



# PCI DSS Survey

## Results

Cisco Security Solutions Marketing  
January 2011

# Table of Contents

Methodology	3
Summary of Findings	5
Detailed Findings	6
Study Team Contact Information	21
Addendum: Elaboration on Key Findings	23

# Methodology

## Timing, Sample Qualifications and Analysis

- This report includes findings from 500 IT security decision makers /influencers (ITDMs) who completed an online survey from November 23, to December 1, 2010
- Respondents were screened to ensure a sample of IT professionals who:
  - Work in Healthcare (n=100), Finance (n=100), Retail (n=100), Education (n=100) or Government (n=100)
  - Have at least some role in setting corporate security policies and/or making security-related IT purchase decisions for their company's network
  - Are involved with their organizations' PCI compliance efforts
  - Are based in the US at organizations with 100 or more employees

# Additional Respondent Profile Information

- 71% of respondents indicated their organizations have been under PCI DSS for more than four years
  - And nearly half have been under PCI compliance since it was announced five years ago
- 17% are Level 1 merchants and 55% are Level 2 or Level 3
- More than half (56%) are primary decision makers within their organizations
- About half (49%) work at organizations with 1000+ employees worldwide

# Summary of Findings

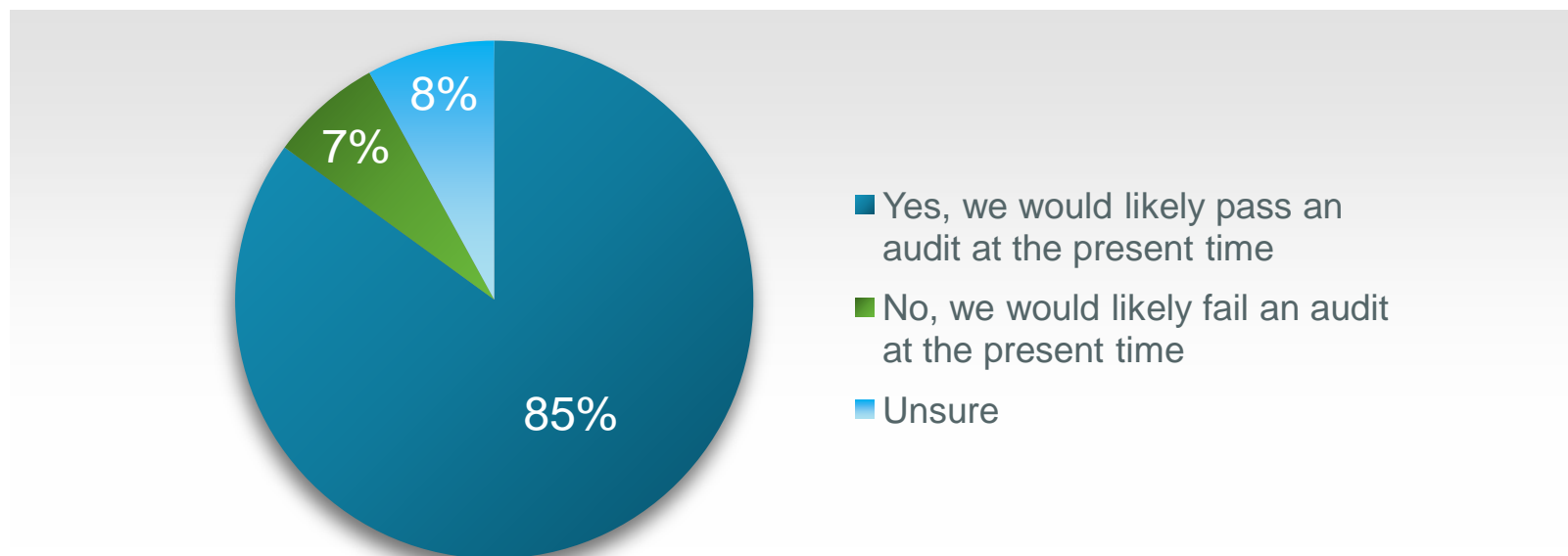
- Organizations have taken significant steps to achieve PCI compliance and believe their current infrastructures would pass assessments.
- Organizations believe they are more secure than they would be if PCI compliance were not required and feel PCI is necessary for protecting cardholder data
- PCI compliance projects can drive or fund other network and information security projects.
- Most organizations plan to increase PCI compliance spending in 2011 including investments to comply with evolving PCI requirements for virtualized environments.
- Educating employees on the proper handling of cardholder data remains the biggest challenge – with regard to PCI compliance – organizations face.

# Detailed Findings

The vast majority (85%) of ITDMs are comfortable that their existing network infrastructure would pass an assessment today for PCI compliance.

## Level of Comfort with Current PCI Compliance

Among IT Security Decision Makers/Influencers  
(Total, n=500)



Q13. Would you be comfortable with your existing network infrastructure if you were to be assessed today for PCI compliance?

Seven in ten ITDMs feel their organization is more secure than it would be if PCI compliance were not required.

