Understanding Your Data Flow

Using Tokenization to Secure Data

Ulf Mattsson

CTO Protegrity

Follow us @ISACANews
#NACACS

VOLUME 6, 2011

ISACA® Journal

Emerging and Evolving IT Risk

Feature

Ulf Mattsson is the chief technology officer of Protegrity, a leader in enterprise data security management, where he created the architecture of the Protegrity Data Security Platform. He is considered one of the founding fathers

Choosing the Most Appropriate Data Security Solution for an Organization

With the rising cost and increasing frequency of data security breaches, companies are starting to reevaluate how they protect their data. External

to put in the time and effort necessary to access sensitive data.

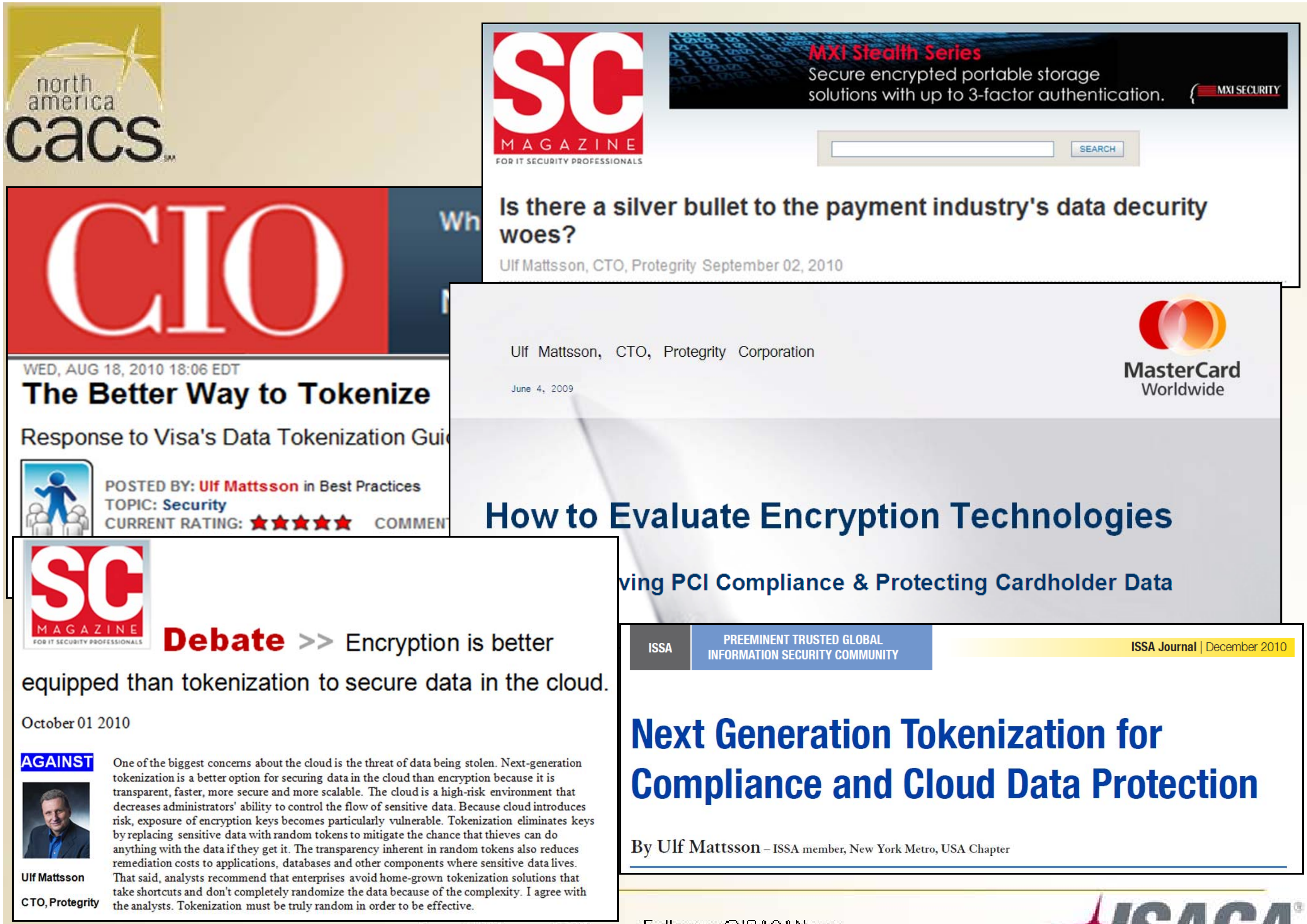
Staying ahead of the bad guys is not an easy

