

Forrester Survey Briefing – Software Risk in Enterprises

Chenxi Wang, Ph.D.
Principal Analyst
Forrester Research

Chris Wysopal
CTO
Veracode Inc.

Today's Speakers



Chenxi Wang, Ph.D., serves as Forrester's Principal Analyst, Security and Risk Mgmt. She is a leading expert on content security, application security, and vulnerability management. Chenxi leads the effort at Forrester to build the application security and Web 2.0 security research portfolio. Chenxi's research builds on her in-depth technical insights and her years of research experience. Chenxi covers topics such as best practices for content and application security, emerging threats, and operational aspects of security deployment.

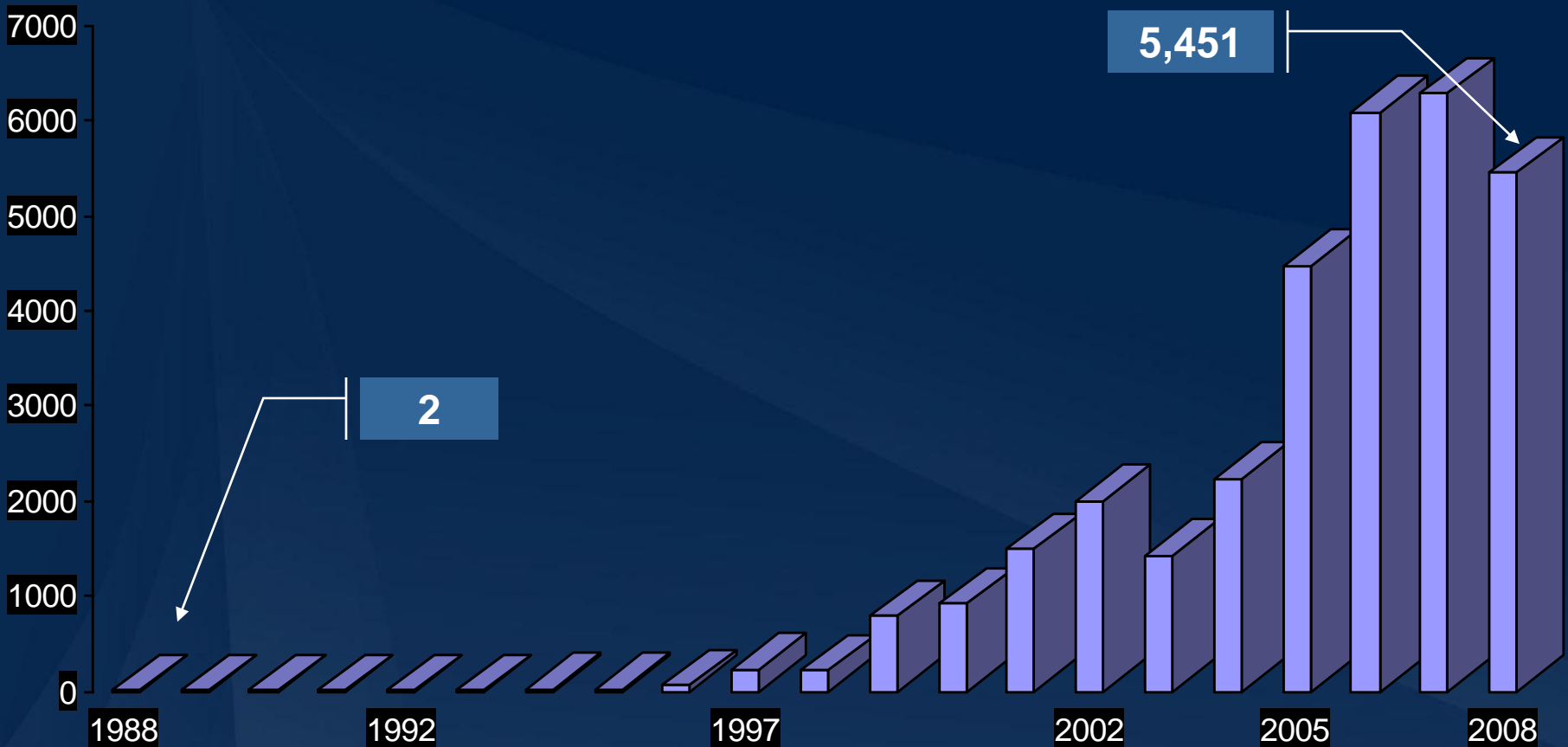


Chris Wysopal, Veracode's CTO and Co-Founder, is responsible for the company's software security analysis capabilities. In 2008 he was named one of InfoWorld's Top 25 CTO's and one of the 100 most influential people in IT by eWeek. One of the original vulnerability researchers, he has testified on Capitol Hill in the US on the subjects of government computer security and how vulnerabilities are discovered in software.

Agenda

- Survey background
- High level survey findings
- Current industry practices of application security
- Application security market outlook
- Summary and recommendations

Software vulnerabilities continue to rise



Number of high and medium vulnerabilities reported in NVD

High profile case

Kaspersky vulnerability exposes sensitive customer database



Conficker exploited a Windows vulnerability



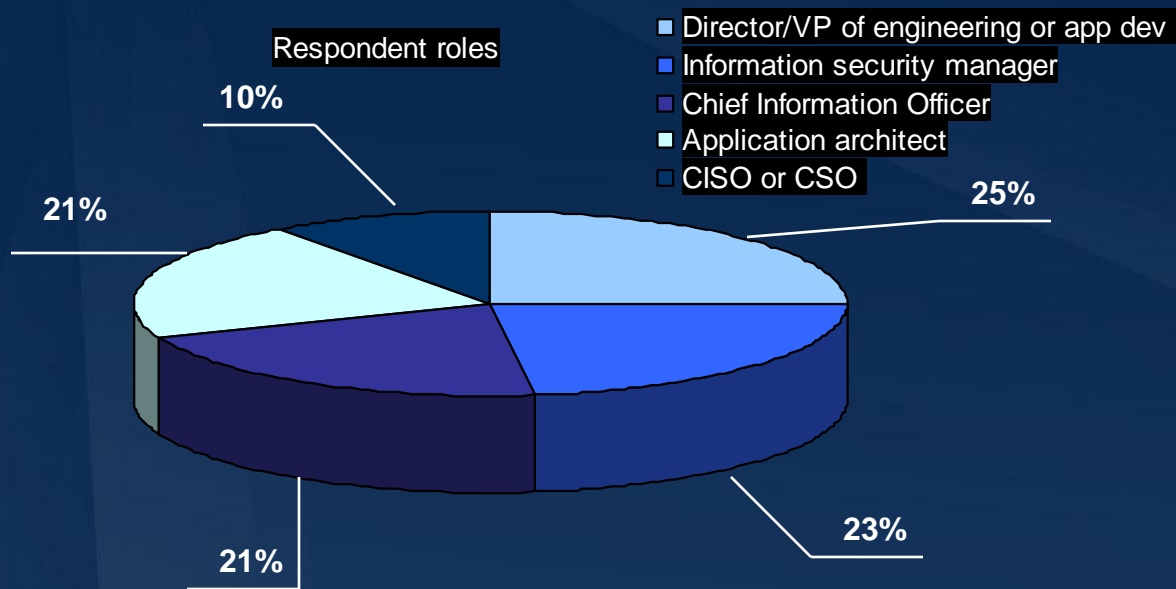
Protecting Against the Rampant Conficker Worm



Conficker infected critical hospital equipment, expert says

A Veracode-sponsored Forrester Survey

- Purpose: a study of software security risk in enterprises
- Survey target: 204 IT professionals, across US and UK companies
- Roles span info sec, app dev, sourcing, app support
- Majority has specific app security responsibilities
- Respondents came from many industry verticals



Many respondents process critical or confidential data

Of the following, what data are you processing with your apps? Select all that apply.



