group, USENIX 2008

FORRESTER®

# Web 2.0 highlights application security

- Increased attack surface
  - » Client side state matters
  - » Code injection is a top security risk
- Developing secure web 2.0 apps is challenging
  - » Security testing is more complex
  - » Authentication/Authorization logic is more complex
- Traditional trust model is broken



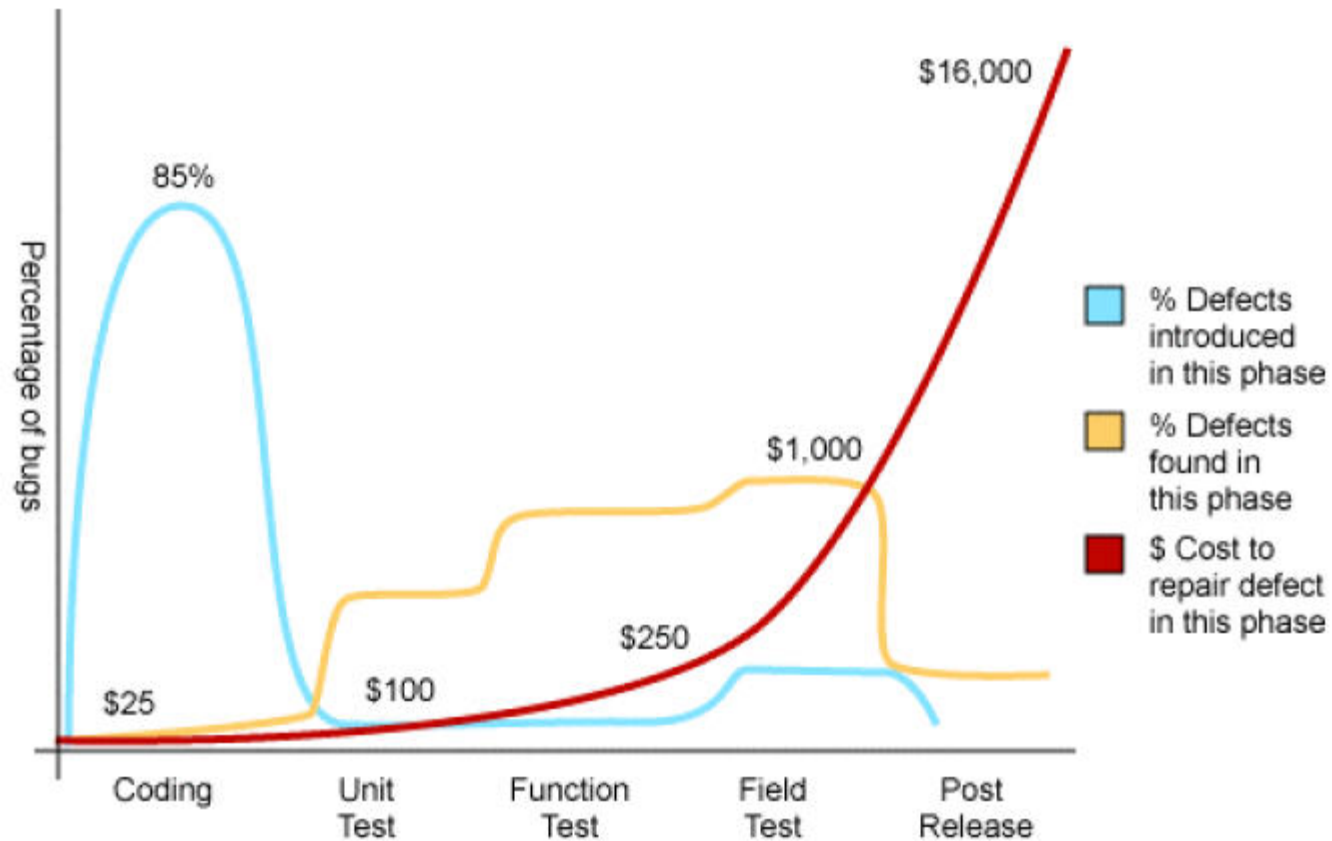
A person in a dark climbing suit is seen from behind, standing on a snow-covered mountain peak. The sky is a deep blue with wispy white clouds. The foreground is filled with textured snow and ice.

