OWASP Security Spending Benchmarks Report

OWASP AppSec DC Nov 13th, 2009

Boaz Gelbord

Executive Director of Information Security, Wireless Generation

Project Leader, OWASP Security Spending Benchmarks Project

Personal Ruminations on Info Security: www.boazgelbord.com

A quick straw poll...

A quick straw poll...

- Does it cost more to produce a secure product than an insecure product?

A quick straw poll...

- Does it cost more to produce a secure product than an insecure product?
- The correct answer is YES

One More Question…

One More Question...

- Do any of you not shop somewhere/not go to a hospital/not enroll in a university because they have had a data breach?

One More Question...

- Do any of you not shop somewhere/not go to a hospital/not enroll in a university because they have had a data breach?
- The correct answer is NO (even if you think it is YES)

Hmmm...

So why do we spend on security?

And how much should we be spending?

- Security imposes extra costs on organizations.
- The "security tax" is relatively well known for network and IT security - 5 to 10% (years of Gartner, Forrester, and other studies).
- No comparable data for development or web apps.
- Regulations and contracts usually require "reasonable measures". What does that mean?

OWASP Security Spending Benchmarks Project

- 20 partner organizations, many contributors.
- Open process and participation.
- Raw data available to community.


CSI
COMPUTER
SECURITY
INSTITUTE


FORTIFY


nCircle


AppSec
CONSULTING
Security Compliance & Assurance

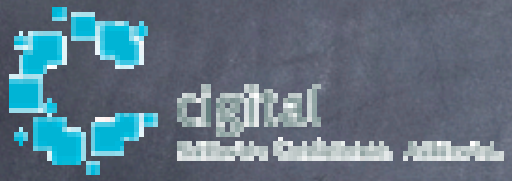

GOTHAM
DIGITAL • SCIENCE


SecTheory


CENZIC


if(is)
internet security.


THE Open GROUP
Making standards work®


digital


IMPERVA


DENIM GROUP


ASPECT SECURITY
Application Security Specialists


ts/sci security


Securosis

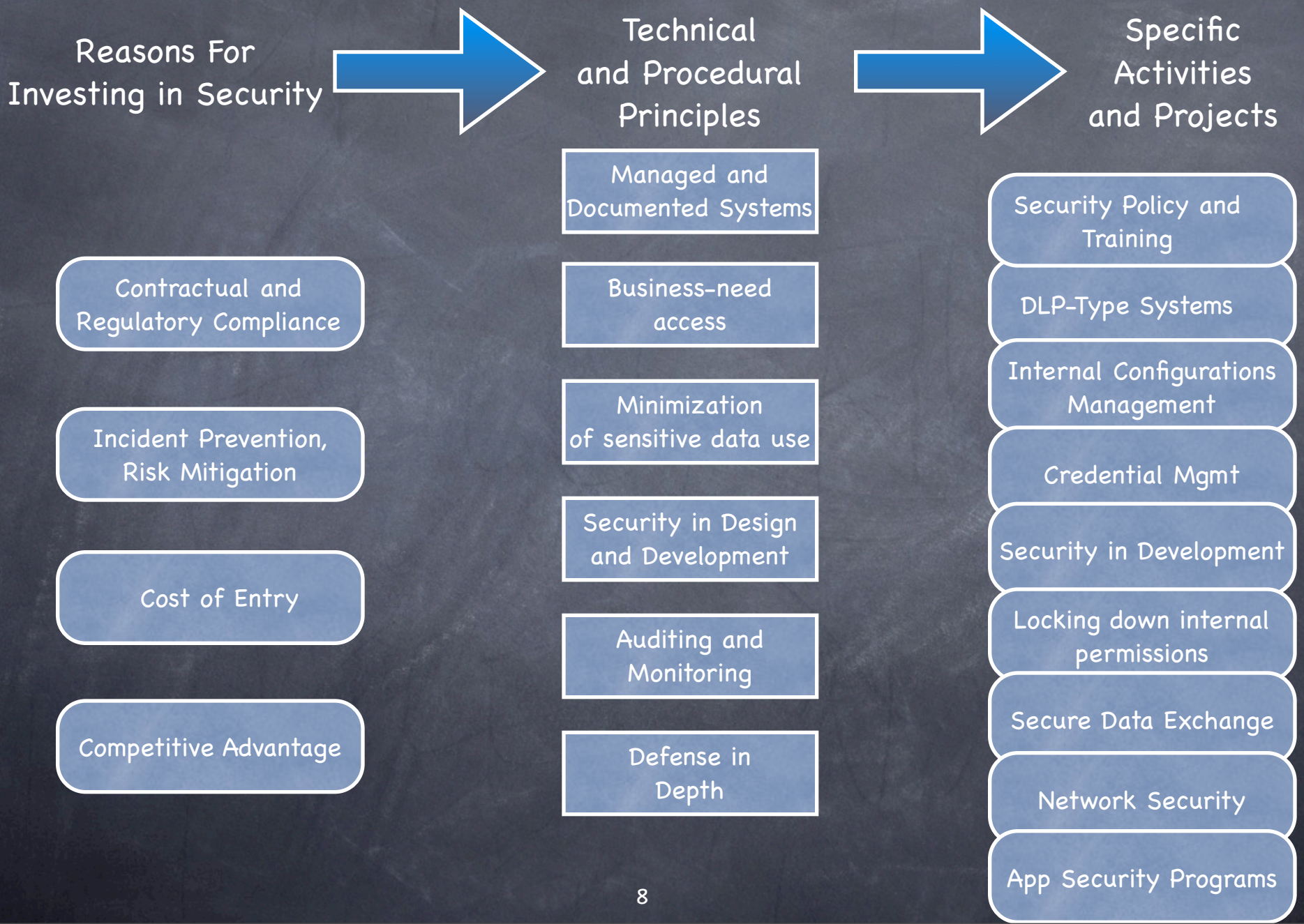

Echelon One, LLC
Executive Security Intelligence


TeleTrusT
Pioneers in IT security.


eema
www.eema.org


MetroSITE
Group


WhiteHat
SECURITY


Reasons For Investing in Security
Technical and Procedural Principles
Specific Activities and Projects
Contractual and Regulatory Compliance
Incident Prevention, Risk Mitigation
Cost of Entry
Competitive Advantage
Managed and Documented Systems
Business-need access
Minimization of sensitive data use
Security in Design and Development
Auditing and Monitoring
Defense in Depth
Security Policy and Training
DLP-Type Systems
Internal Configurations Management
Credential Mgmt
Security in Development
Locking down internal permissions
Secure Data Exchange
Network Security
App Security Programs

The 10000' View For Most Organizations

Legal and Regulatory Compliance

Because We Have To

Incident Prevention, Risk Mitigation

Cost of Entry

Because This is What Everyone Else Does

Competitive Advantage

Really?

Regs are Not App Sec Friendly...

- Regulations, contracts, and RFPs are usually based on the notion of "reasonable effort" - state regulations, HIPAA, FTC, SEC, Red Flags Rule.
- When regulations do get technical, they focus on old school security fetishes like firewalls, SSL, encryption, biometric passes in server rooms.

A Few Examples

- PCI Prioritized Approach
- Massachusetts 201 CMR 17.00
- The encryption exemption in state data breach notification laws
- HIPAA Notification Form
- Recent SEC Action
- Most of the contracts/RFPs/Vendor security whitepapers I have seen...

A Real World Example of Where Your PII Lives...

- Small company with a few dozen employees sells widgets over the Internet.
- They pay an outsourced team to develop a Joomla/Drupal/whatever site to build a widget-lovers community where users can connect. All sorts of PII involved in the app.
- They deploy their site on a shared hosting/VPS model and basically only interact with the App from a web admin interface.
- They know a bit about the technical details of their app but not much. Actually, no actual web developers were really involved in the building or deployment of the app.

Here is What Company A Did...

- Asked their developer team in India to develop code securely. Referenced OWASP Top 10 or similar list.
- Told their development team that services and database users needed to run with minimum privilege. Dev team balked. Company A agreed to pay a bit extra.
- Did a bit of reading on best practices for Joomla/Drupal/whatever security and tried to implement as much of this as possible. Maybe even hired someone to lock down their server.
- Configured their servers so admin interfaces are only available from their IP range.

And Here is What Company B Did...

- Installed anti-virus on all employee machines.
- Bought a firewall for the corporate network.
- Maybe even got two-factor tokens for network access.
- Made sure everything is going over SSL everywhere.
- Put a biometric reader on the entrance to the local data center.
- Encrypted all laptops.

One more poll question...

One more poll question...

- Which company is more likely to be in compliance with state laws and other regulations?

One more poll question...

- Which company is more likely to be in compliance with state laws and other regulations?
- The correct answer is Company B

And one final question...

And one final question...

- Which company is more likely to suffer a data breach?

And one final question...