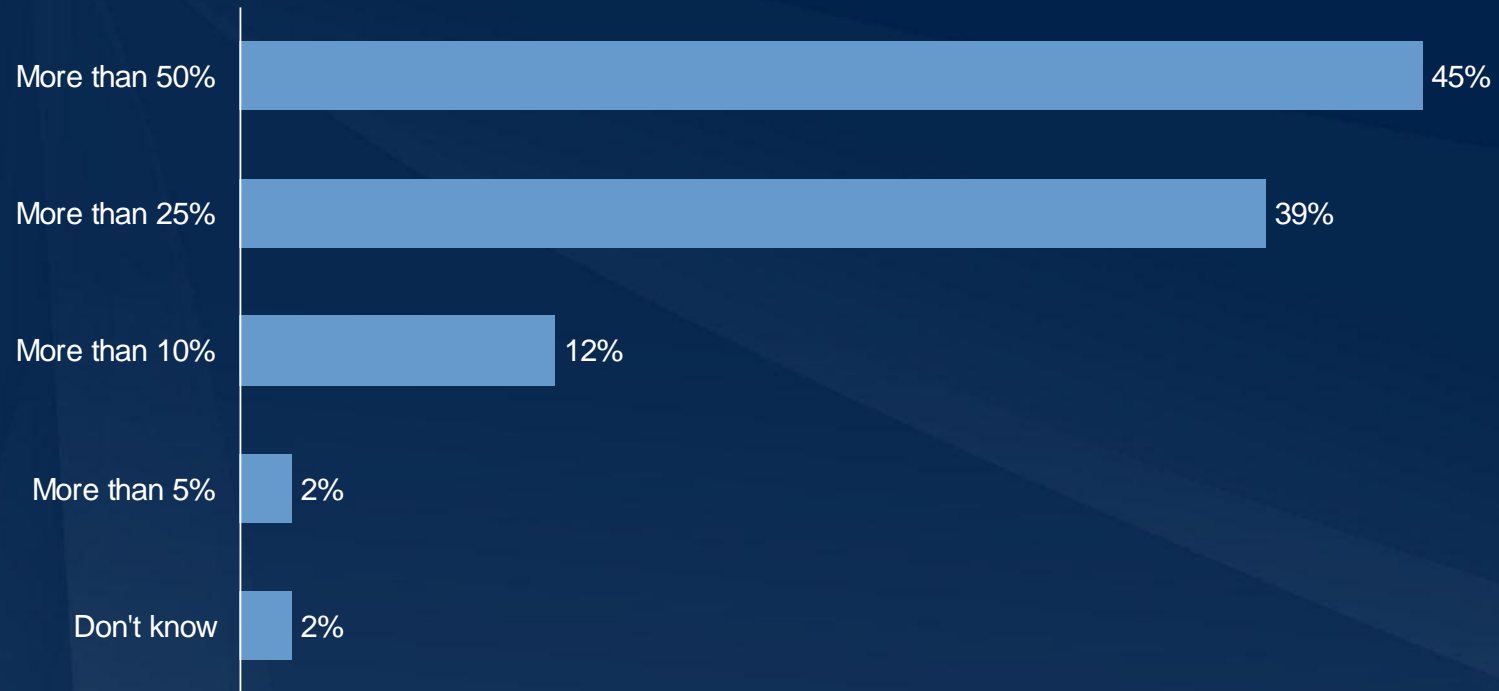
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

Many have extensive compliance requirements

What percentage of your application is subject to compliance regulation, either external or internal regulations?



Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

Survey: Software Security Risk in Enterprises

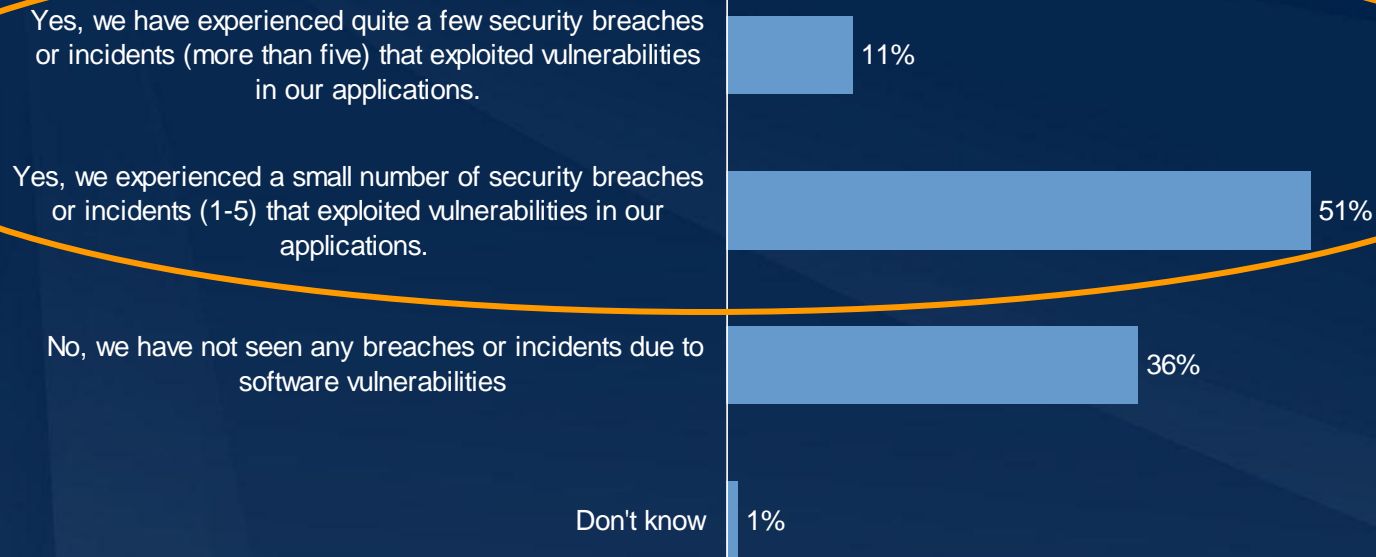
HIGH LEVEL SURVEY FINDINGS

High level findings

- Many firms experienced breaches exploiting software vulnerabilities
- Yet a great many do not know the security quality of their critical applications
- And many do not have adequate policies mandating application security
- Developer training is largely ad hoc
- There is a disconnect between investment level in application security and threats targeting applications
- Many firms begin to require extensive testing of COTS software

62% experienced security breaches exploiting software vulnerabilities in the last year

In the last 12 months, have you experienced any security incidents or breaches due to a software vulnerability in your applications?