**Security has to be baked in  
rather than painted on ...**



# Why Security during development?

85% of code flaws are introduced during coding

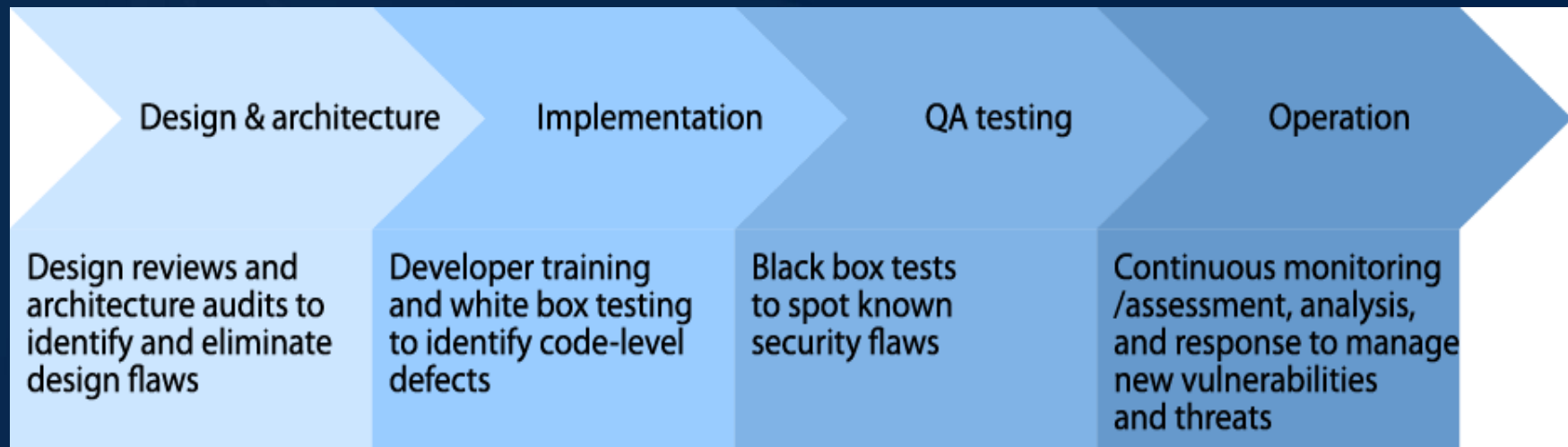


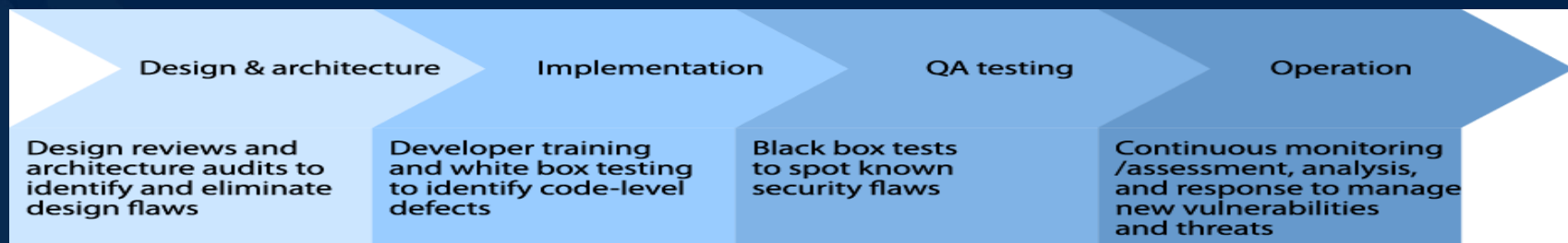
Source: *Applied Software Measurement*, Capers Jones, 1996