- Which company is more likely to suffer a data breach?
- The correct answer is Company B

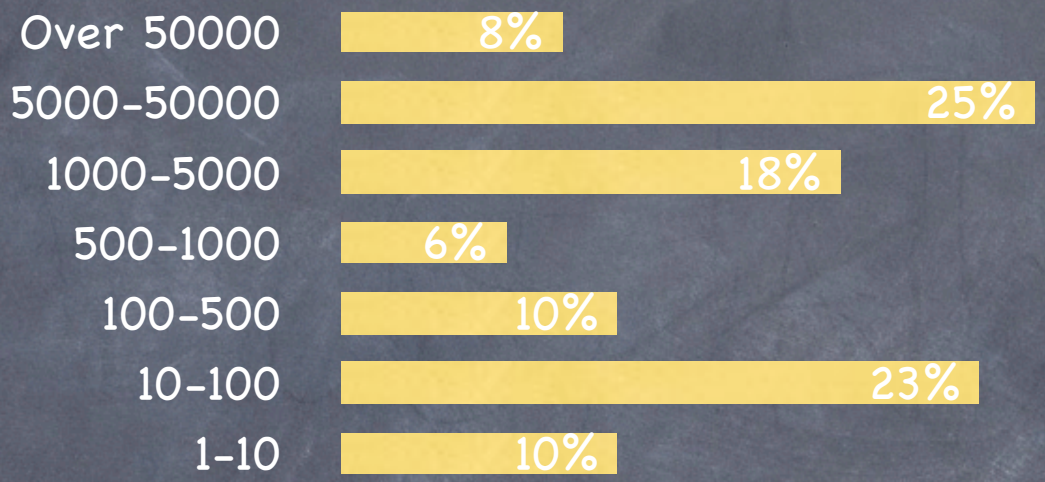
So the only think left to finance your app sec program is the "reasonable spend" argument...

As a community we need to get some consensus on what constitutes reasonable spend...

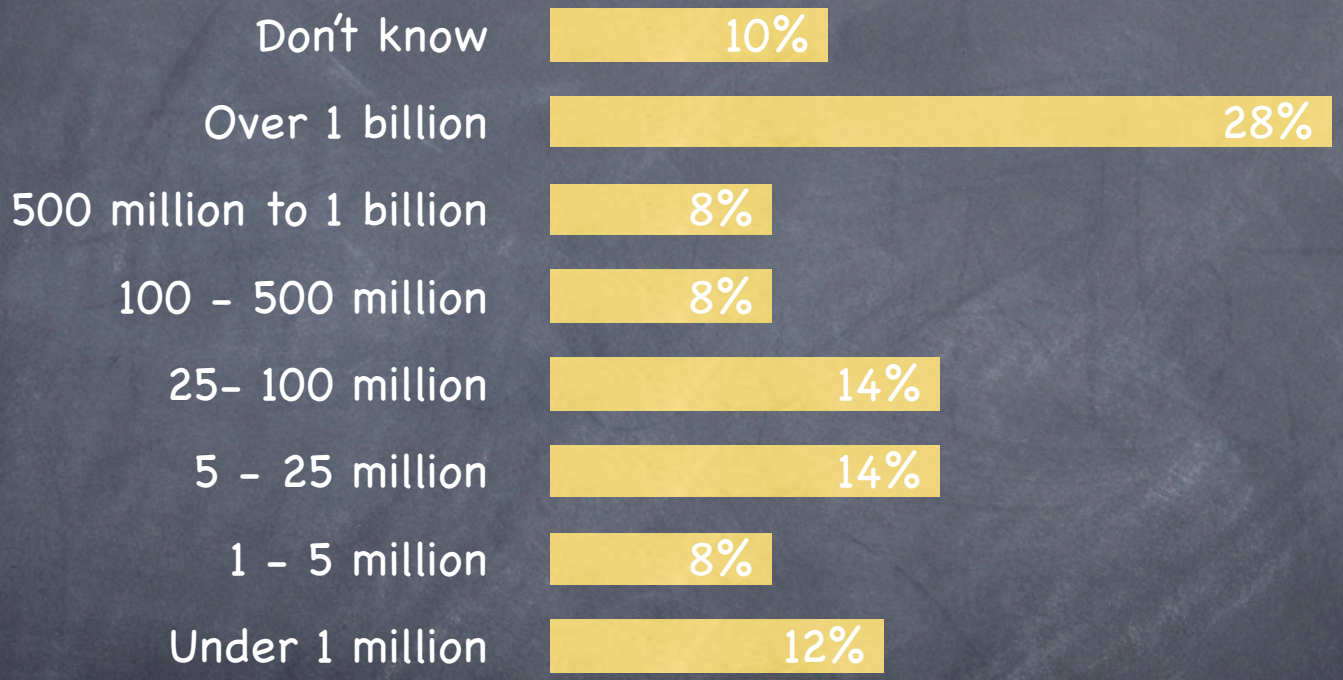
- First survey focussed on general web application spending.
- Second survey focussed on cloud computing.
- Responses currently being gathered for third survey.
- Approximately 50 companies profiled in each case.

- We do not collect IP addresses
- Most of the partners are security vendors
- Relatively small respondent base
- Meant to stimulate a discussion on security spending benchmarks.