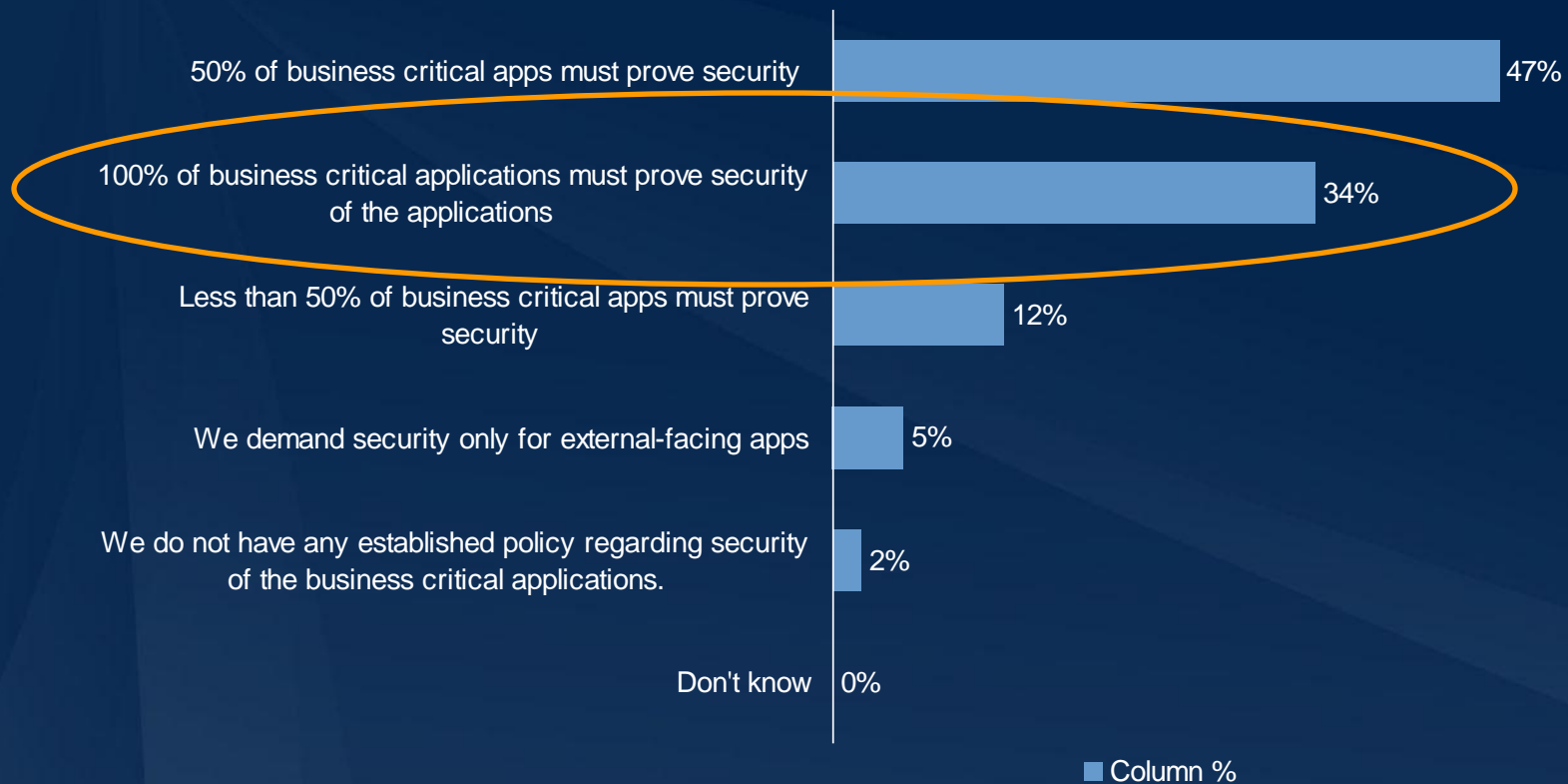


Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

But many do not know the security quality of their business-critical apps

What is your internal policies and procedures regarding security of your application, either imposed by infosec or by the application team?



Only 34% require all business critical apps to prove security quality

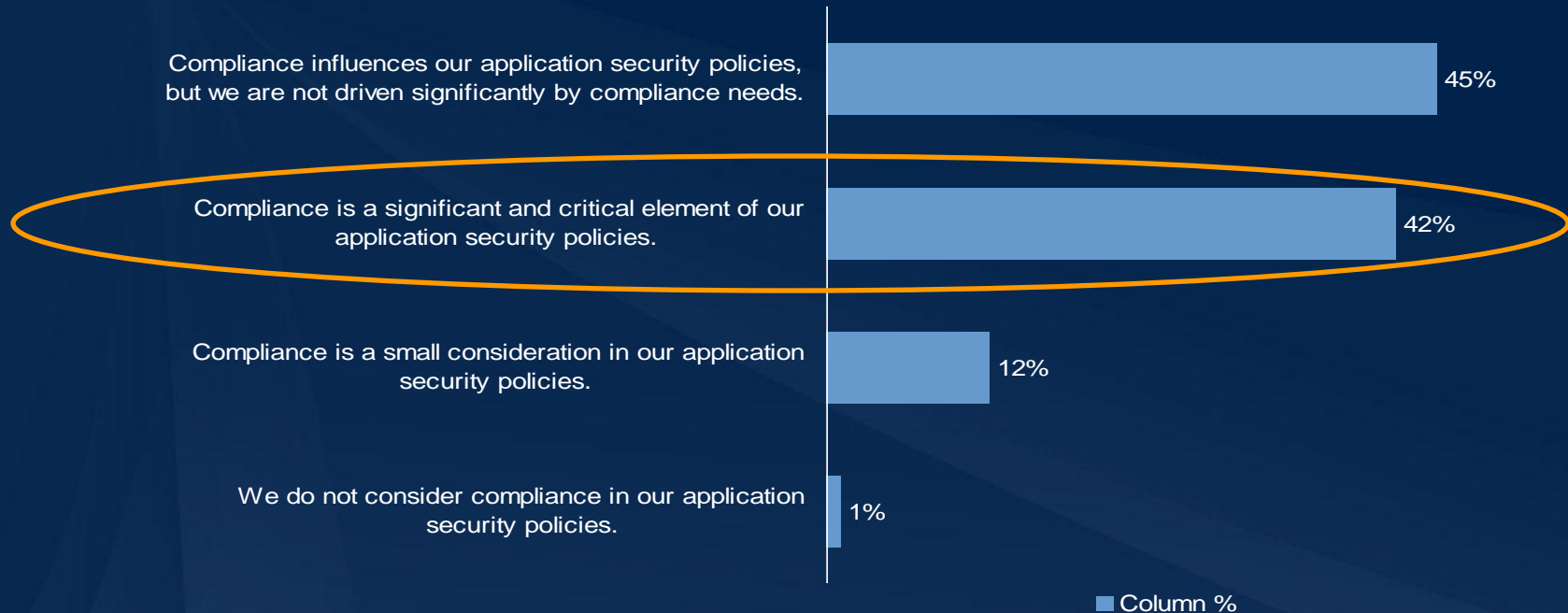
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