## Why security during development - recap

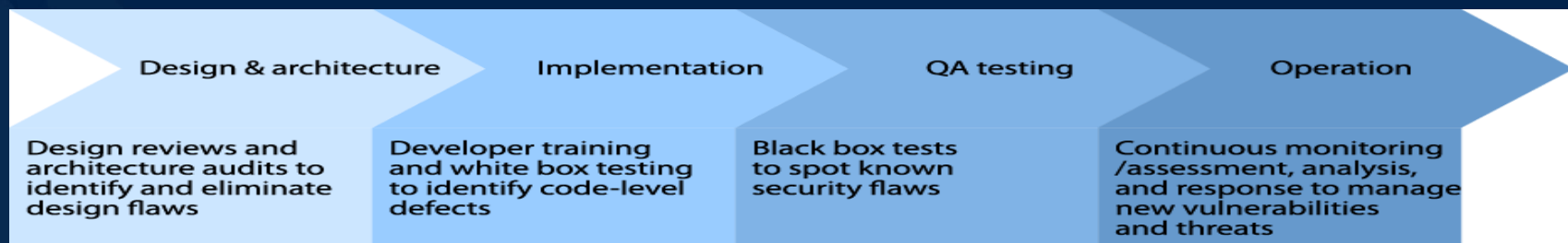
- ▶ The #1 reason: to catch vulnerabilities before attackers do
- ▶ Reduce cost of fixing bugs and vulnerabilities
  - ▶ Example: \$30,000 post release, \$3,000 integrated testing, \$500 development
- ▶ Help to achieve regulatory compliance
  - ▶ PCI, HIPAA, Sarbanes-Oxley, ...

# An application lifecycle view of security





- Begin with requirements
  - » What business asset does the software represent?
  - » What assets of value are accessible from the software?
  - » What protections must be provided for those assets?
- Design and architecture review
  - » What kind of operational environment
  - » What are the threats to my assets in this environment?
  - » What threat-mitigation measures must be provided?

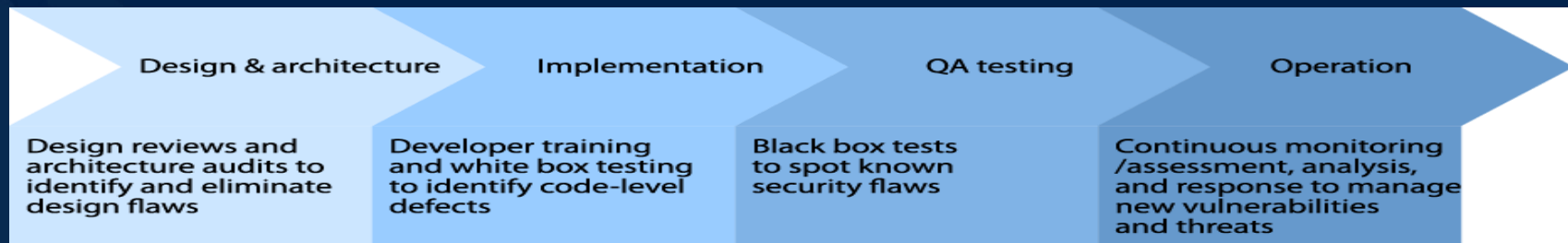


- Develop a company secure coding guidelines and standard
  - » Libraries of approved security functions
  - » Vulnerability remediation process
- Develop language-specific checklists
- Utilize code-level analysis tools
  - » Static analysis tools
  - » Security testing tools
- Code reviews and walkthroughs

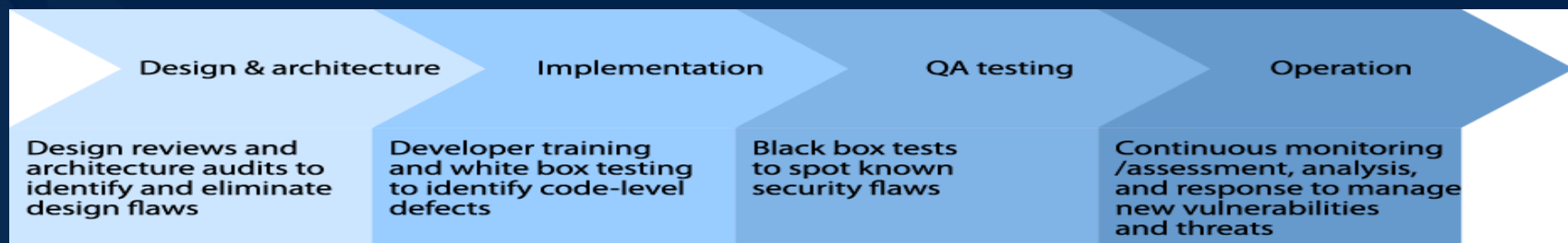
# Specific code-level guidelines

- Validate input from all untrusted data sources, including web inputs, environmental variables, network interfaces, and user controlled content
- Do not use any unsafe functions
- Sanitize all data sent downstream
- Use tried-and-true crypto packages: e.g, Bouncy castle,
- Verify security policies are enforced
- Do not hard-code default and test accounts
- Default deny: base access decisions on permission rather than exclusion