ISACA online conferences

Enterprise Data Protection -
Understanding Your Options
and Strategies

Ulf Mattsson

north america cacs



SC MAGAZINE FOR IT SECURITY PROFESSIONALS

SEARCH

Is there a silver bullet to the payment industry's data decurity woes?

Ulf Mattsson, CTO, Protegrity September 02, 2010

CIO

WED, AUG 18, 2010 18:06 EDT

The Better Way to Tokenize

Response to Visa's Data Tokenization Gui

POSTED BY: Ulf Mattsson in Best Practices
TOPIC: Security
CURRENT RATING: ★★★★★ COMMENT

Ulf Mattsson, CTO, Protegrity Corporation

June 4, 2009

MasterCard Worldwide

How to Evaluate Encryption Technologies

ving PCI Compliance & Protecting Cardholder Data

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Debate >> Encryption is better equipped than tokenization to secure data in the cloud.

October 01 2010

AGAINST

Ulf Mattsson
CTO, Protegrity

One of the biggest concerns about the cloud is the threat of data being stolen. Next-generation tokenization is a better option for securing data in the cloud than encryption because it is transparent, faster, more secure and more scalable. The cloud is a high-risk environment that decreases administrators' ability to control the flow of sensitive data. Because cloud introduces risk, exposure of encryption keys becomes particularly vulnerable. Tokenization eliminates keys by replacing sensitive data with random tokens to mitigate the chance that thieves can do anything with the data if they get it. The transparency inherent in random tokens also reduces remediation costs to applications, databases and other components where sensitive data lives. That said, analysts recommend that enterprises avoid home-grown tokenization solutions that take shortcuts and don't completely randomize the data because of the complexity. I agree with the analysts. Tokenization must be truly random in order to be effective.

ISSA PREEMINENT TRUSTED GLOBAL INFORMATION SECURITY COMMUNITY

ISSA Journal | December 2010

Next Generation Tokenization for Compliance and Cloud Data Protection

By Ulf Mattsson – ISSA member, New York Metro, USA Chapter

twitter

Follow us @ISACANews
#NACACS

ISACA®
Trust in, and value from, information systems

Ulf Mattsson, CTO Protegrity

- 20 years with IBM Development & Global Services
- Started Protegrity 1994
- Inventor of 22 patents – Encryption and Tokenization
- Member of
  - PCI Security Standards Council (PCI SSC)
  - American National Standards Institute (ANSI) X9
  - International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security
  - ISACA (Information Systems Audit and Control Association)
  - Information Systems Security Association (ISSA)
  - Cloud Security Alliance (CSA)

Session topics

- Discuss threats against data
- Review solutions for securing data
  - Evaluate different options for data tokenization and encryption
- Review case studies
  - Discuss how to stay out of scope for PCI DSS
- Review data protection cost efficiency
  - Introduce a business risk approach
- Discuss cloud and outsourced environments

THIEVES ARE STEALING OUR DATA!