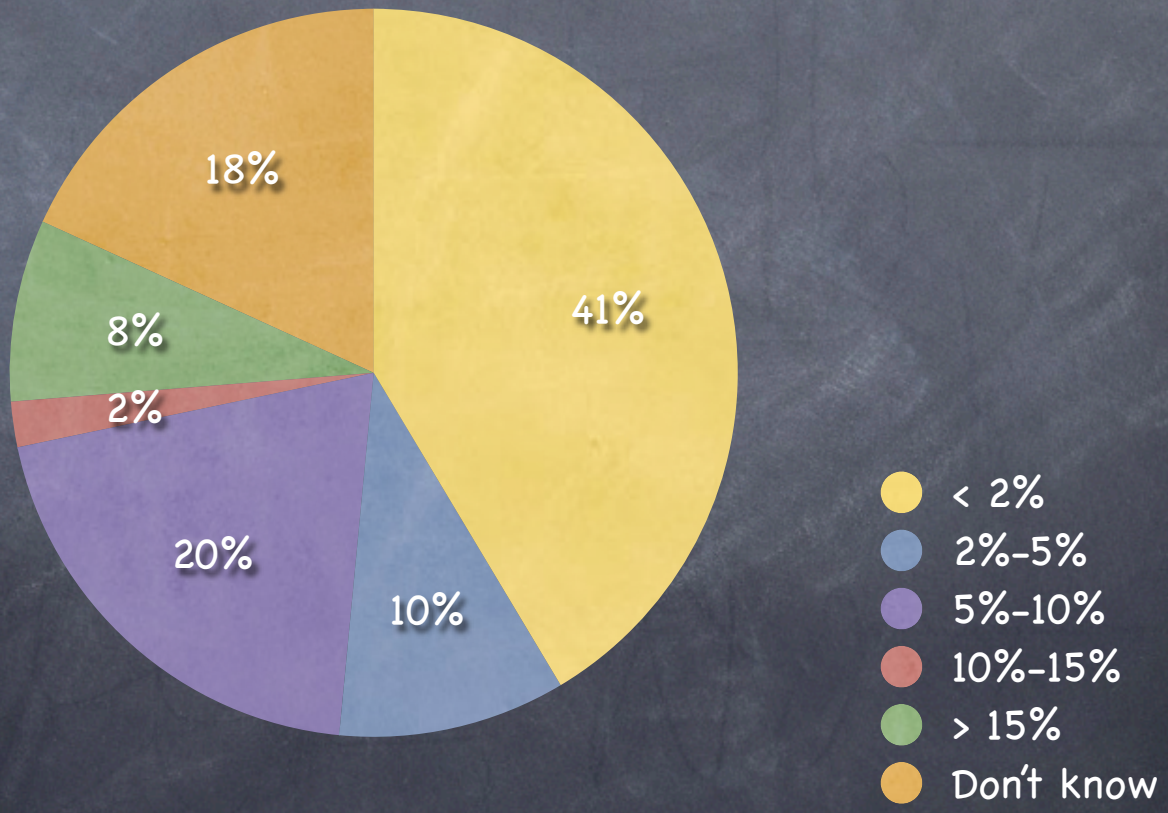
Number of Employees



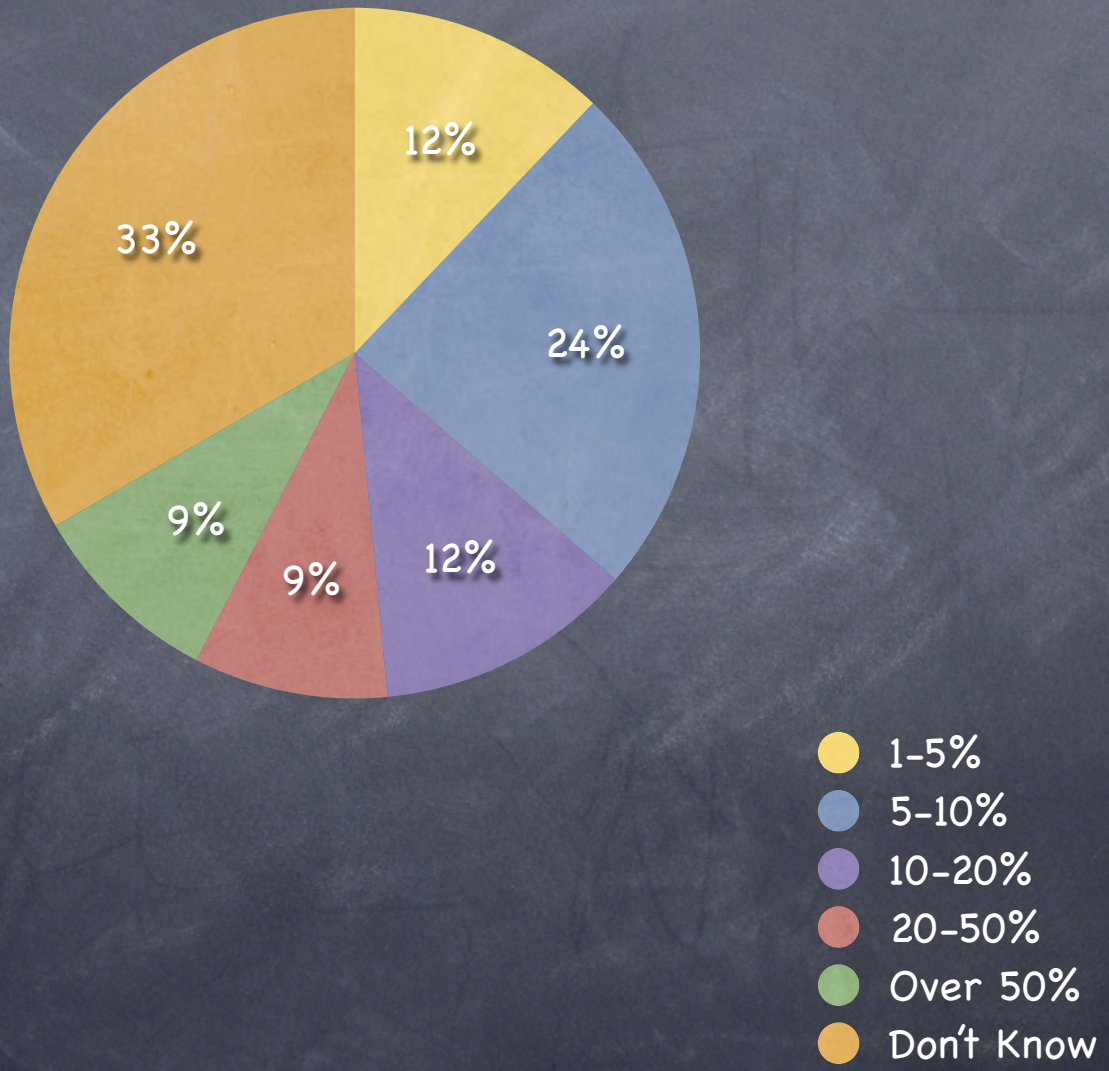
Annual Revenue



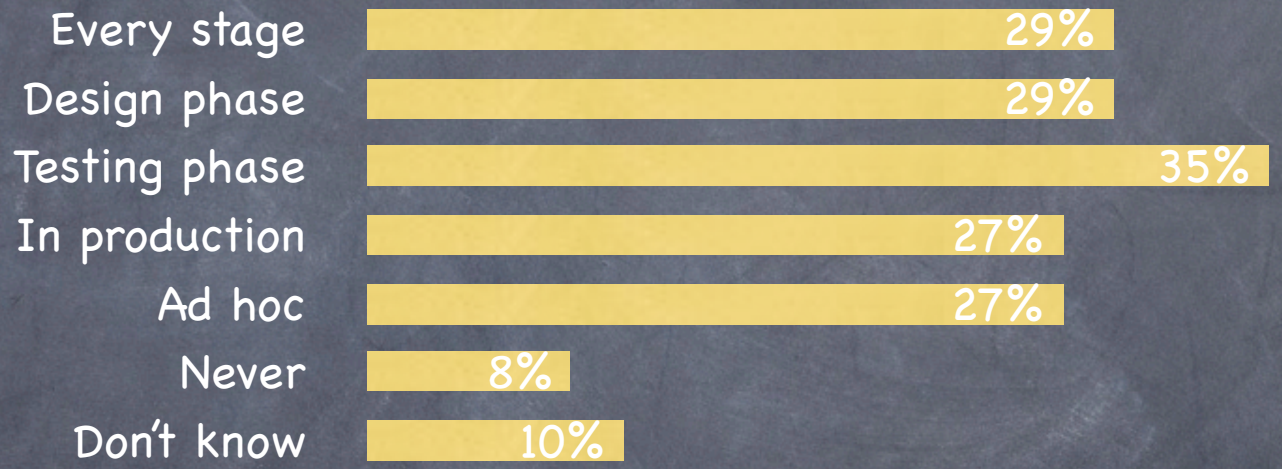
Percentage of Development Headcount Spent On Security



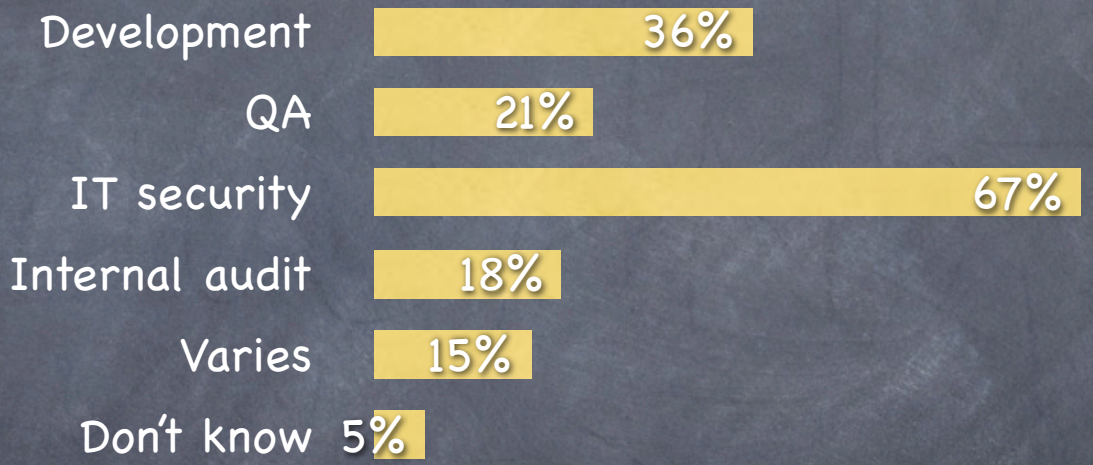
Percentage IT Budget on Web App Security



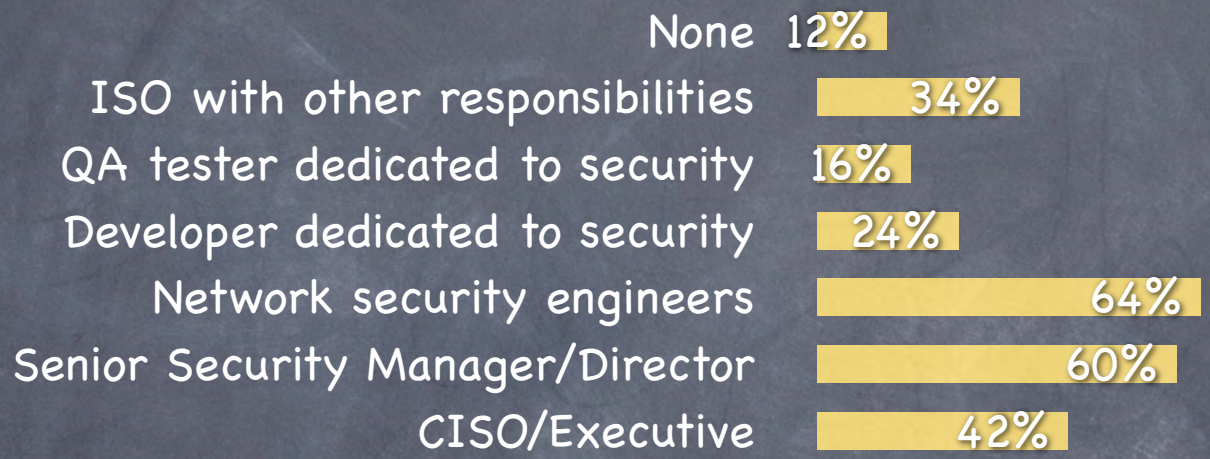
Security Checkpoints



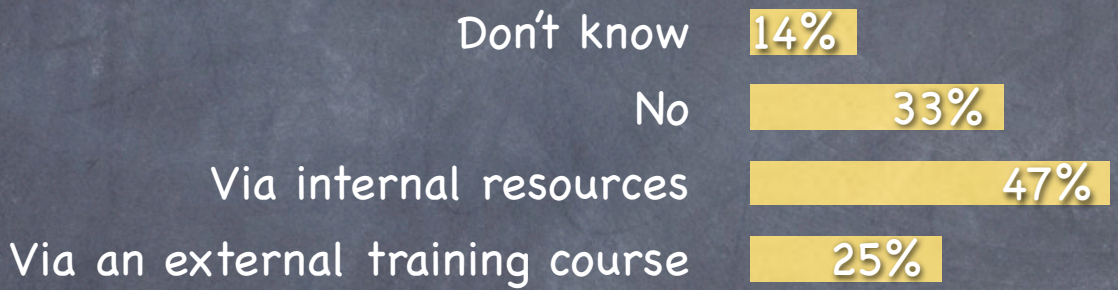
Organizational Responsibility For Security Reviews