### Attitudes Toward Requiring PCI Compliance

Among IT Security Decision Makers/Influencers  
(Total, n=500)

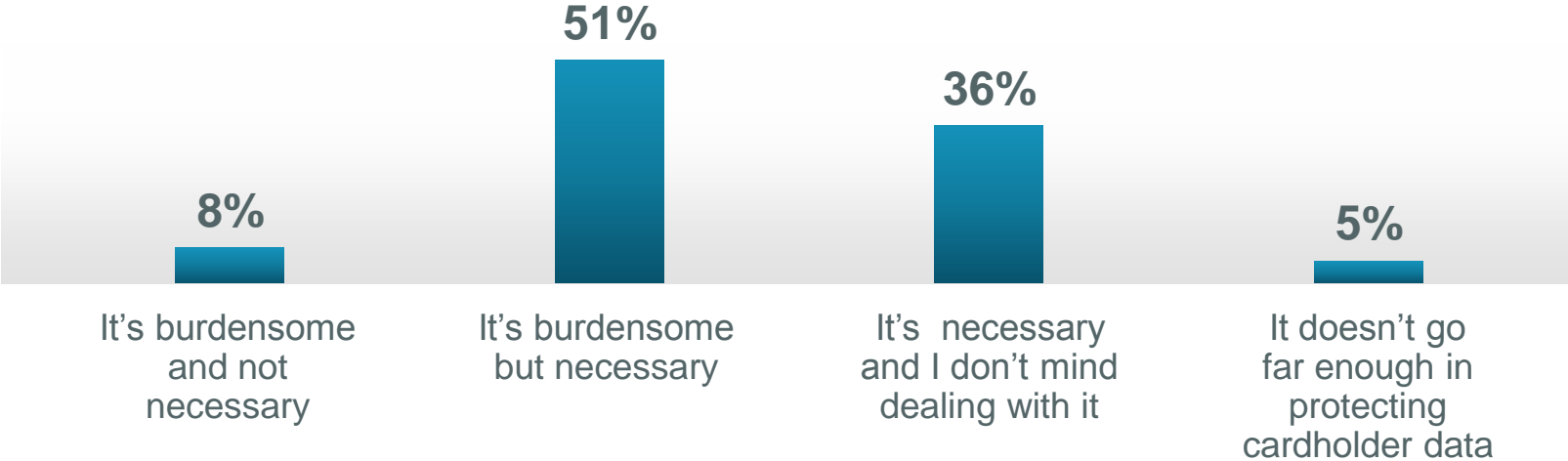


Q14. Do you feel your organization is more secure than it would be if PCI compliance were not required?

# 87% of ITDMs indicate PCI compliance is necessary.



## General Sentiment Regarding PCI Compliance Among IT Security Decision Makers/Influencers (Total, n=500)

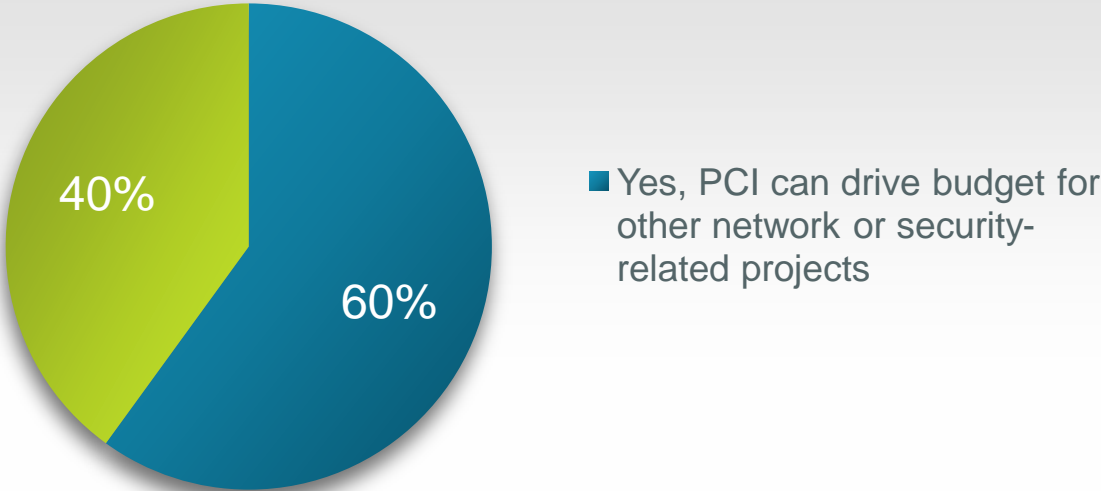


Q15. What is your general sentiment regarding PCI compliance?

Six in ten ITDMs indicate PCI can drive budget for other network or security-related projects.