Albert Gonzalez
20 Years In US Federal Prison

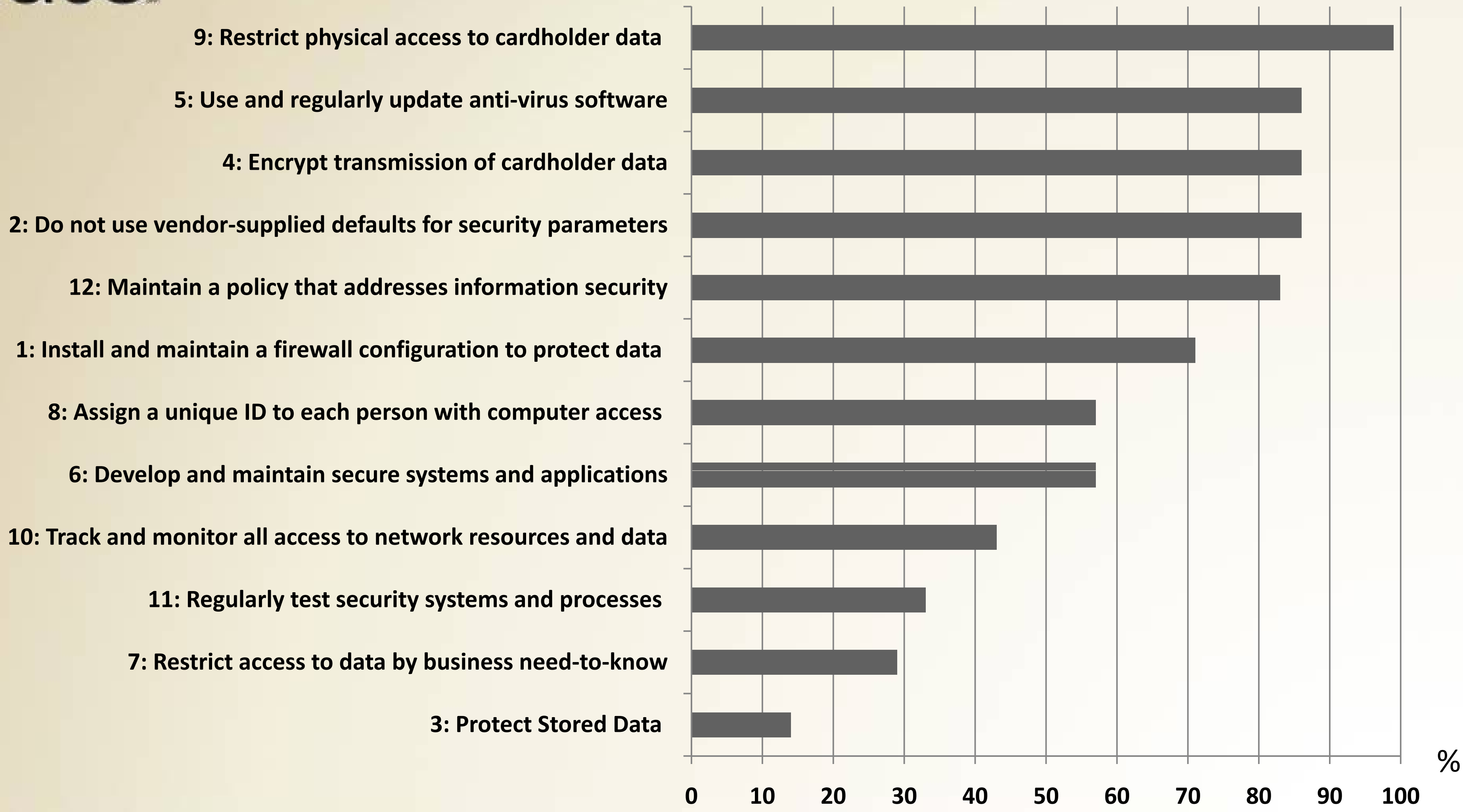
US Federal indictments:

1. Dave & Busters
2. TJ Maxx
3. Heartland HPS
   - Breach expenses $140M

Source: http://en.wikipedia.org/wiki/Albert_Gonzalez

Source: http://www.youtube.com/user/ProtegrityUSA

What about Breaches & PCI?
Was Data Protected?