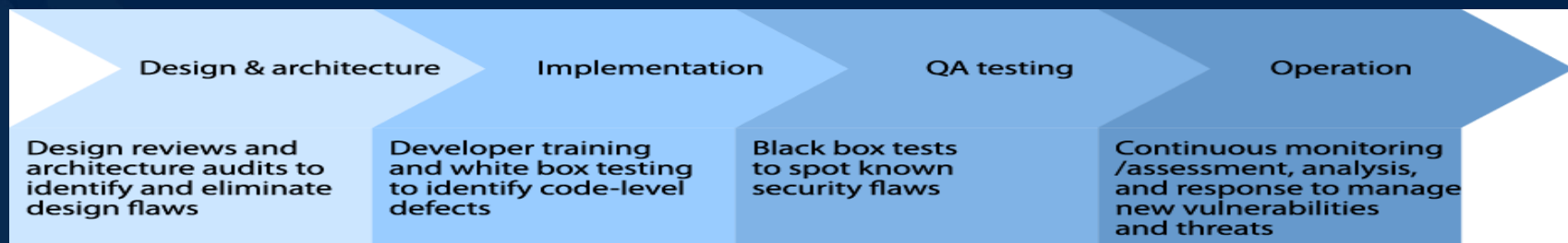




- Fault injection
- Fuzzing
- Black-box and automated penetration testing
- Augment with manual testing
- Whittaker and Thompson, *How To Break Software Security*, Addison-Wesley, 2004



- Secure configuration
  - » Disable all default accounts at the end of installation
  - » Force the user to set strong administrative passwords
  - » Configure appropriate logging and auditing procedures
- Secure operation
  - » Consider web application firewall
  - » Periodically conduct penetration and black box testing