**Leveraging PCI Compliance Projects**  
Among IT Security Decision Makers/Influencers  
(Total, n=500)

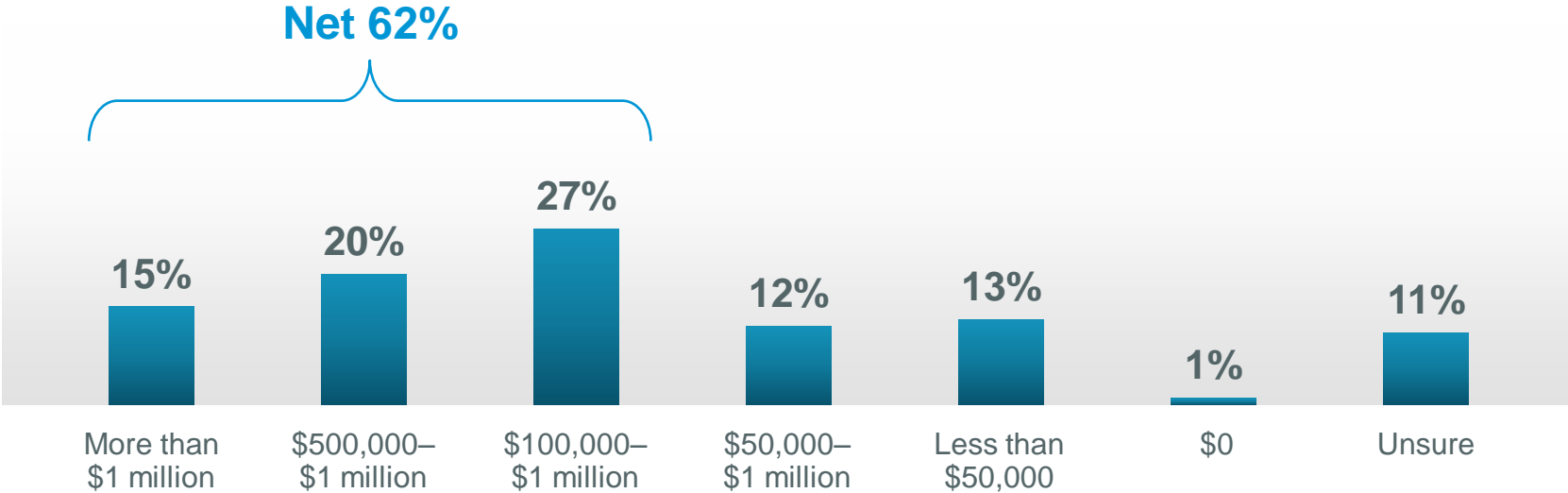


**Q31. Do you leverage PCI compliance projects to drive or fund your other network or network security projects?**

More than six in ten ITDMs estimate their organization has spent \$100K or more on PCI compliance in the last five years.

### Five Year Spending on PCI Compliance

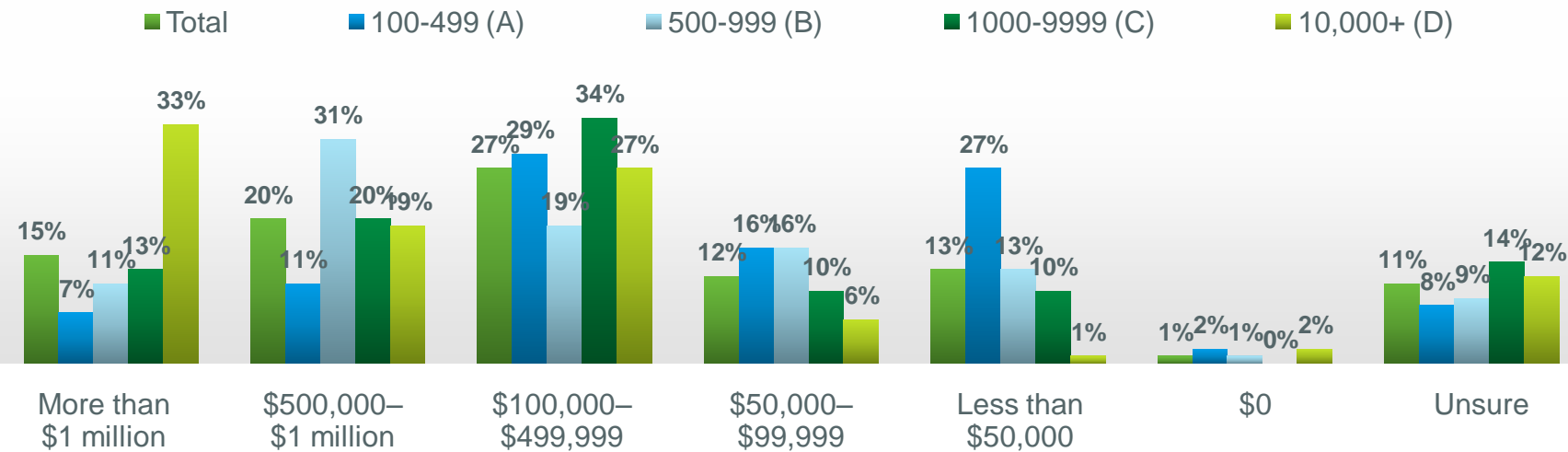
Among IT Security Decision Makers/Influencers  
(Total, n=500)



Q28. How much do you estimate your organization has spent on PCI compliance in the last five years?

Over the past five years, larger companies tend to have spent more on PCI compliance compared to smaller companies.

### Five Year Spending on PCI Compliance Among IT Security Decision Makers/Influencers (By Organization Size)



Q28. How much do you estimate your organization has spent on PCI compliance in the last five years?