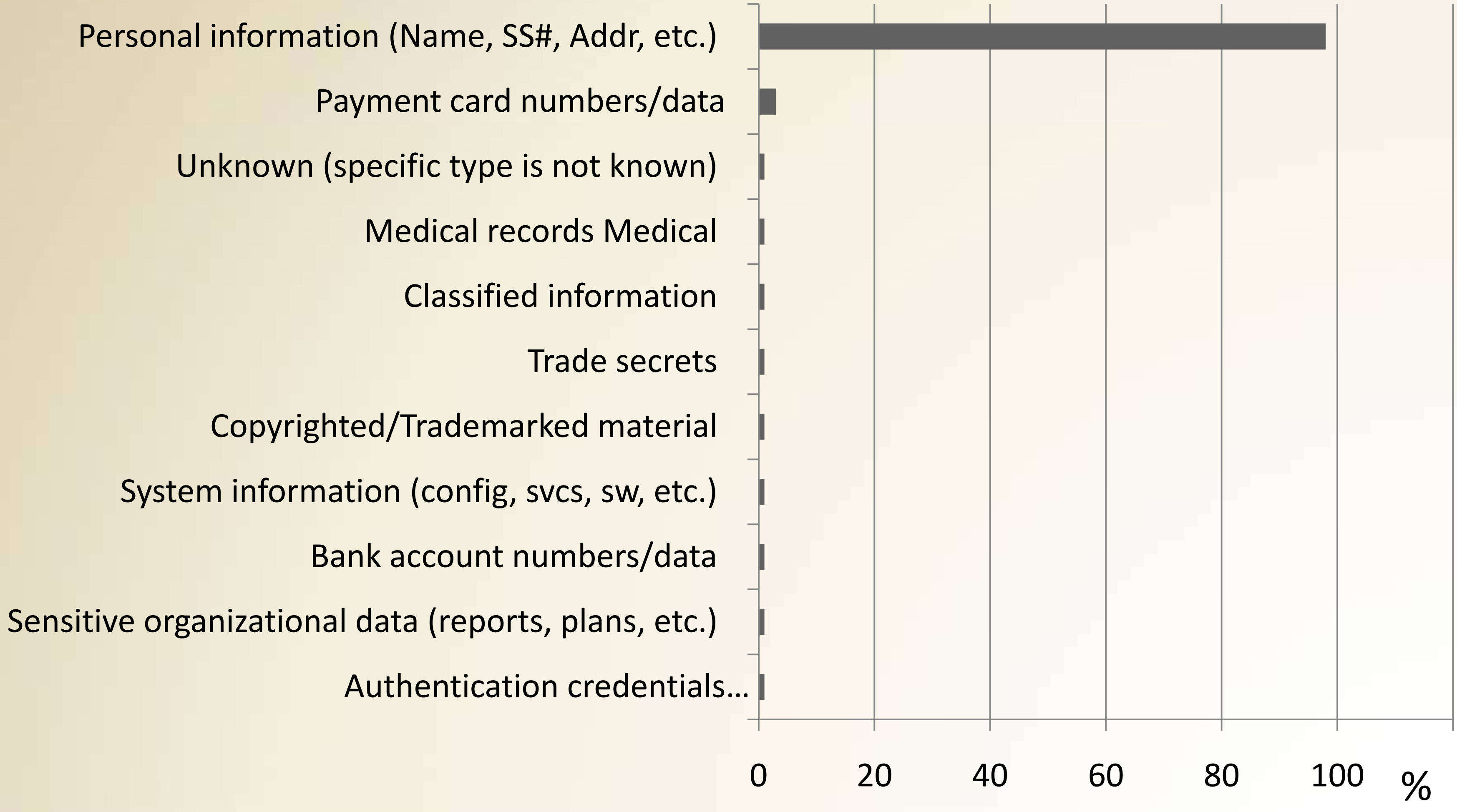


Based on post-breach reviews. Relevant Organizations in Compliance with PCI DSS. Verizon Study

Follow us @ISACANews
#NACACS

WHAT TYPES OF DATA ARE UNDER ATTACK NOW?