Compliance requirements are not considered sufficiently

Q12: How much does compliance regulation affect your application security policies?



Only 42% considers compliance a significant factor for their application security policies

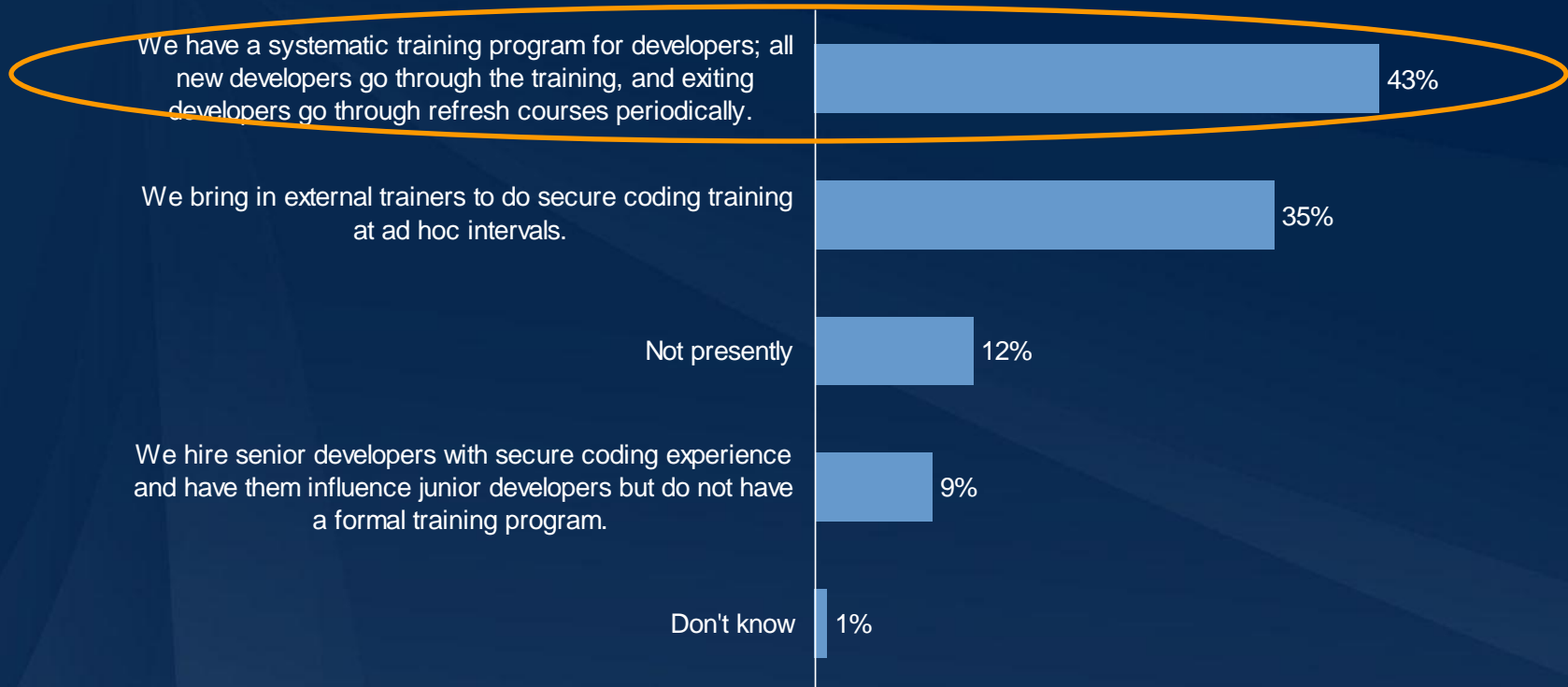
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

Only 43% have systematic training for developers

Do you have a developer training program for secure coding and security awareness?



Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

Survey: Software Security Risk in Enterprises

CURRENT APPLICATION SECURITY PRACTICES

Third-party code is used pervasively



These applications are processing PII, critical and confidential data

Companies do not have adequate policies to ensure security of open source code

What is your understanding towards security of open source components?

We treat open source code the same as internally developed code, and put it through the same security review and audit process.

38%

We realize there is a certain amount of security risks associated with using open source code, but presently we are not doing anything particular to address open source security.

34%

We consider open source code secure because we trust the code is thoroughly vetted by the open source community.

10%

We have special tools we use to evaluate the security of open source code.