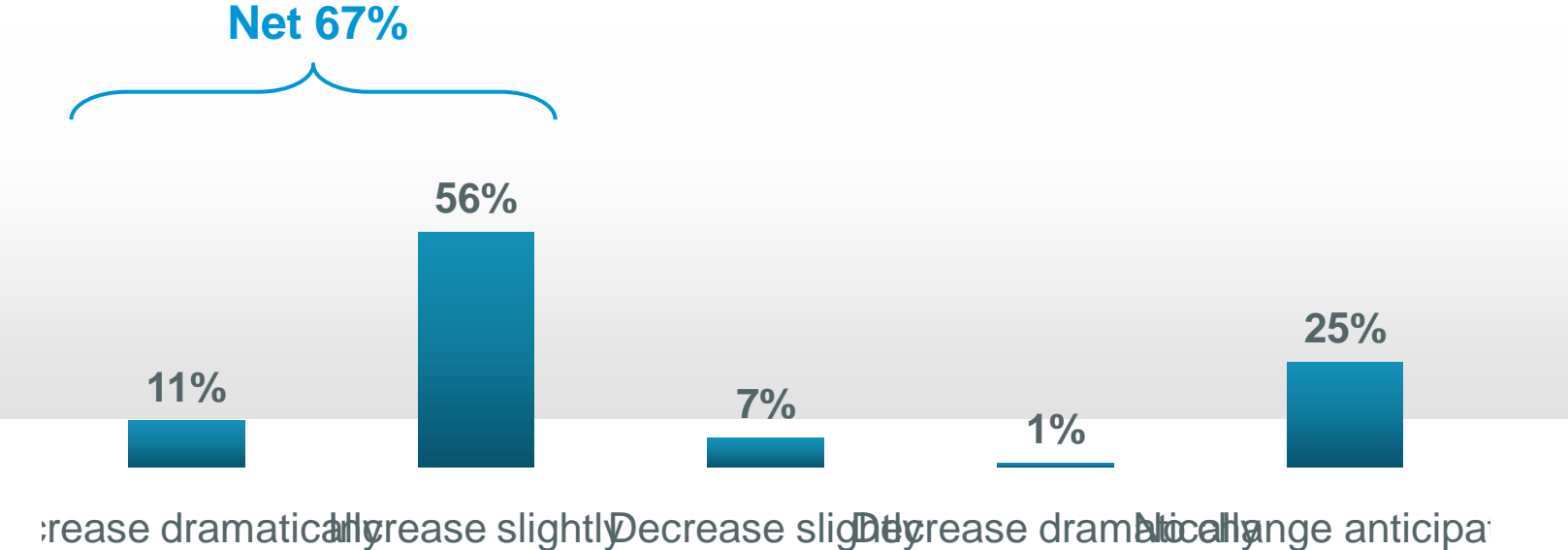
Base: Total, n=500; 100-499, n=132; 500-999, n=121; 1000-9,999, n=136; 10,000+, n=111

A/B/C/D/E indicate significant differences at the 95% confidence level.

Most ITDMs (67%) think their spending on PCI compliance will increase in the next year.



### Changes in PCI Compliance Spending Among IT Security Decision Makers/Influencers (Total, n=500)

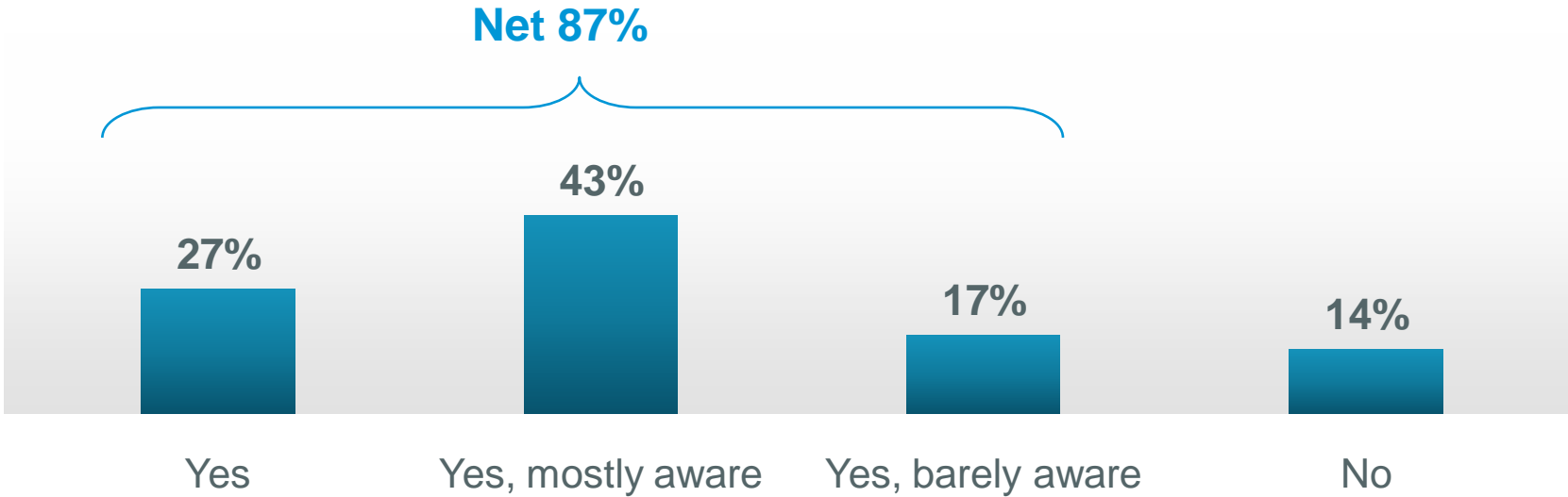


Q30. Do you think your spending on PCI compliance will increase or decrease in the next year?

The vast majority of ITDMs (87%) are at least somewhat aware of the clarifications and recommendations associated with the newly announced PCI DSS 2.0 standards.