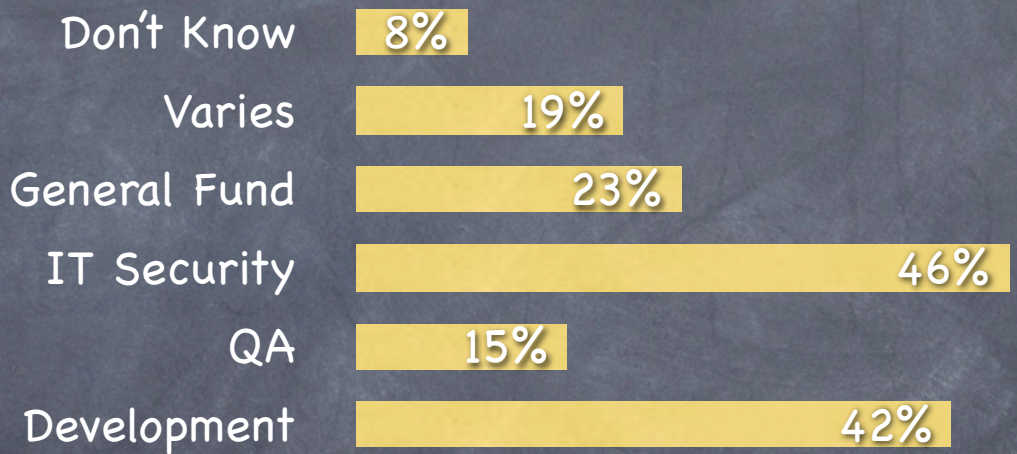
Personnel


None 12%
ISO with other responsibilities 34%
QA tester dedicated to security 16%
Developer dedicated to security 24%
Network security engineers 64%
Senior Security Manager/Director 60%
CISO/Executive 42%

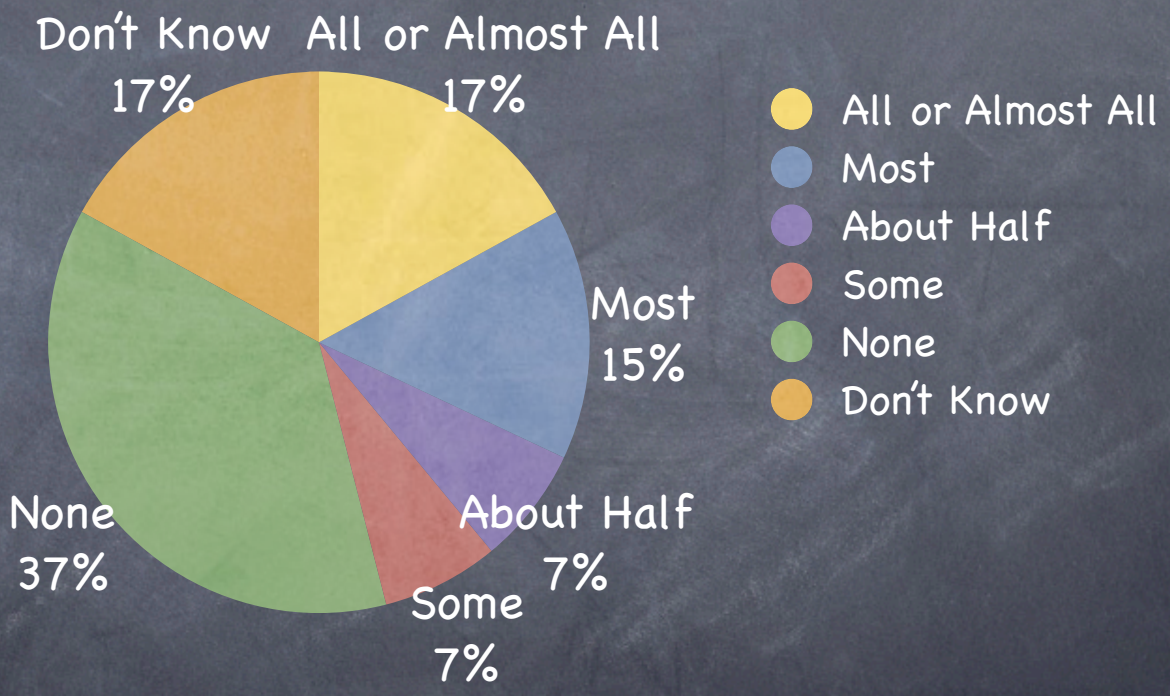
Provide developers with training



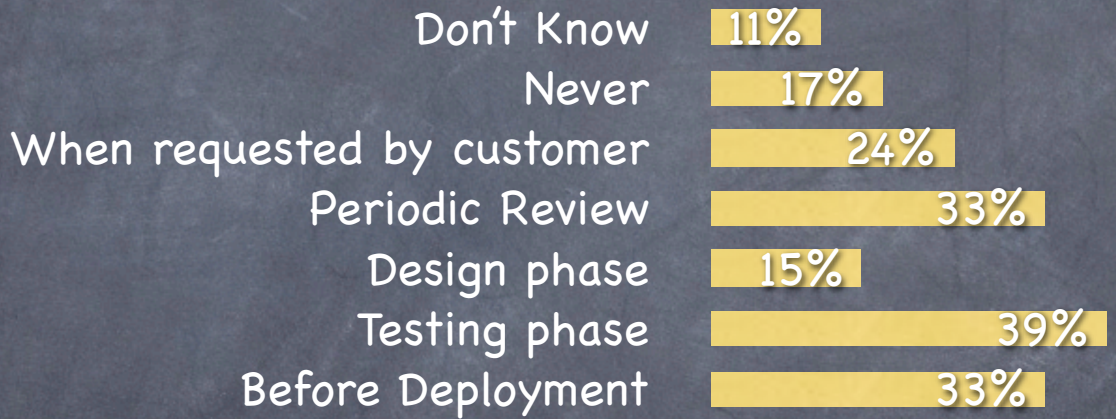
Budget for training costs



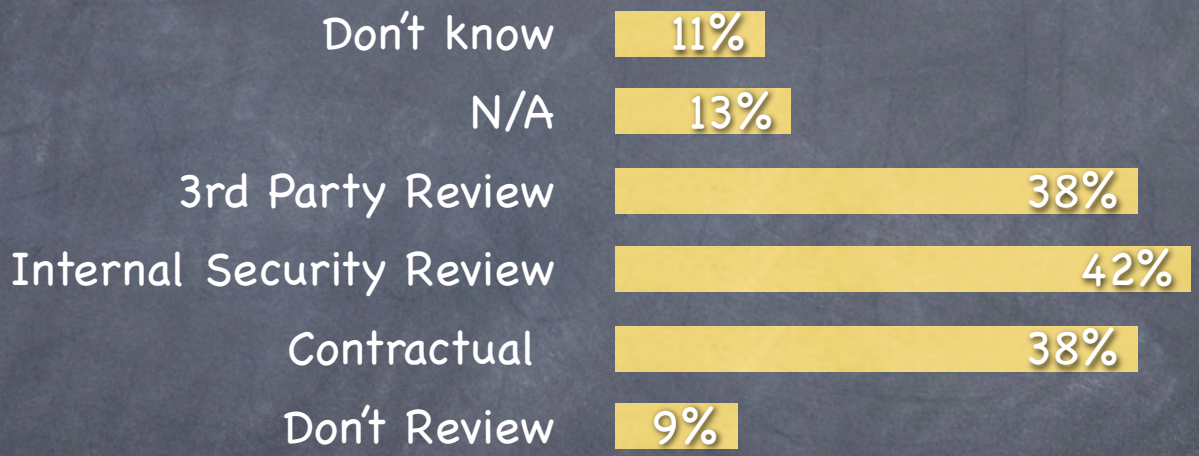
Percentage of Applications Organizations Defend with Web Application Firewalls