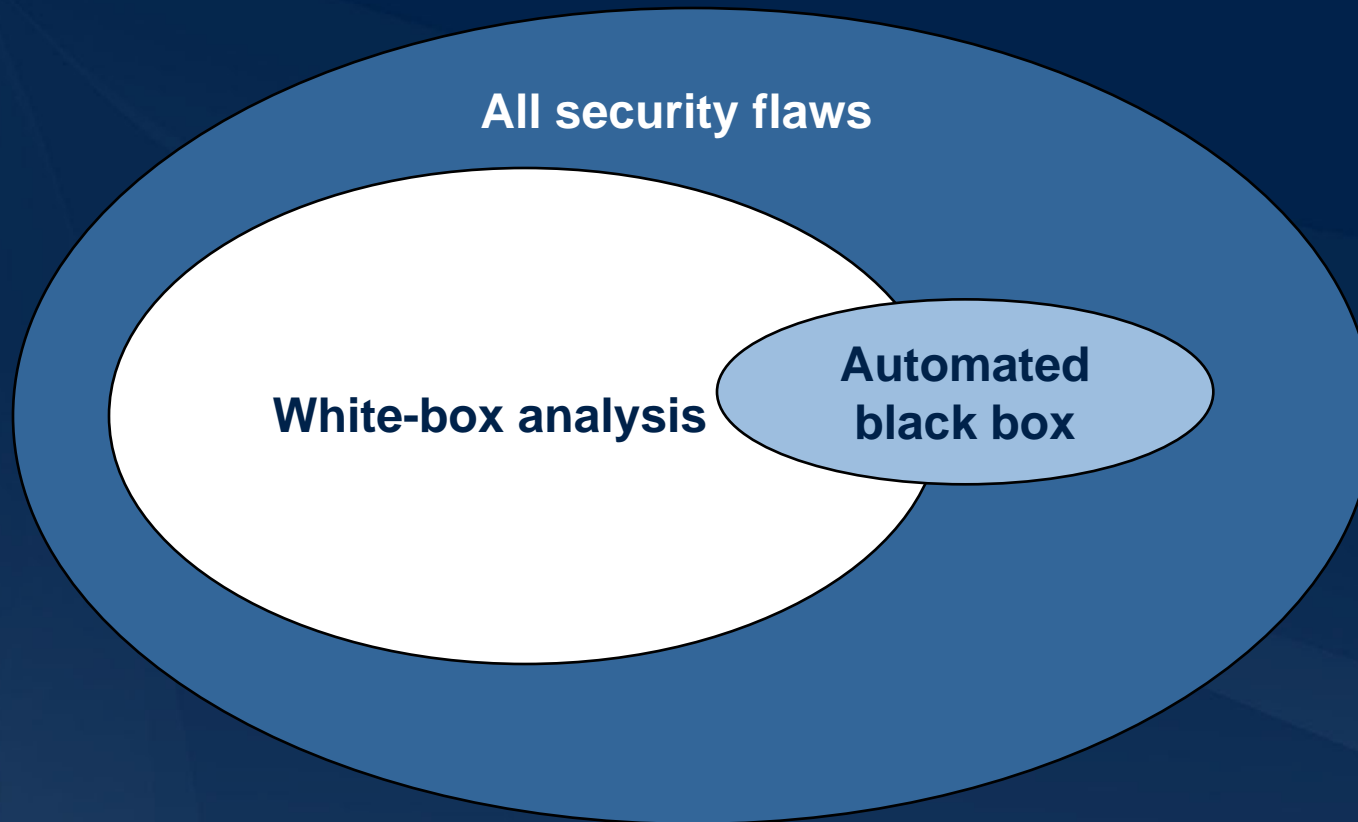
- Maintenance

- » Enforce all of your secure software development processes for maintenance releases of code
- » Integrate with change management procedures
- » Make sure that your maintenance engineers fully understand the intended use and architecture of the product and adhere to operational principles
- » Have an incident response plan

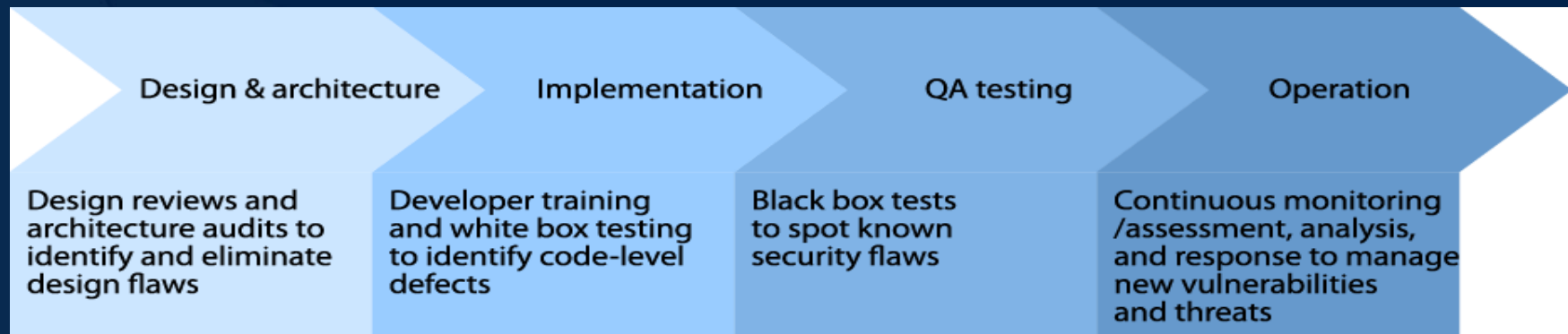
# How are companies adopt SDLC?

- >65% companies have penetration testing and black box scanning
- Source code security technology is by far the smallest
  - » Developers are under time-to-market pressure
  - » Security tools render false positives are not acceptable