**Awareness of PCI DSS 2.0 Standards**  
Among IT Security Decision Makers/Influencers  
(Total, n=500)

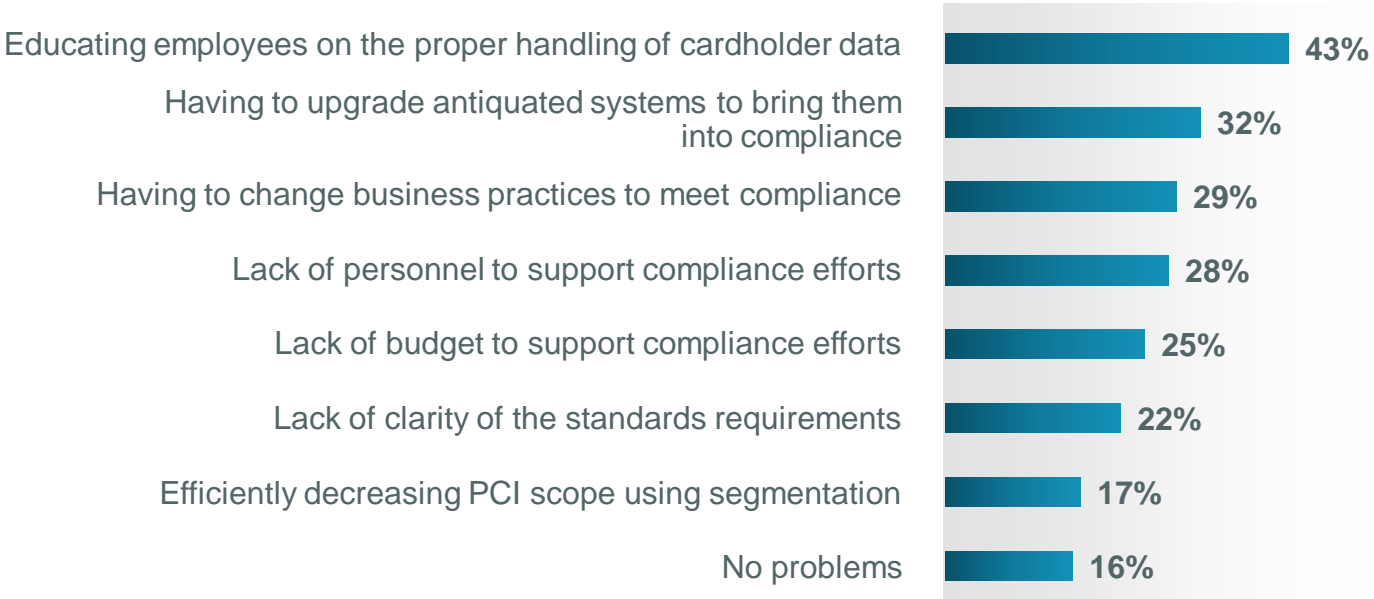


Q21. Are you aware of the clarifications and recommendations associated with the newly announced PCI DSS 2.0 standards?

Educating employees on the proper handling of cardholder data and having to upgrade antiquated systems are the leading problems ITDMs experience regarding PCI compliance.

### Challenges to PCI Compliance

Among IT Security Decision Makers/Influencers  
(Total, n=500)

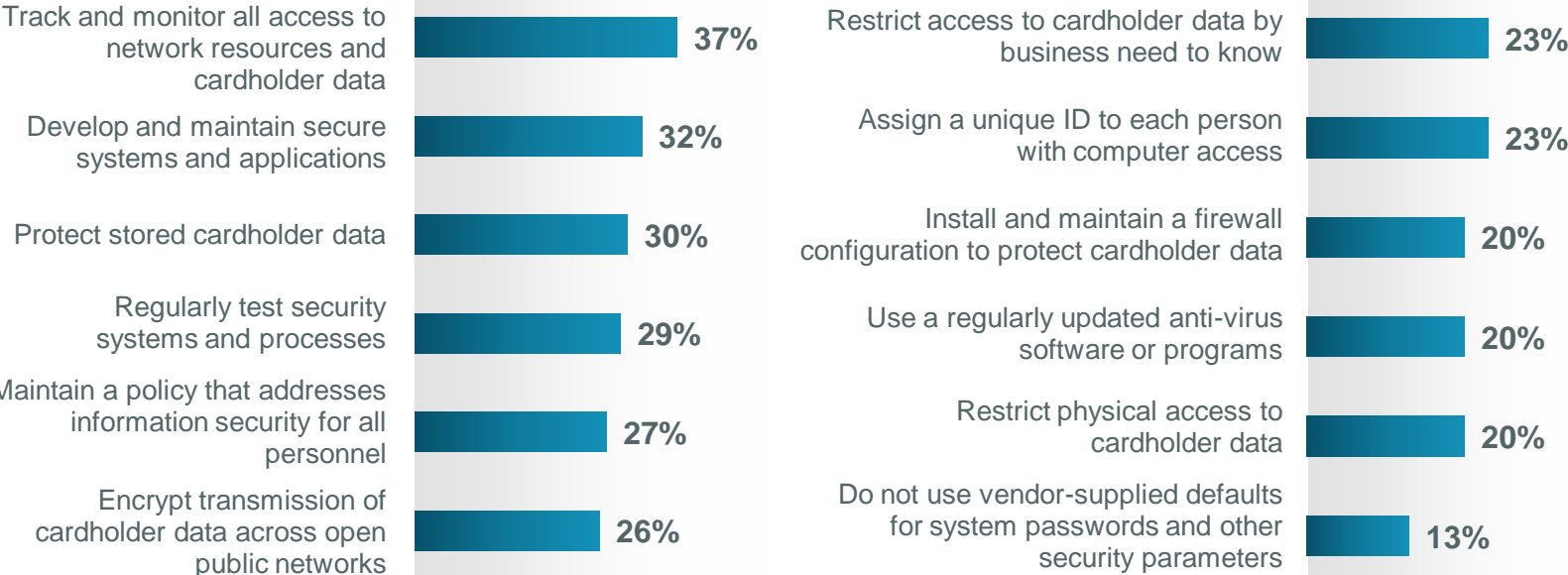


Q33. What problems are you experiencing with regard to PCI compliance? Check all that apply.