9%

We do not have a policy regarding the security of open source code

5%

Don't know

3%

Not doing anything

49% are not doing anything regarding security of open source code

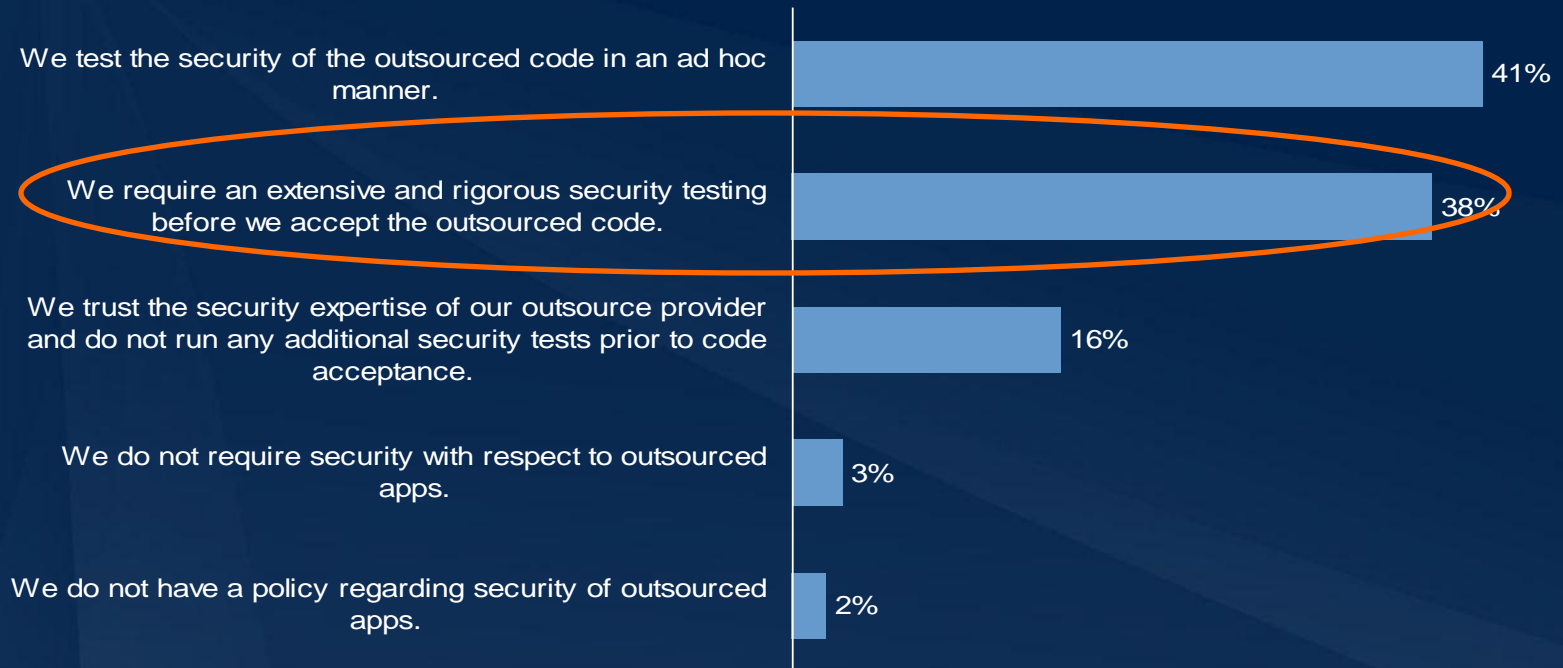
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

Many do not have adequate policies to ensure security of outsourced code

What is your policy regarding security of outsourced applications?



62% are not doing rigorous testing for open source code

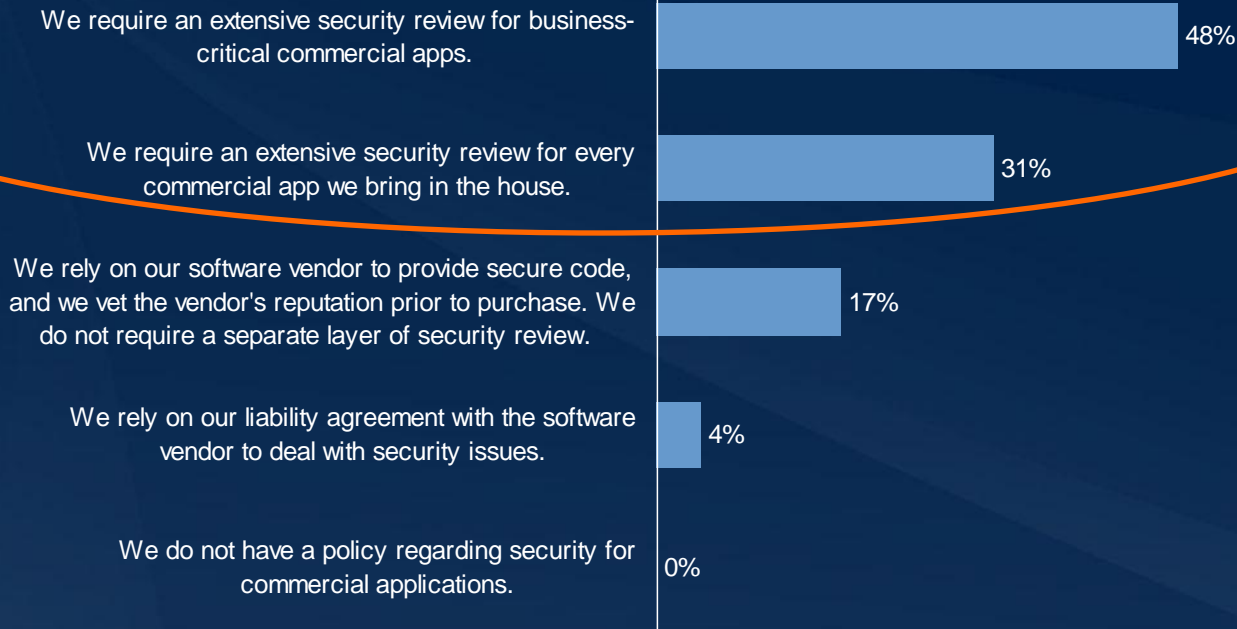
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

Exception: Many reported policies for extensive testing of COTS apps

What is your policy regarding the security of commercial applications?