# Comparing white-box and black-box



# 1 + 1 > 2?



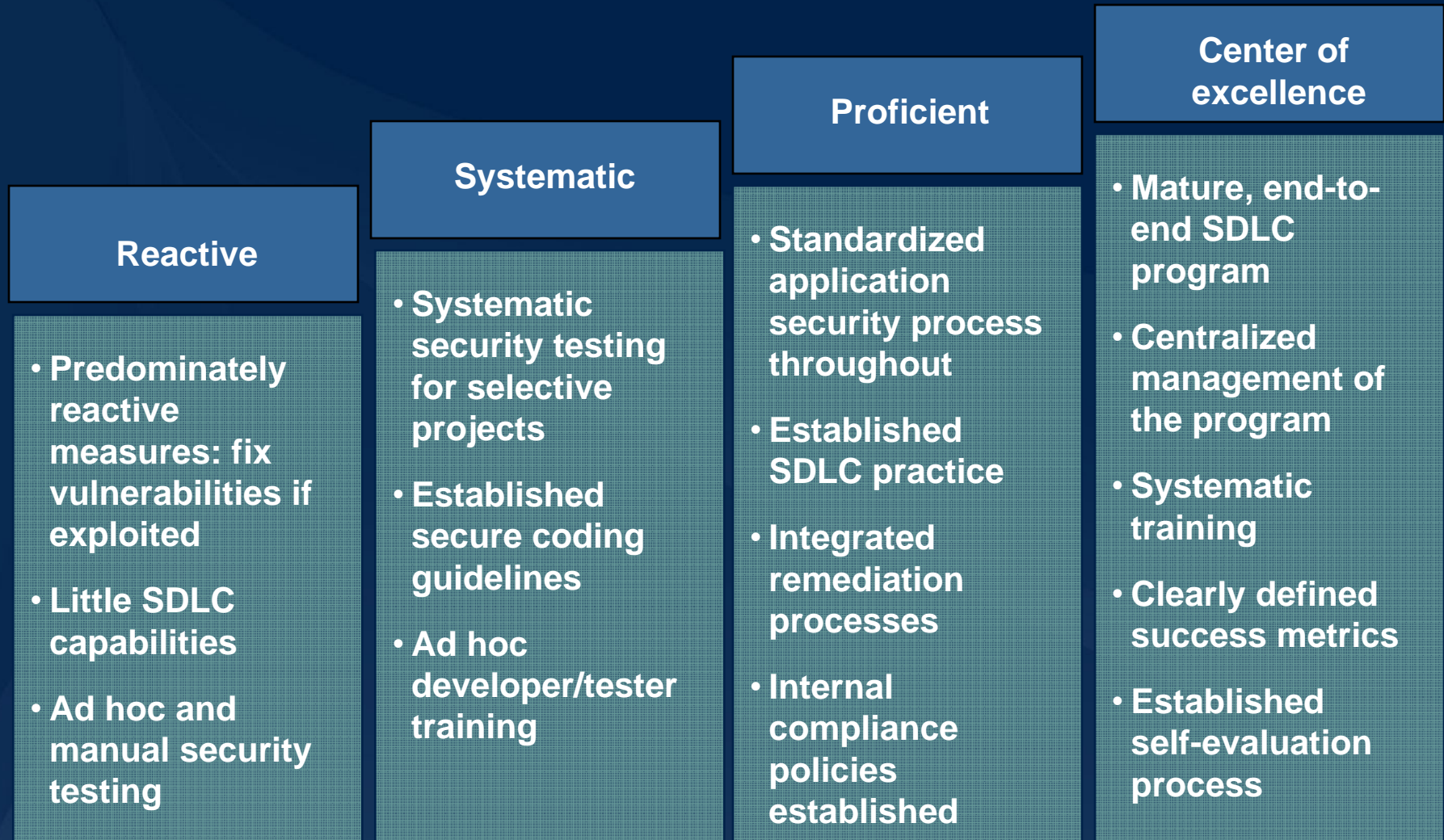
- **Integrated whitebox and blackbox, e.g.,**
  - » **Using black box tests to verify white-box findings**
  - » **Use white-box analysis to guide black box tests**
- **Users should demand integrated vendor functionality**
  - » **Only combine reports is not enough**



# Developer training is essential

- Defense in depth
- The principle of least privilege
- The principle of segregation
- Fail closed or fail secure
- Enforce known good traffic (white-list approach)
- Verify trust model
- Keep it simple. Complex designs increase the likelihood of security flaws.
- ...

# Build your application security maturity





# A look at trends going forward

# The consumer experience

The screenshot shows a Facebook profile for Chenxi Wang. The top navigation bar includes 'facebook', 'Profile', 'edit', 'Friends', 'Inbox (16)', and links for 'home', 'account', 'privacy', and 'logout'. The left sidebar contains a search bar, a list of applications (Photos, Groups, Events, Marketplace, My Family, and a Green Patch group), and an advertisement for 'Evanston's Newest Condos' for 'Grand Bend' in Green Bay. The main profile area features a large profile picture of Chenxi Wang, her name, and a status update asking 'What are you doing right now?'. Below this, her personal information is listed: Sex: Female, Relationship Status: Married to Chris Olston (Silicon Valley, CA), and Birthday: January 12. A 'Mini-Feed' section displays recent activity, including photos tagged by Maria Mancera De Contente and Pedram Keyani, and group additions to 'Friends of CERIAS'. The 'Friends' section shows 95 friends, with profiles for Joan Digney, John Viega, and Kevin Lai visible. The right sidebar contains a 'Mini-Feed' of recent updates, including group additions and status changes.

facebook Profile edit Friends ▾ Inbox (16) ▾ home account privacy logout

**Search**

**Applications** edit

- Photos
- Groups
- Events
- Marketplace
- My Family
- (Lil) Green Patch
- more

**Evanston's Newest Condos**

**GRAND BEND**  
GREEN BAY

The amenity-rich 1 and 2 bedroom condos of Grand Bend at Green Bay feature unique floorplans and distinctive details. Now open!