# Organizations are not particularly troubled by specific PCI requirements suggesting that the requirements are considered reasonable.



## PCI Requirements Causing The Most Issues Among IT Security Decision Makers/Influencers (Total, n=500)

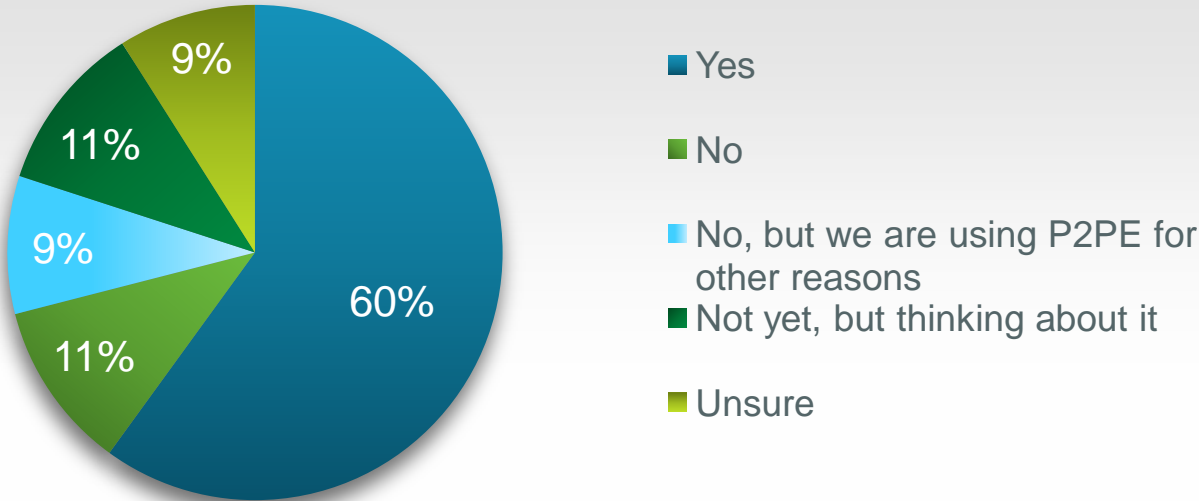


Q35. Of the twelve PCI requirements, which do you feel cause the most issues for achieving or maintaining compliance? (Please select the top three)

Six in ten ITDMs are using point to point encryption (P2PE) to simplify their compliance efforts and possibly reduce the scope of their next PCI assessment.

### Use of P2PE to Simplify Compliance Efforts

Among IT Security Decision Makers/Influencers  
(Total, n=500)



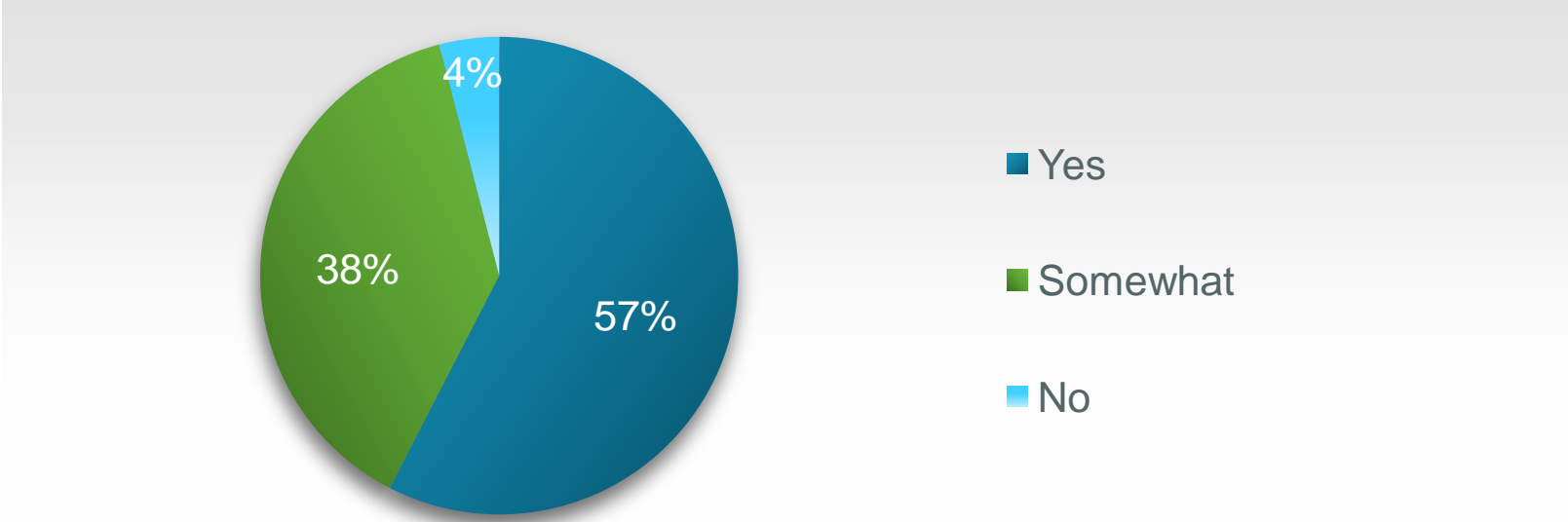
Q27. Are you using point to point encryption (P2PE) to simplify your compliance efforts and possibly reduce the scope of your next PCI audit?