■ Column %

79% employ extensive review for COTS apps

Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

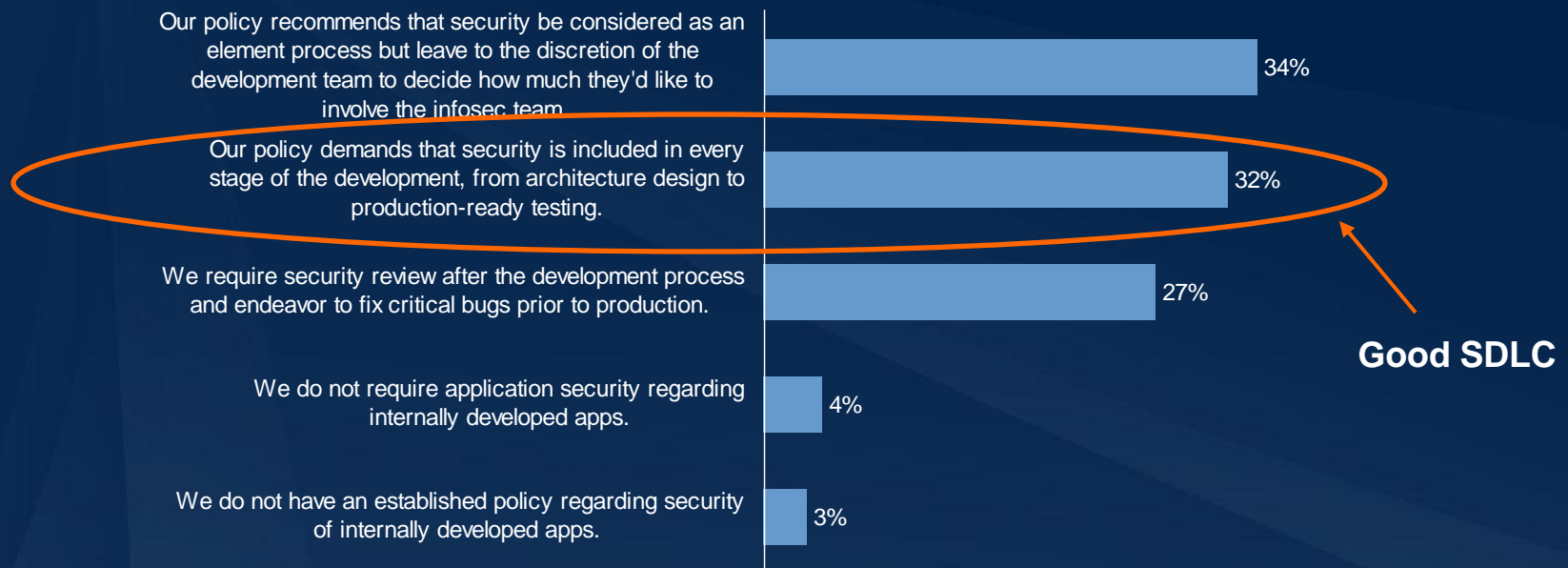
FORRESTER®



What about internally developed applications?

Many do NOT mandate security in every stage of the development process

What is your policy regarding security of internally developed applications?



Only 32% reported a comprehensive secure development life cycle approach

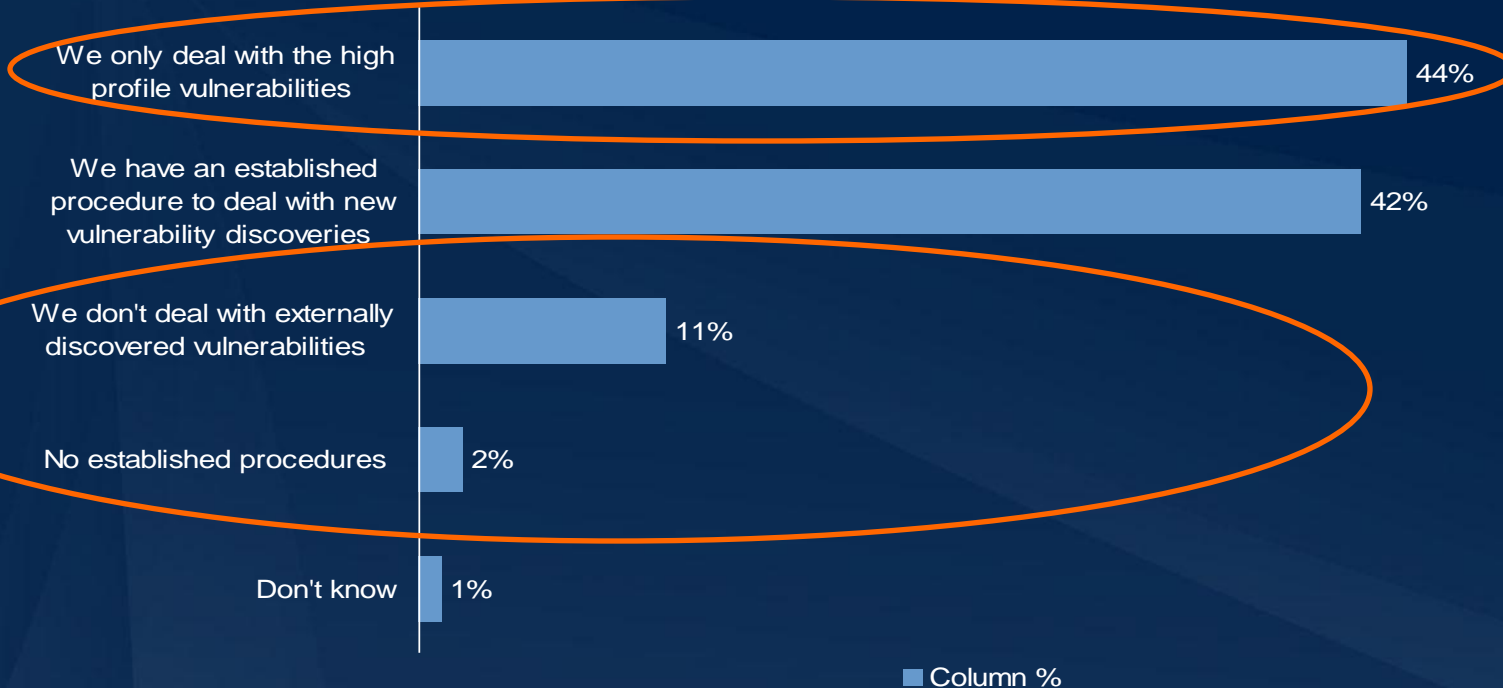
Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

FORRESTER®

58% of companies do NOT have established procedures to handle vulnerability information systematically

Q13: How do external discoveries of new software vulnerabilities impact your security policies?

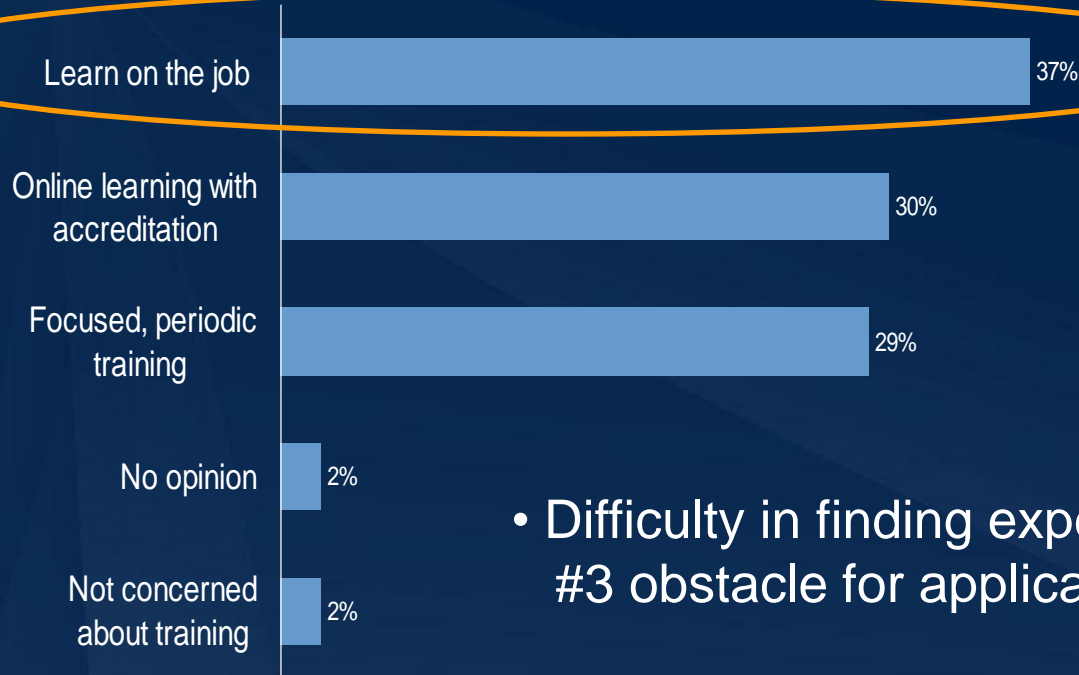


Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

Developer training is ad hoc

Q25: In your opinion, what is the best way to deliver developer training in secure coding and security awareness?