Third Party Security Reviews

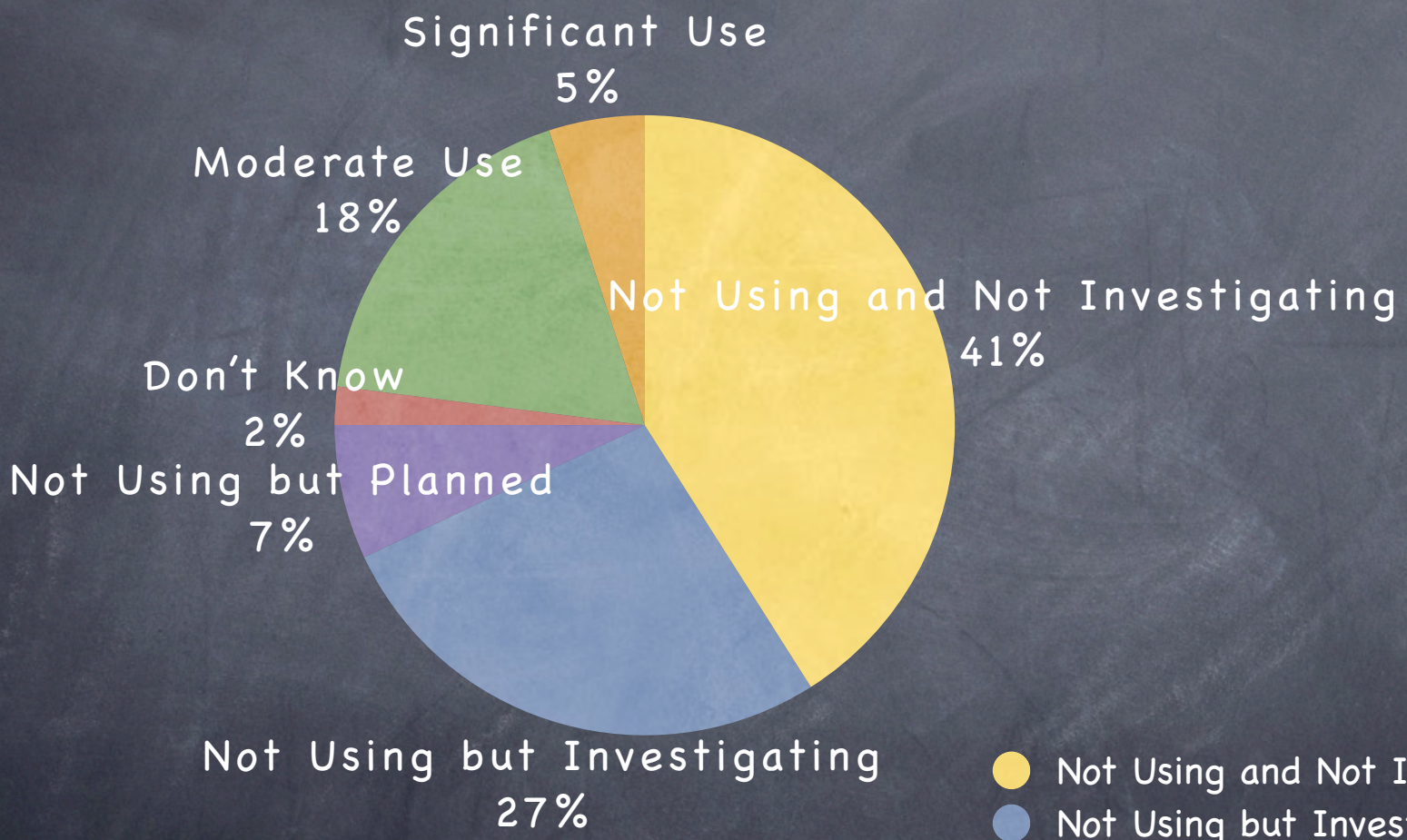


Ways of Reviewing Outsourced Code

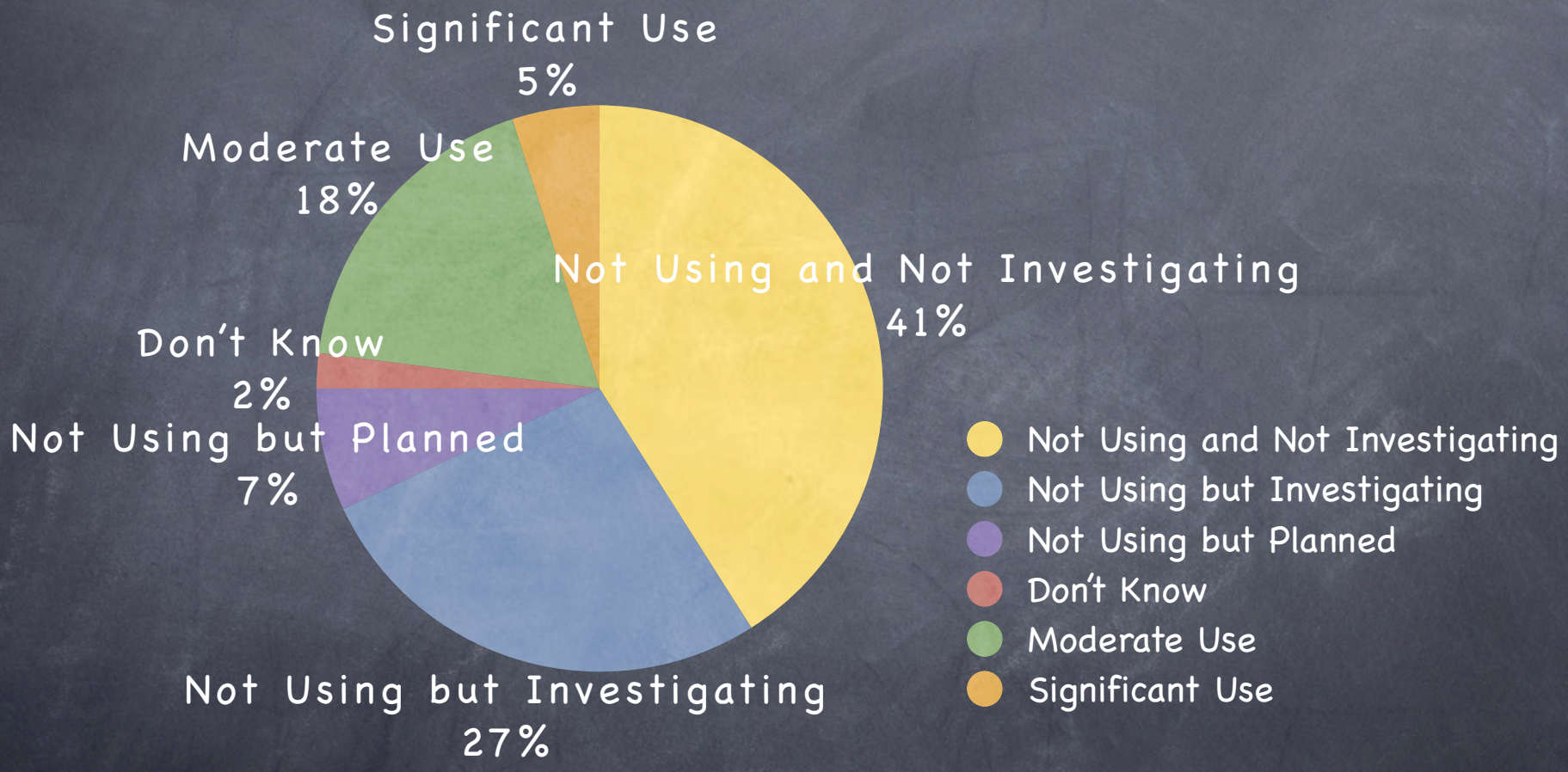


- Organizations that have suffered a public data breach spend more on security in the development process than those that have not.
- Web application security spending is expected to either stay flat or increase in nearly two thirds of companies.
- Half of respondents consider security experience important when hiring developers, and a majority provide their developers with security training. 38% have a third party firm conduct a security review of outsourced code.
- At least 61% of respondents perform an independent third party security review before deploying a Web application while 17% do not (the remainder do not know or do so when requested by customers).
- Just under half of the surveyed organizations have Web application firewalls deployed for at least some of their Web applications.

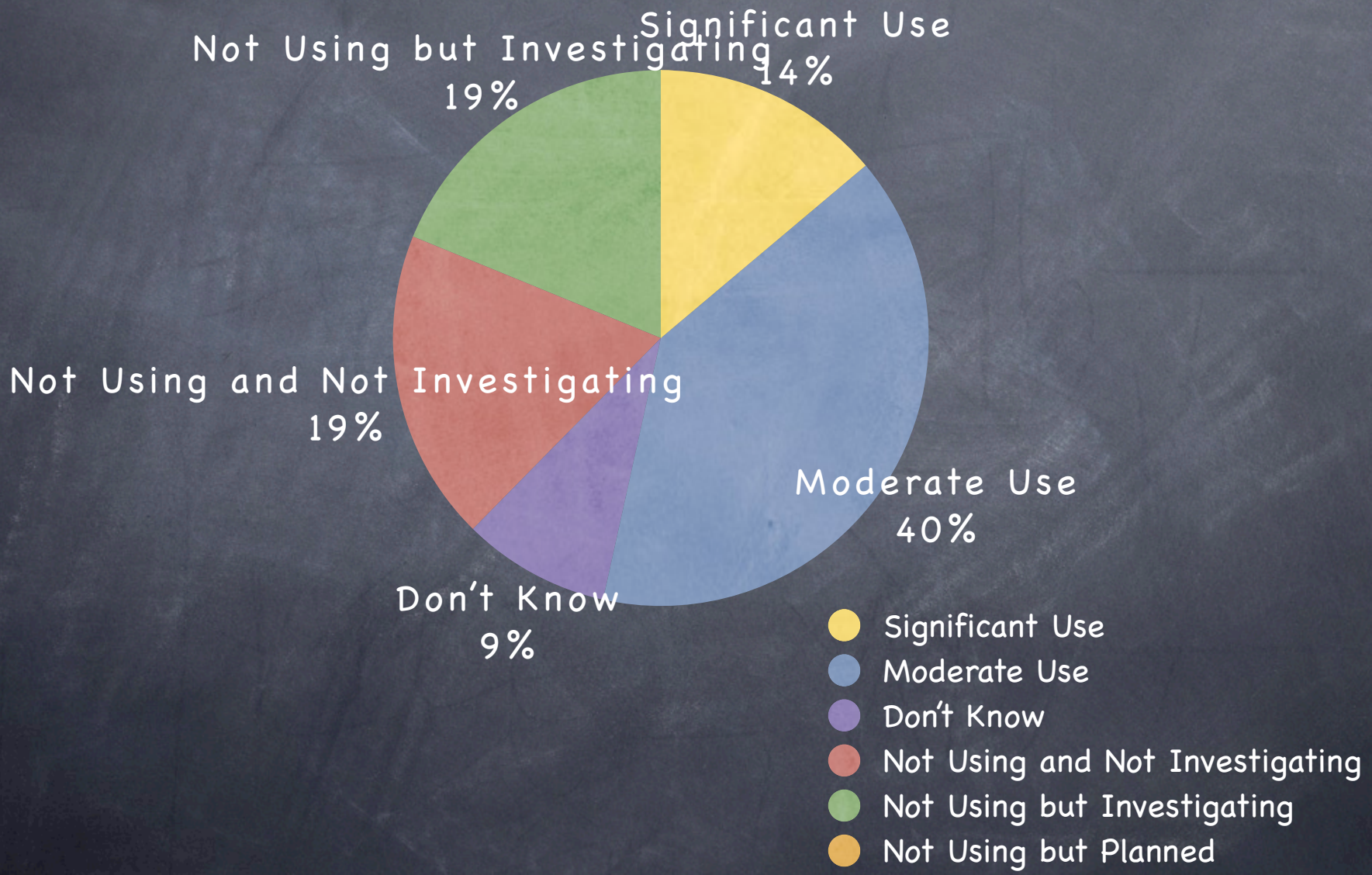
IaaS


Significant Use
5%
Moderate Use
18%
Not Using and Not Investigating
41%
Don't Know
2%
Not Using but Planned
7%
Not Using but Investigating
27%
Not Using and Not Investigating
Not Using but Investigating
Not Using but Planned
Don't Know
Moderate Use
Significant Use