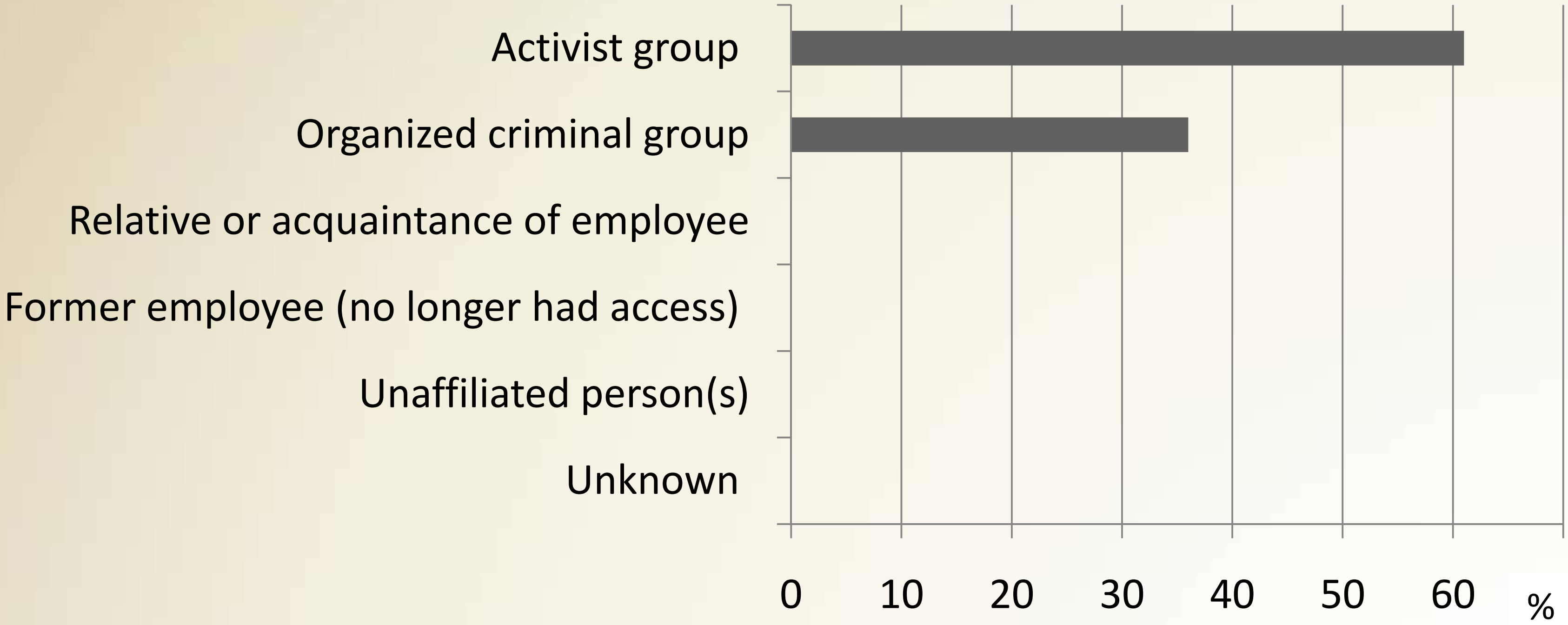
What Data is Compromised?