More Ads | Advertise

**Chenxi Wang**  
What are you doing right now?

Sex: Female  
Relationship Status: Married to Chris Olston (Silicon Valley, CA)  
Birthday: January 12

**Mini-Feed**  
Displaying 7 stories Import | See All

**July 21**

- Maria Mancera De Contente tagged Chenxi in 2 photos. 2:26pm  
Tagged in: **Gaby's Bday**

**July 4**

- Chenxi joined the group Friends of CERIAS. 4:28am Comment
- Chenxi and Garrett Wu are now friends. 4:28am Comment

**July 3**

- Pedram Keyani tagged Chenxi in a photo. 8:21pm  
Tagged in: **birthday 2008**

**June 30**

- Chenxi and Weidong Shao are now friends. 8:12am Comment

**June 27**

- Chenxi is experiencing painfully slow Internet connections. 7:33am Comment

**June 25**

- Chenxi wrote on Pablo Stern's wall. 12:30am

**Friends**  
95 friends See All

- Joan Digney
- John Viega
- Kevin Lai

# The enterprise experience

**General Ledger Transaction**

Journal Type

- ☒ Billing
- ☐ Disbursement
- ☐ Employee Payroll
- ☐ General
- ☐ Purchase (Accts Pay)
- ☐ Receipt
- ☐ Other

Transaction

Date: 12/31/2003

Number:

Balance:

New Abort

High Entry Save

List Quit

☒ Enter Vendor by Id Code

Line Item

**Distribution Allocation**

☐ Distribute via Allocation

Total Basis:

Total Value:

Contract:

Vendor:

Invoice:

Account:

Distribution:  Auto Balance

Amount:

Status: ☐ New Line

Support

Contracts Vendors **Accounts** Invoices

Account:

Description:

New

Account	Description
1100	CASH - IN BANK - REGULAR
1102	CASH - SAVINGS
1105	CASH - PAYROLL ACCOUNT

Recordset

Contract	Vendor	Invoice	Account	Amount
----------	--------	---------	---------	--------



A snowboarder wearing a bright yellow jacket, white pants, and a white helmet is captured mid-jump against a clear blue sky. The snowboarder is positioned in the upper left quadrant of the frame, with a spray of snow trailing behind them. The background features a vast, snow-covered mountain range under a deep blue sky. In the foreground, dark evergreen trees are visible, some partially covered in snow. The overall scene conveys a sense of adventure and outdoor recreation.

**The consumer and  
enterprise experience  
gap will disappear ...**

# Prediction ...

- Reputation will be pervasive
  - » Reputation for program/code
- Ways to recognize invariants in the code
  - » Innovative fingerprinting technology
- Ways to analyze software
  - » Faster than current emulation technology
- Reputation will live in the cloud
- Optimization on the gateway



# Summary

Application security is not

- Patching, encryption
- Even secure coding

Application security is

- Applying information security principles to software engineering and operations
- Process of designing, building, deploying, and maintaining software that cannot easily be misused for malicious purposes



# Information resources for application security

- Open Web Application Security Project (OWASP) Top Ten at <http://www.owasp.org>
- Web Application Security Consortium (WASC) Threat Classification at <http://www.webappsec.org>
- Chenxi Wang, Ph.D. “Managing Application Security from beginning to end”, Forrester research report, October 2007.
- Michael Howard. “Writing Secure code for Windows Vista,” Microsoft Press, 2007
- Gary McGraw. *Software Security: Building Security In.* Addison-Wesley, 2006
- “Improving Web Application Security: Threats and Countermeasures,” Microsoft Press, 2003





# Thank you.

Questions?

Slides: [www.forrester.com/owaspnyc2008](http://www.forrester.com/owaspnyc2008)

- Chenxi Wang  
Principal Analyst  
Forrester Research
- Email  
[cwang@forrester.com](mailto:cwang@forrester.com)
- Blog  
[blogs.forrester.com/srm](http://blogs.forrester.com/srm)