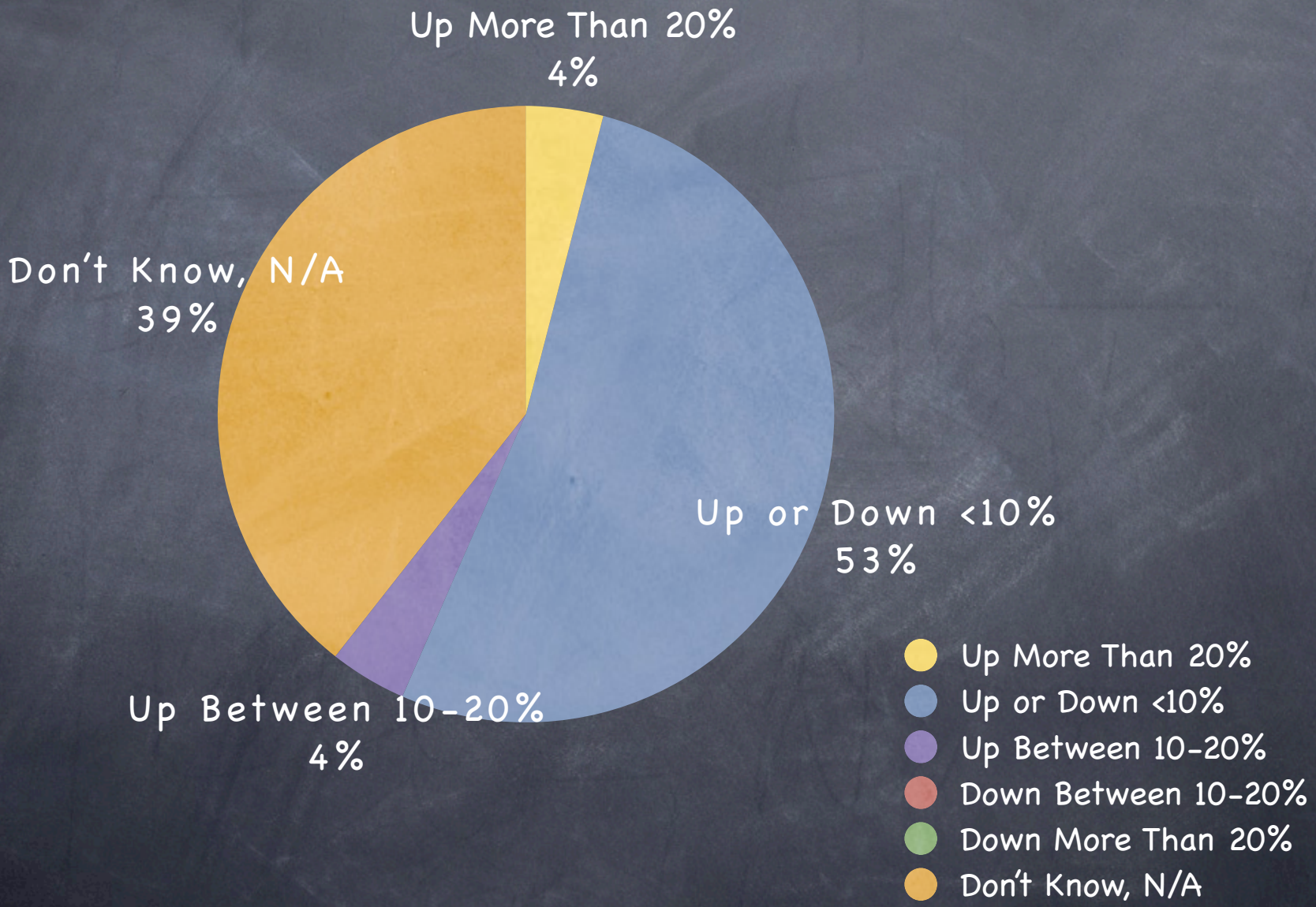
PaaS


Significant Use
5%
Moderate Use
18%
Not Using and Not Investigating
41%
Don't Know
2%
Not Using but Planned
7%
Not Using but Investigating
27%
Not Using and Not Investigating
Not Using but Investigating
Not Using but Planned
Don't Know
Moderate Use
Significant Use

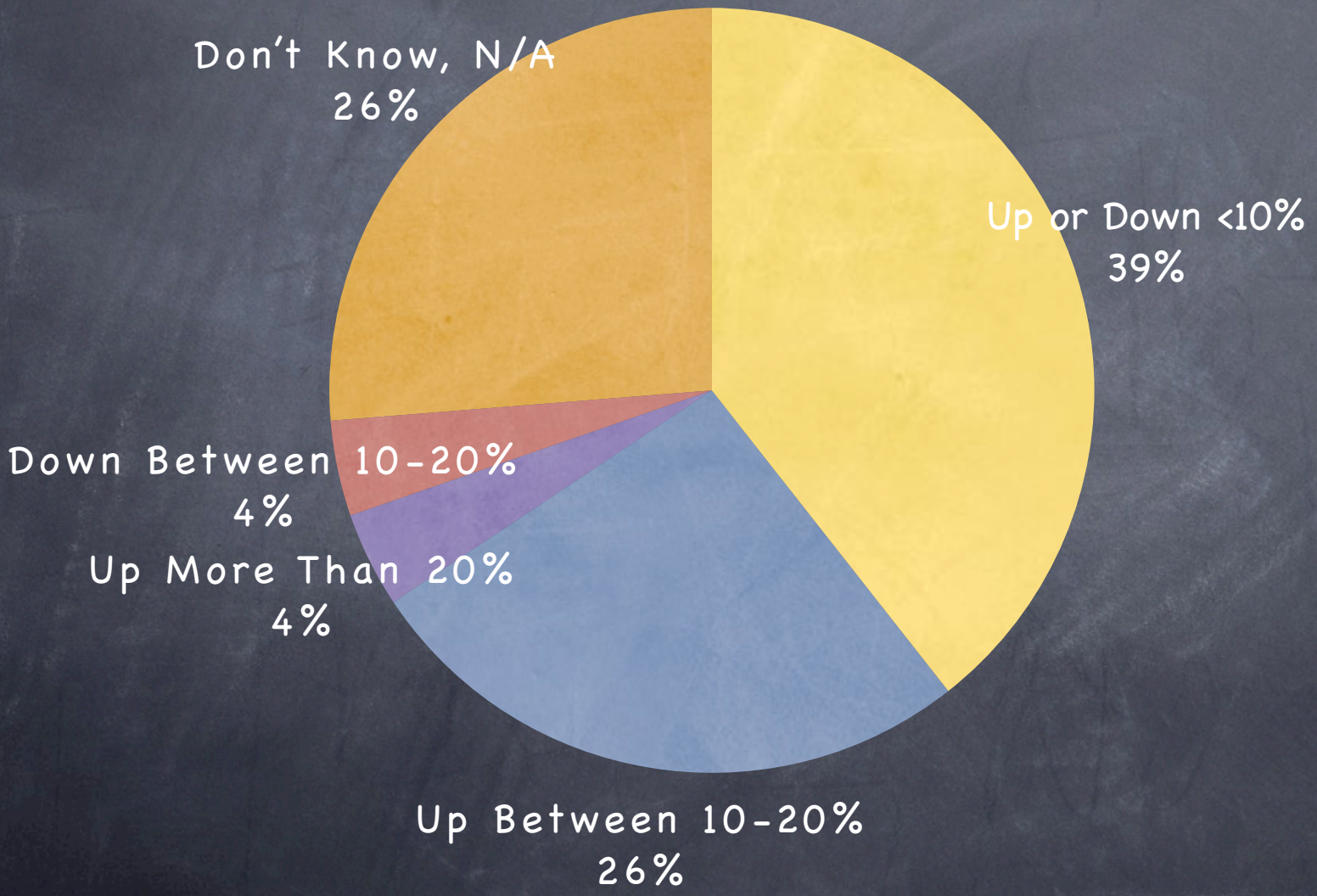
SaaS


Significant Use
14%
Not Using but Investigating
19%
Not Using and Not Investigating
19%
Moderate Use
40%
Don't Know
9%
Significant Use
Moderate Use
Don't Know
Not Using and Not Investigating
Not Using but Investigating
Not Using but Planned