By percent of records. Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

Follow us @ISACANews
#NACACS

Today “Hacktivism” is Dominating



By percent of records
Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

Growing Threat of “hacktivism” by Groups such as Anonymous

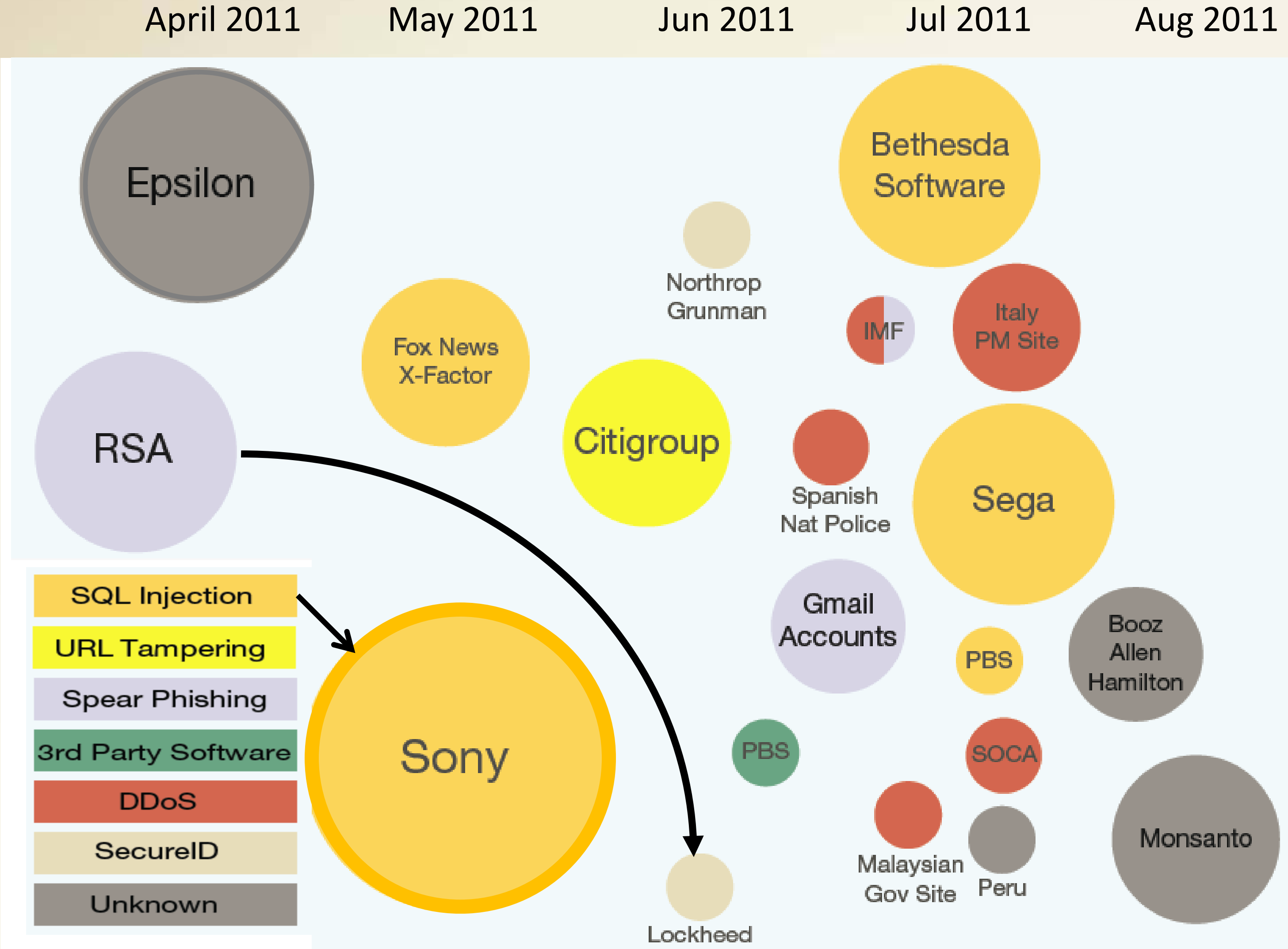
Attacks by Anonymous include

- 2012: CIA and Interpol
- 2011: Sony, Stratfor and HBGary Federal

Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/, http://en.wikipedia.org/wiki/Timeline_of_events_involving_Anonymous