# More than half of ITDMs are satisfied with their current virtualization security posture.



## Satisfaction with Virtualization Security Posture

Among IT Security Decision Makers/Influencers  
(Total, n=500)

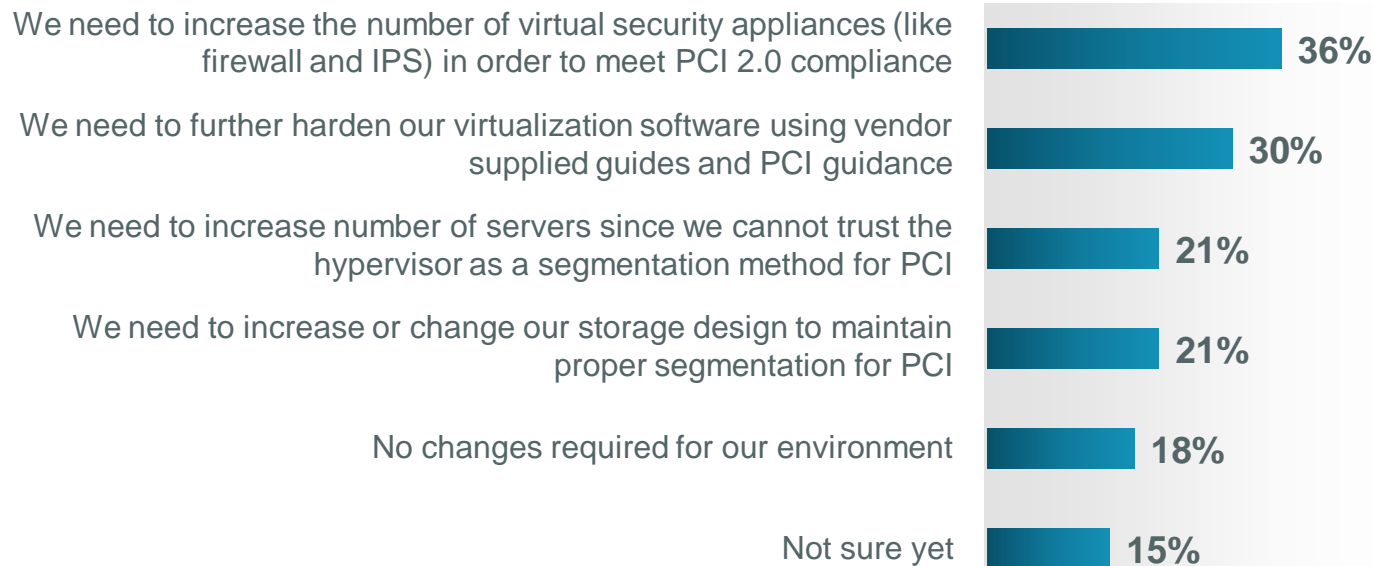


Q22. Virtual environments have been identified in the PCI 2.0 standard as “system components” that must be secured. Are you satisfied with your current virtualization security posture?

More than one in three ITDMs anticipate needing to increase the number of virtual security appliances (like firewall and IPS) in order to meet PCI 2.0 compliance.

### Changing to Meet PCI Compliance

Among IT Security Decision Makers/Influencers  
(Total, n=500)