- Difficulty in finding experienced developer is the #3 obstacle for application security initiatives
- Only 43% of organizations have systematic developer training program

Base: 204 IT Professionals

Many firms have a false sense of security when it comes to application security practices

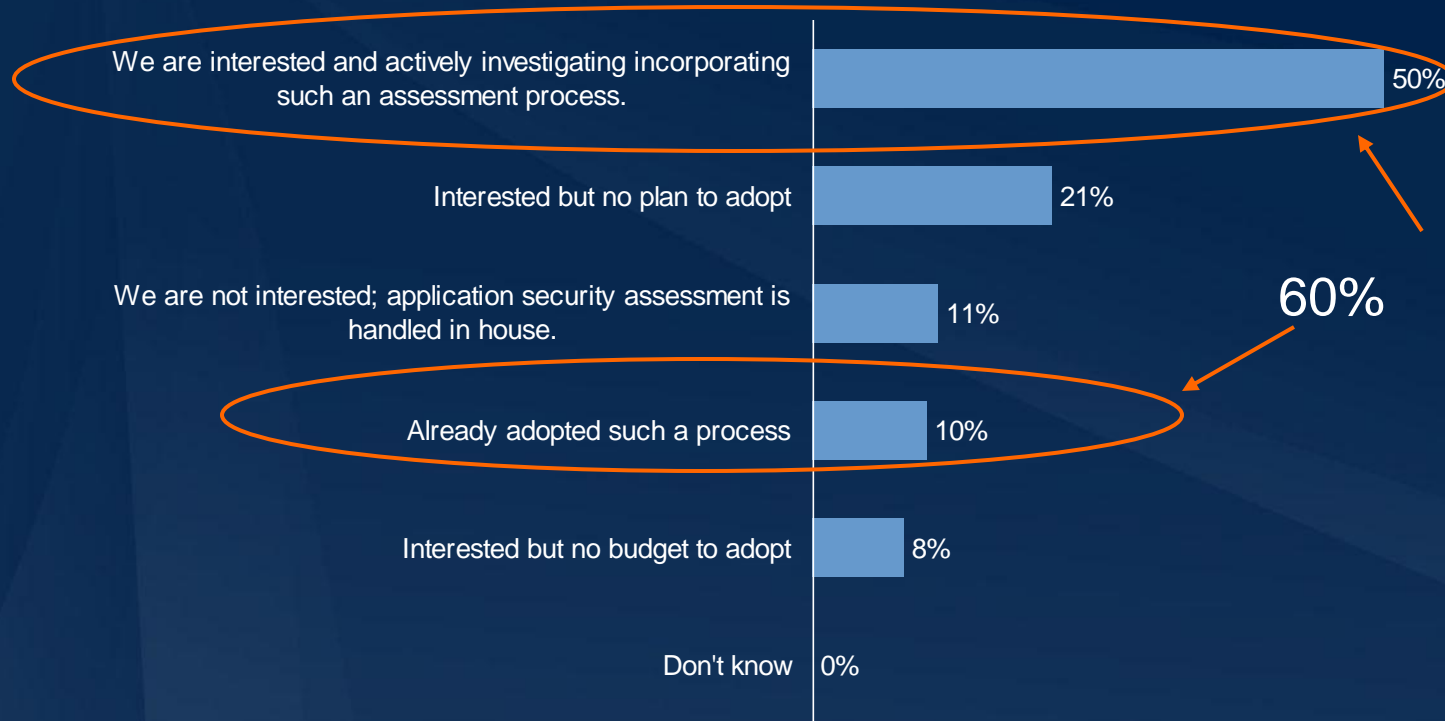
- Case #1
 - » 74% say their appdev team takes the leading role in application security initiatives
 - » 68% say the appdev team works “closely” with information security team
 - » However, only 32% have extensive SDLC processes
 - » Conclusion: Security team is used, at best, in an ad hoc fashion
- Case #2
 - » 94% say they know at least the security quality of at least half of their apps
 - » But 40% say they do not know the security quality of COTS, open source and outsourced code
 - » And we know COTS, open source, and outsourced code is used extensively
 - » Conclusion: the 94% number reflect inflated confidence

Survey: Software Security Risk in Enterprises

APPLICATION SECURITY OUTLOOK, SUMMARY & RECOMMENDATIONS

60% are interested in (or already adopted) third-party assessment of outsourced and commercial applications

For security reasons, would your organization be interested in incorporating a third-party security assessment as part of your software procurement process either for commercial or outsourced applications?