Let’s Review Some Major Recent Breaches

Attack Type, Time and Impact $



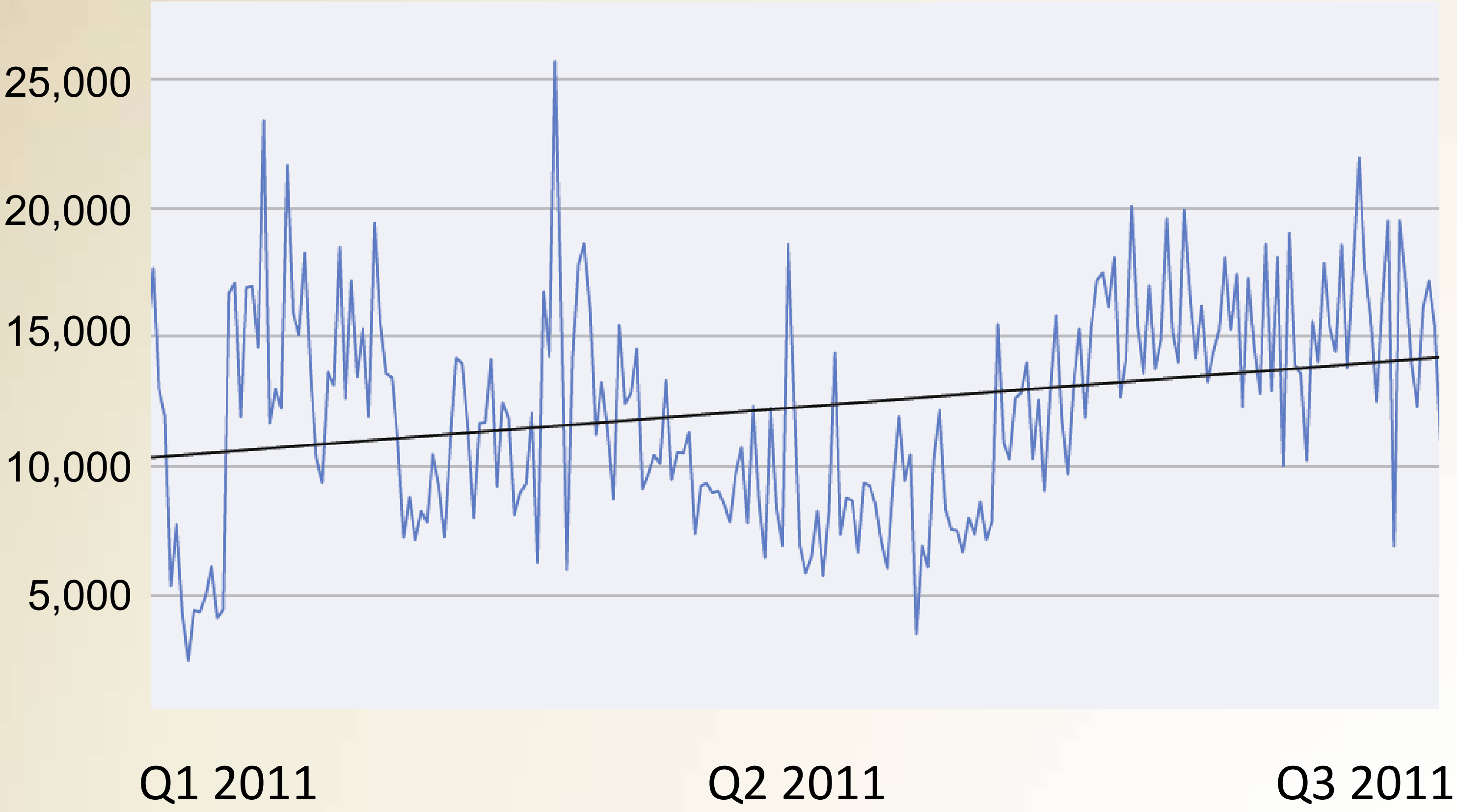
Source: IBM 2012 Security Breaches Trend and Risk Report

Follow us @ISACANews
#NACACS

The Sony Breach & Cloud

- Lost 100 million passwords and personal details stored in clear
- Spent $171 million related to the data breach
- Sony's stock price has fallen 40 percent
- For three pennies an hour, hackers can rent Amazon.com to wage cyber attacks such as the one that crippled Sony
- Attack via **SQL Injection**