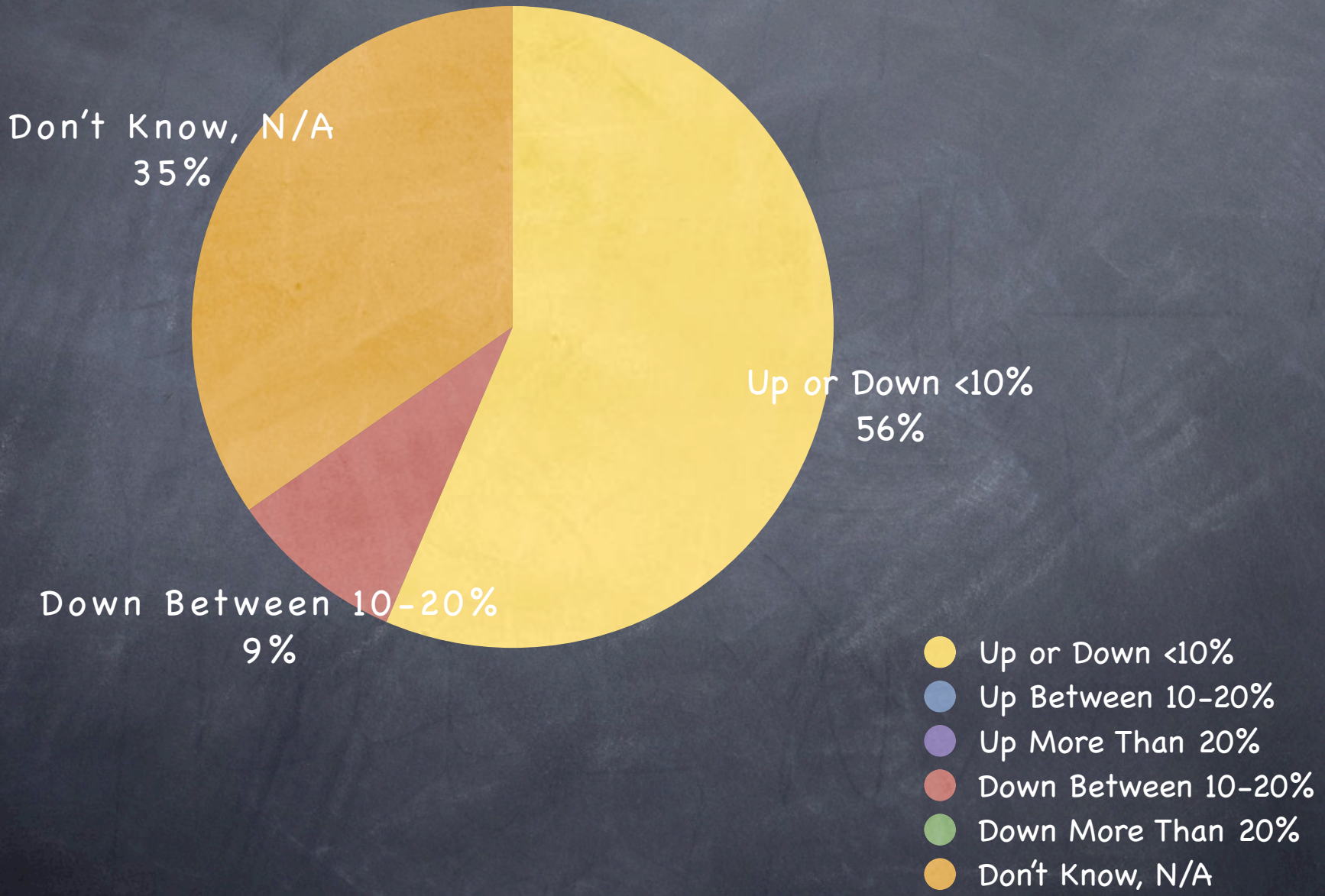
SaaS - Spending Changes on Network Security



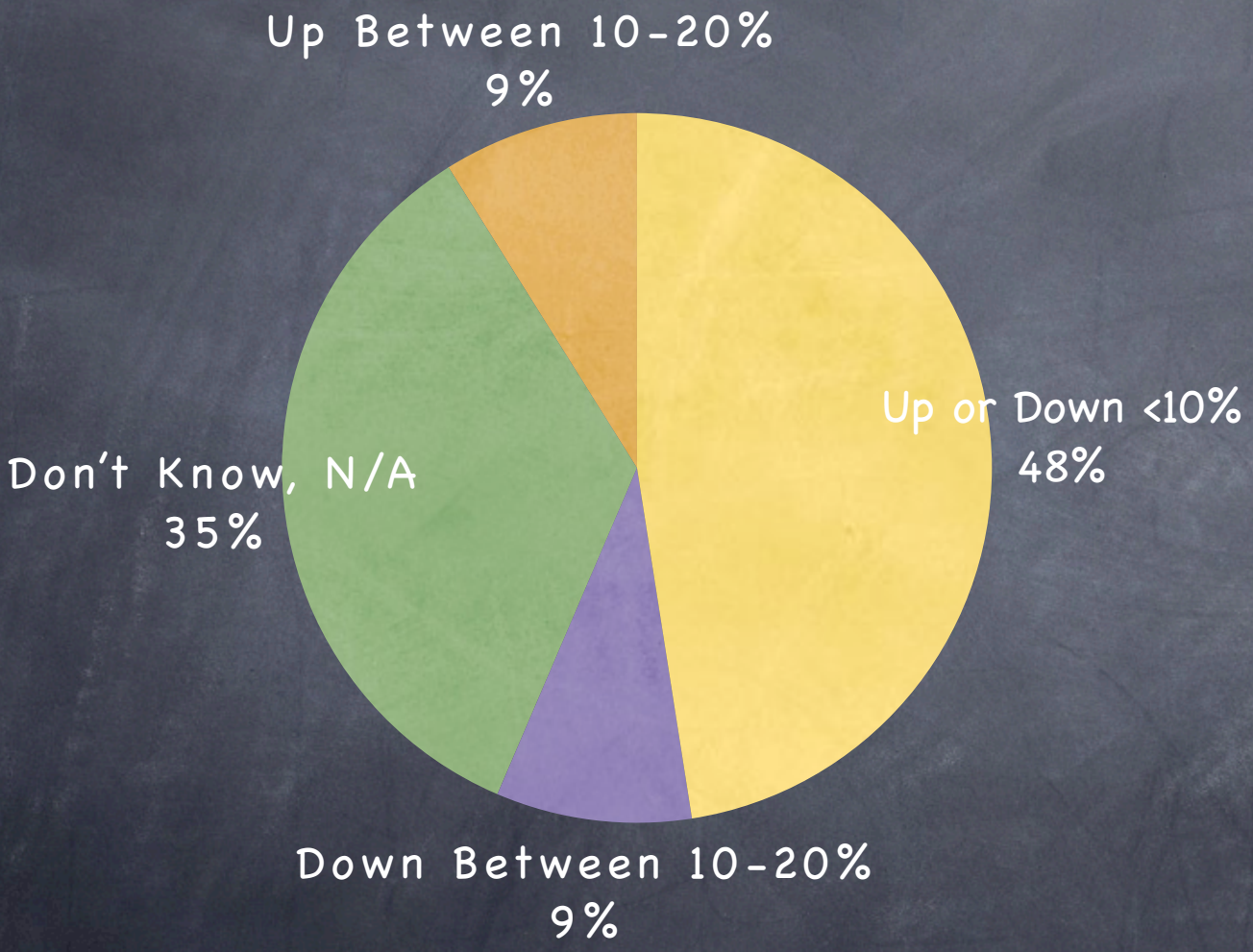
SaaS Spending Changes - Third Party Security Reviews



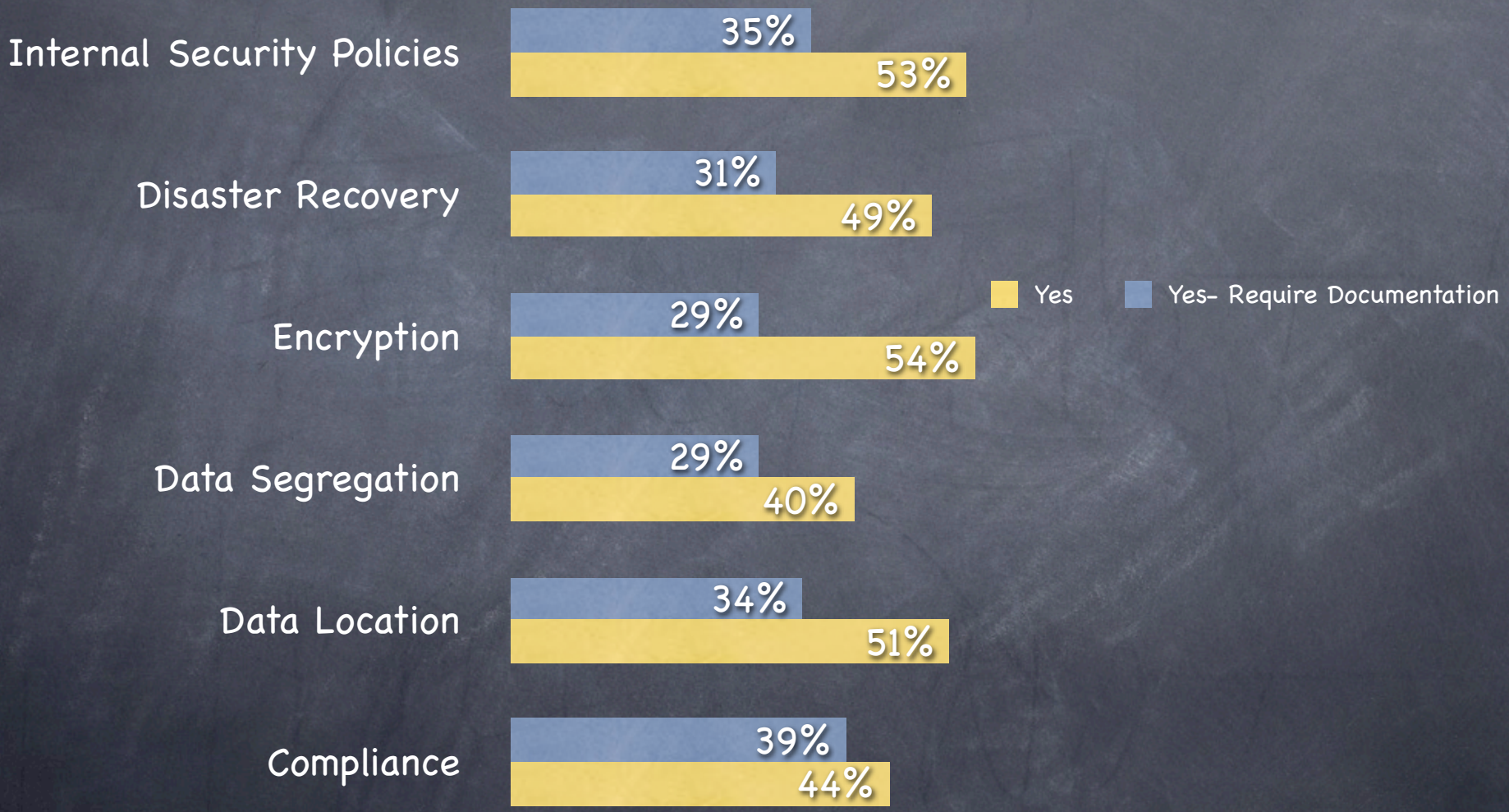
SaaS Spending Changes - Security Personnel