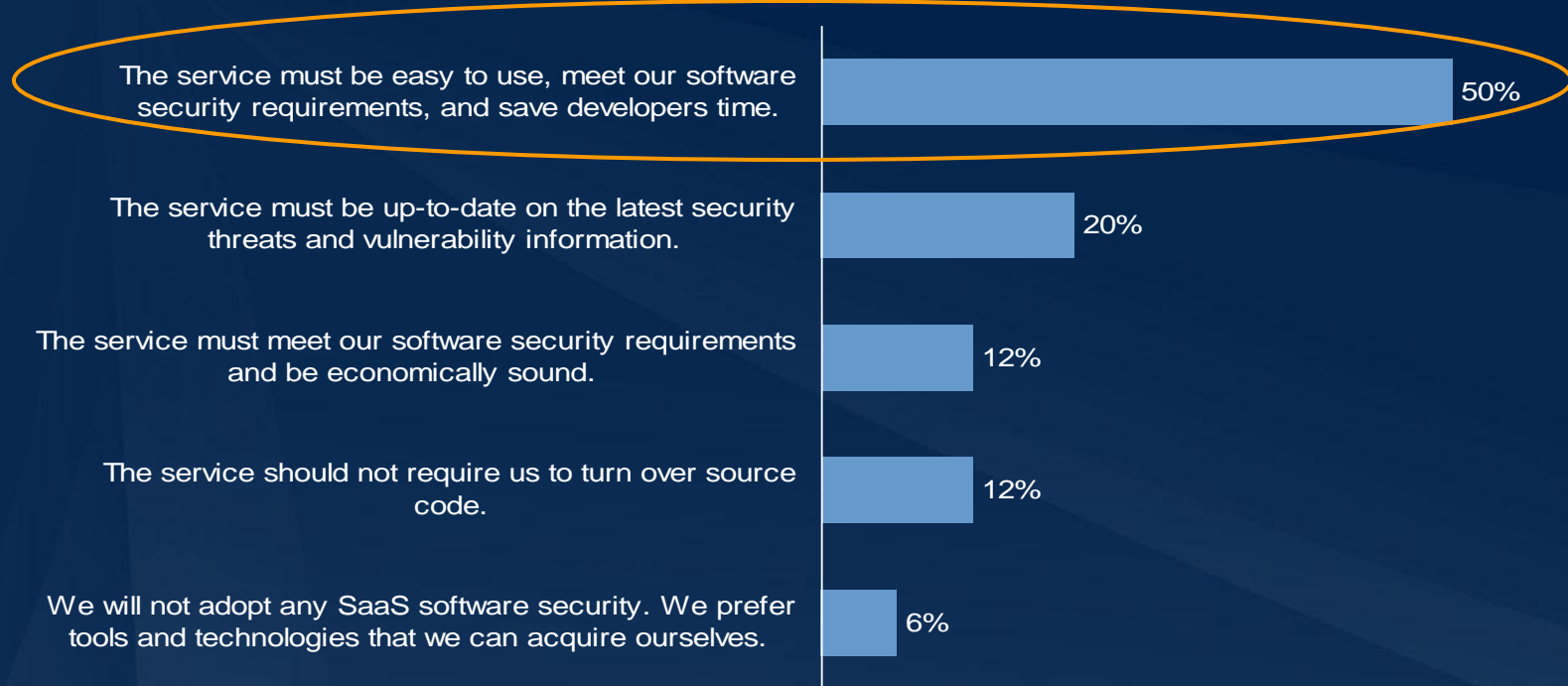


Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

Easy to use and save developer time is the top criteria for third-party services

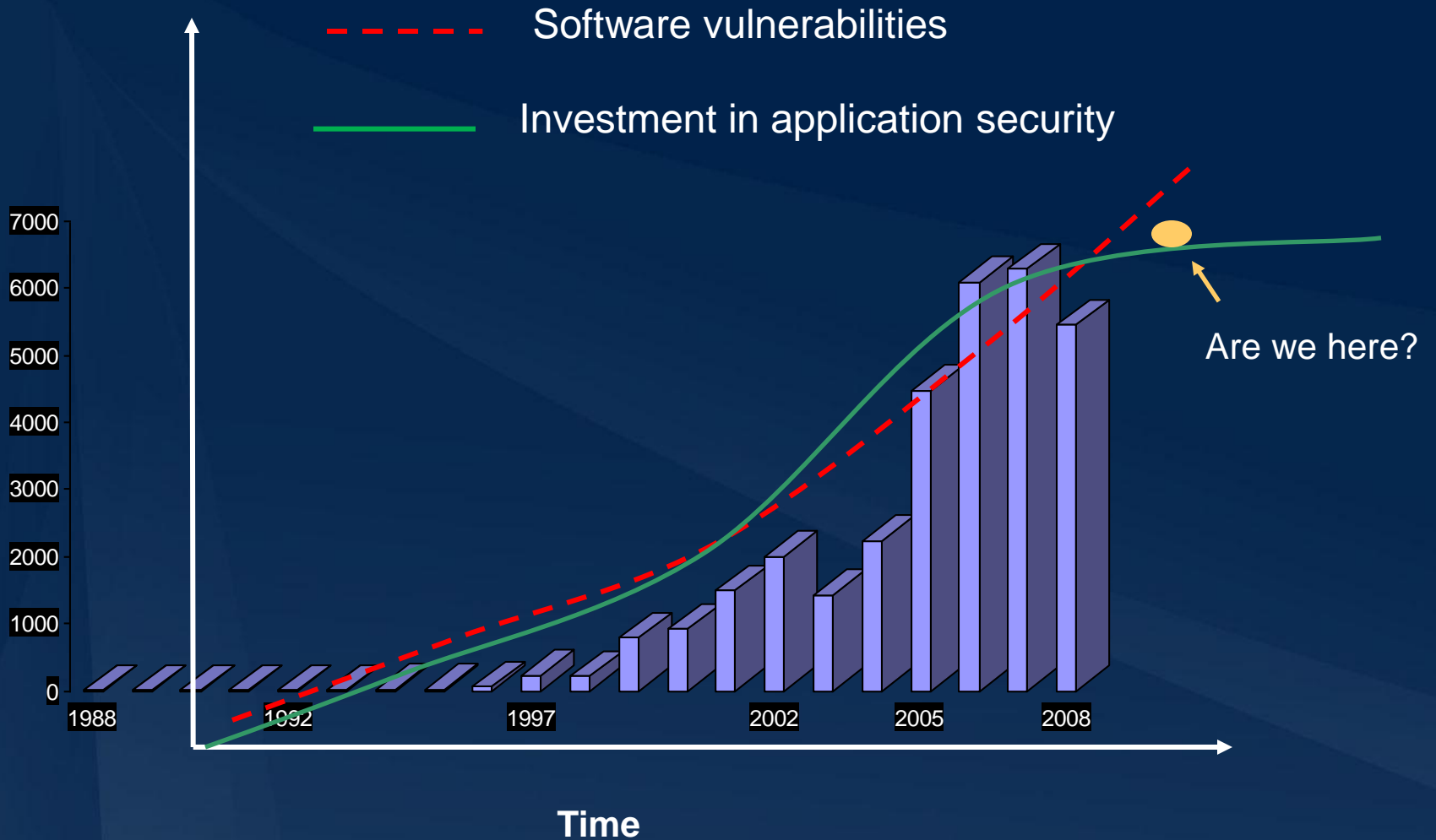
If you were to adopt software security in the cloud, what would be the top criterion for such a service?



Base: 204 IT Professionals

Source: Online Survey of 204 Application and Risk Management Professionals. A commissioned study conducted by Forrester Consulting on behalf of Veracode, March, 2009

What's wrong with this picture?



Summary

- Application vulnerability volume is on the rise, so are incidents
- Many firms do not have adequate policies regarding security testing and assurance for software applications
- Requirements for secure COTS are beginning to surface in the industry
- There is a disconnect between application security investment outlook and the threat level

Recommendations

- Re-examine your appsec policies
 - » Focus on threats carried by third-party code
 - » Focus on internal development practices (SDLC)
- Heed compliance requirements in your policies
- 12-month game plan
 - » Continue to invest in application security mandates by regulatory compliance
 - » Employ rigorous testing and assurance procedures for critical apps
 - » Consider third-party assessment services to save cost and optimize capacity planning

A person is climbing a dark rock face on the left side of the image. The background shows a vast mountain range with snow-capped peaks under a clear blue sky. The overall scene is dimly lit, suggesting either dawn or dusk.

Thank you.

Questions?

- **Chenxi Wang**
Principal Analyst
Forrester Research
- **Email**
cwang@forrester.com
- **Blog**
blogs.forrester.com/srm