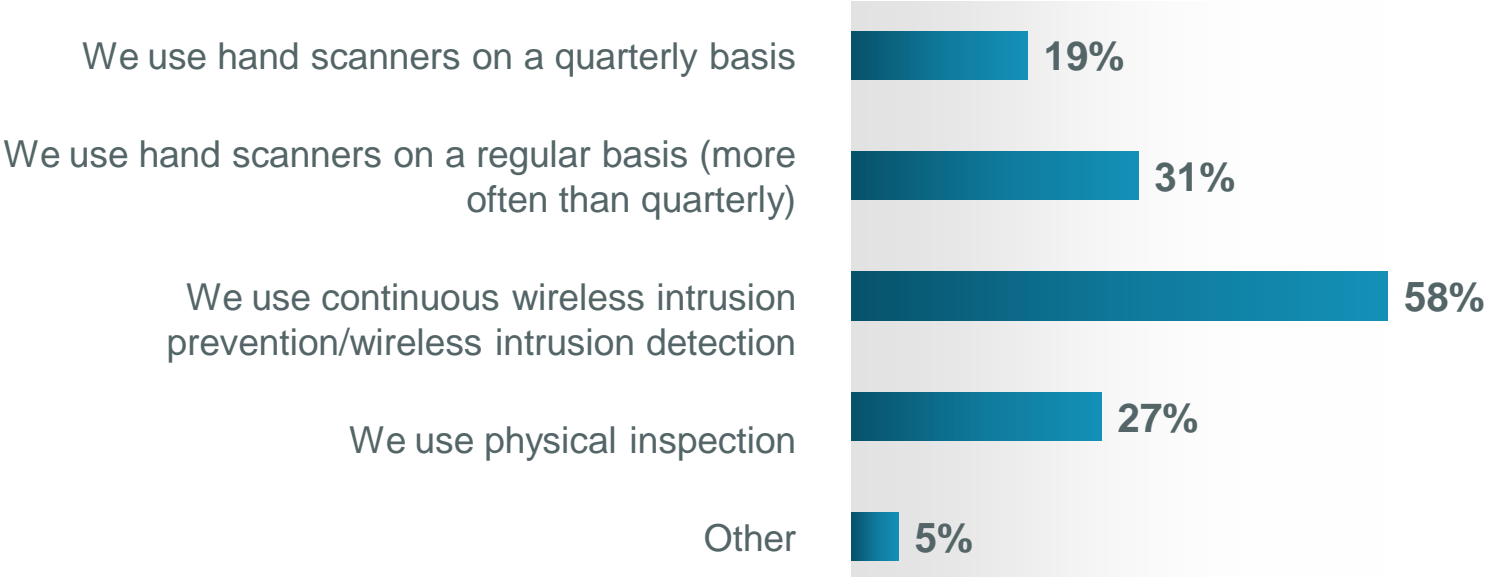


**Q23. How do you anticipate needing to change your virtual environment to meet PCI compliance? Please check all that apply.**

# Nearly six in ten ITDMs use continuous wireless intrusion prevention/wireless intrusion detection to uncover wireless rogue access.



## Detecting Wireless Rogue Access Among IT Security Decision Makers/Influencers (Total, n=500)



Q25. How do you detect wireless rogue access? Please check all that apply.

Thank you.

Contact Info:

**Fred Kost**

Marketing Director, Security Solutions  
408 853 6098  
frkost@cisco.com

**Chris Barker**

PR Manager  
206 256 3067  
chrbarke@cisco.com



# Addendum: Elaboration on Key Findings

# Key Findings

## Attitudes Toward PCI Compliance

- ITDMs (85%) tend to be comfortable with their existing network infrastructure and feel they would pass a PCI assessment at the present time—particularly those in the Finance (92%) and Retail (92%) industries
  - Relative to other ITDMs, a significantly larger proportion who work in Government (17%) are unsure if they would pass an assessment.
- Most IT Security Decision Makers (70%) feel their organization is more secure than it would be if PCI compliance were not required, driven by nearly four in ten (38%) who feel ‘much more secure’
  - Retail and Finance ITDMs indicate the strongest feeling of security as a result of PCI compliance—50% indicate their organization is ‘much more secure’ because of compliance
- The vast majority (87%) of ITDMs indicate that PCI compliance is necessary
- With similar attitudes across industries, most ITDMs indicate that other regulations /laws/ standards enhance (43%) or that they both enhance or inhibit (42%) their ability to be compliant

# Key Findings

## Activities to Promote PCI Compliance

- About one quarter (26%) of ITDMs resource PCI compliance efforts using outsourced experts/consultants, while more than four in ten (42%) ITDMs use in-house staff
- Nearly half (45%) of ITDMs use EMV (Europay, MasterCard and VISA, the global standard for inter-operation) to reduce fraud in face-to-face transaction environments. Roughly one in four (23%) are not using EMV yet, but are thinking about it
  - Use of EMV to reduce fraud in face-to-face transaction environments tends to be driven by Finance (60%) and Retail (51%) ITDMs, compared to other industries
- Six in ten ITDMs (60%) are using point to point encryption (P2PE) to simplify their compliance efforts and possibly reduce the scope of their next PCI audit
- ITDMs tend to uncover wireless rogue access through continuous wireless intrusion prevention/wireless intrusion detection (58%)
- 81% retain documentation that shows how PCI DSS scope was determined and keep the results for assessor review

# Key Findings

## New Standards: PCI DSS 2.0 and Changing Needs

- ITDMs tend to indicate a strong level of awareness of the clarifications and recommendations associated with the newly announced PCI DSS 2.0 standards—particularly those in Finance and Retail

A considerable proportion of ITDMs in Government are unaware of the clarifications and recommendations associated with the newly announced PCI DSS 2.0 standards

- More than half (57%) of ITDMs, including a significant proportion of those in Finance (70%), are satisfied with their current virtualization security posture

- ITDMs tend to indicate the need to increase the number of virtual security appliances (like firewall and IPS) in order to meet PCI 2.0 compliance (36%) or further harden their virtualization software using vendor supplied guides and PCI guidance (30%)

Relative to other industries, considerable proportions of ITDMs in Education (19%) and Government (20%) are not sure how to change their virtual environment to meet PCI compliance

# Key Findings

## Organizational Spending on PCI Compliance

- More than one third of ITDMs indicate their organization spent \$500K or more on PCI compliance in the past five years
  - This organizational spending tends to be driven by the financial industry, followed by retail, as well as larger organizations
  - Education, healthcare and government tend to spend less on PCI compliance
- With little variation across industries, most ITDMs (67%) indicate their organization's spending on PCI compliance will increase over the next 12 months
- Six in ten ITDMs, driven by a significant proportion of those in finance, indicate PCI can drive budget for other network or security-related projects

# Key Findings

## Challenges to PCI Compliance

- The leading problem ITDMs in healthcare, finance, retail and education experience with regard to PCI compliance is educating employees on the proper handling of cardholder data
  - ITDMs in government indicate that lack of budget to support compliance efforts is their #1 problem
- The #1 PCI requirement that causes the most issues for maintaining compliance it:
  - In Healthcare and Finance: “Track and monitor all access to network resources and cardholder data”
  - In Education and Government: “Develop and maintain secure systems and applications”
  - In Retail: “Protect stored cardholder data”