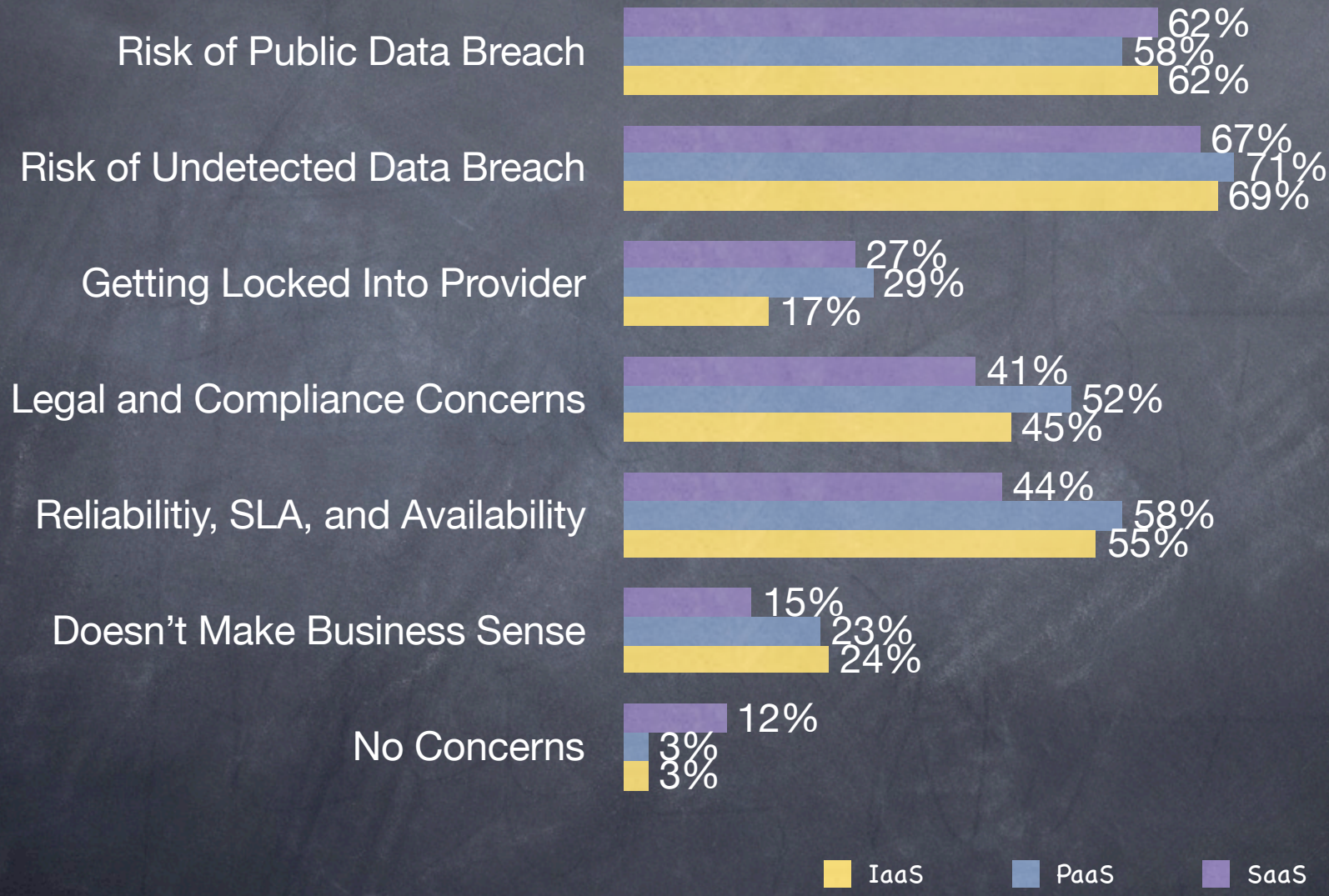
SaaS Spending Changes - Identity Management



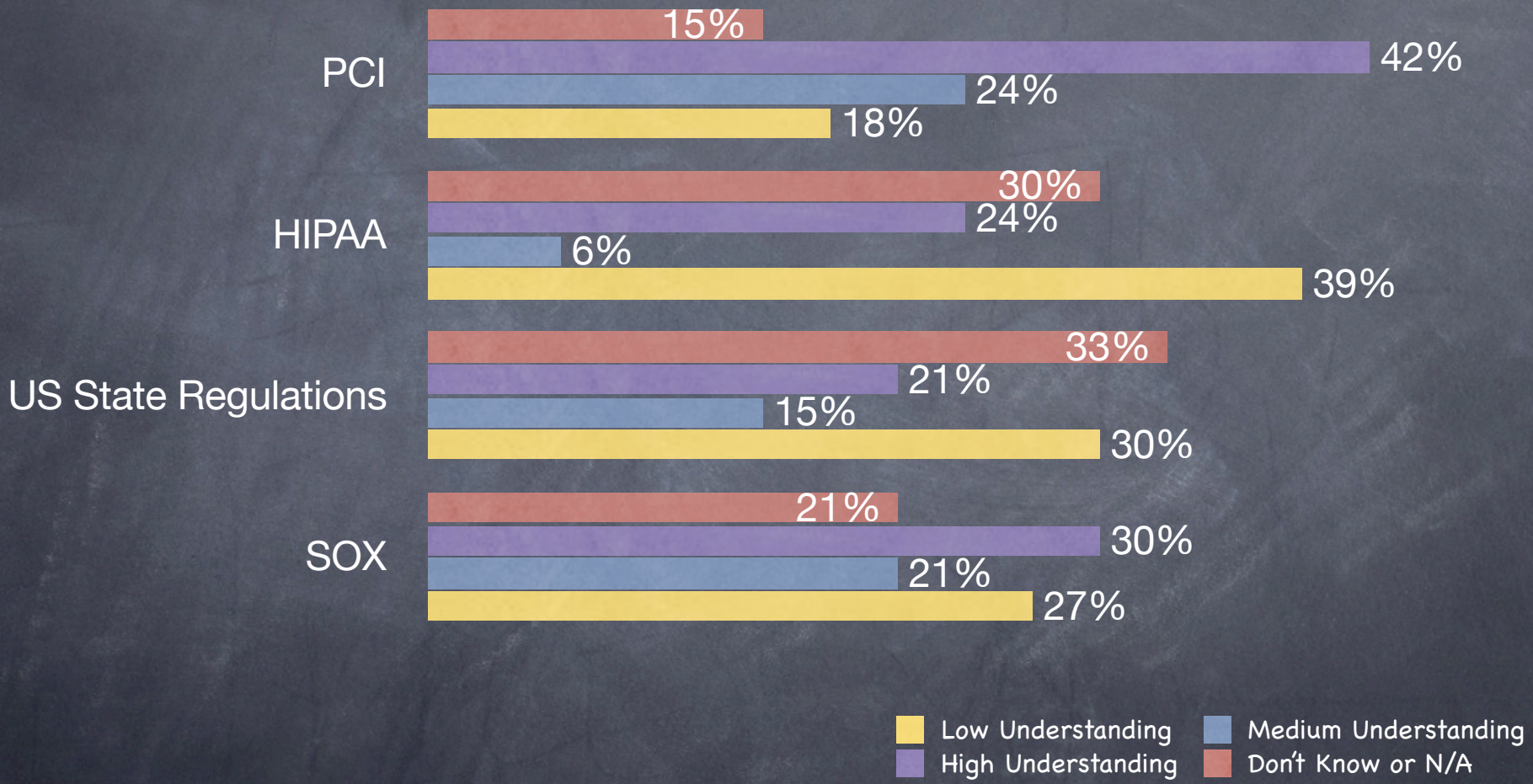
Inquire About Issue With Third Party



Concerns with Cloud Computing



Level of Understanding Cloud Computing



Cloud Summary

- Software-as-a-Service is in much greater use than Infrastructure-as-a-Service or Platform-as-a-Service.
- Security spending does not change significantly as a result of cloud computing
- Organizations are not doing their homework when it comes to cloud security.
- The risk of an undetected data breach is the greatest concern with using cloud computing, closely followed by the risk of a public data breach.
- Compliance and standards requirements related to cloud computing are not well understood.

- Currently collecting responses for the third survey.
- Partners assist in promoting survey, analyzing results, and providing strategic input.
- Current status of project can always be found on OWASP website.
- New partners are always welcome.