SQL Injection Attacks are Increasing



Source: IBM 2012 Security Breaches Trend and Risk Report

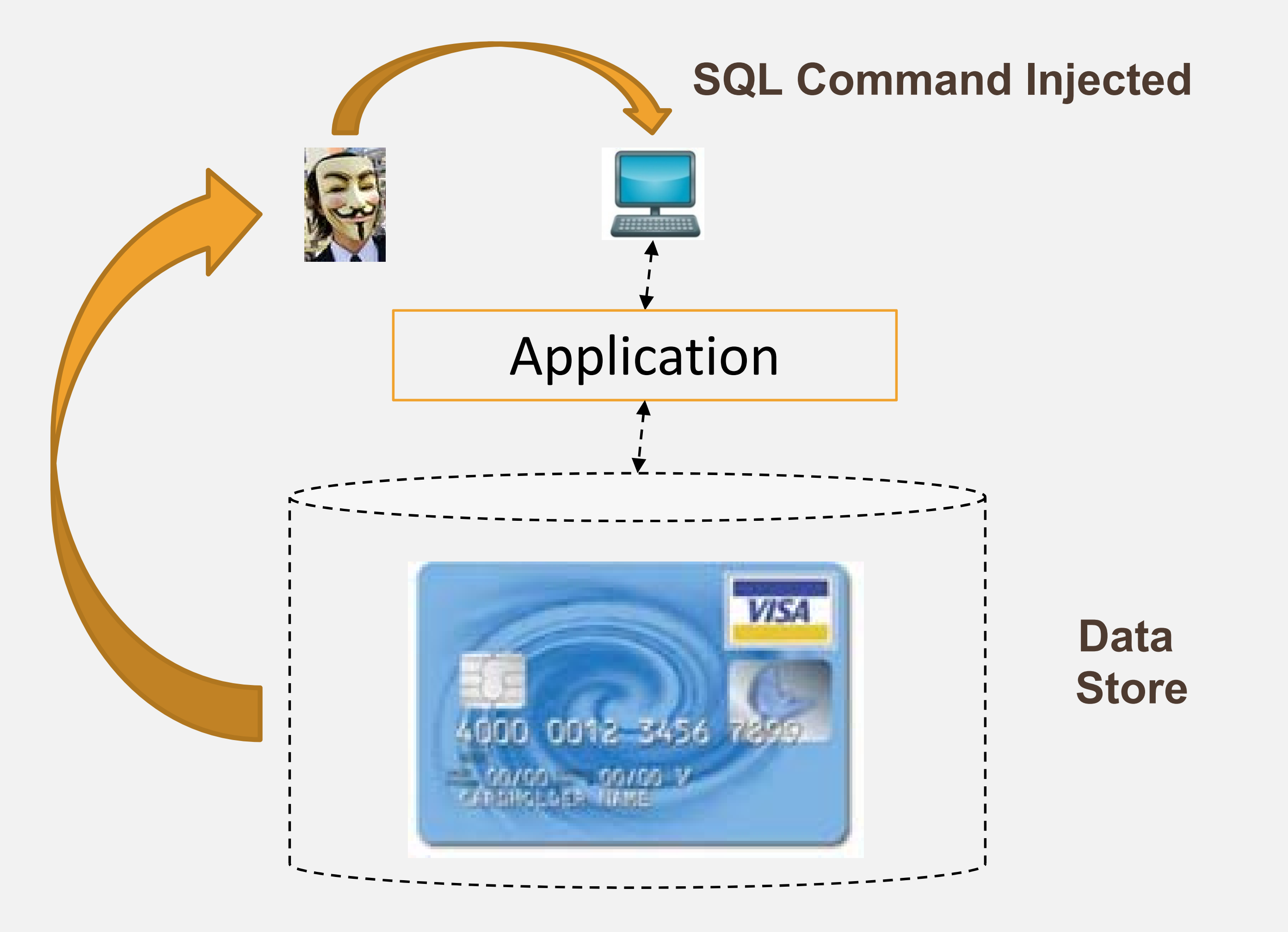
Follow us @ISACANews
#NACACS

WHAT IS SQL INJECTION?

Follow us @ISACANews
#NACACS

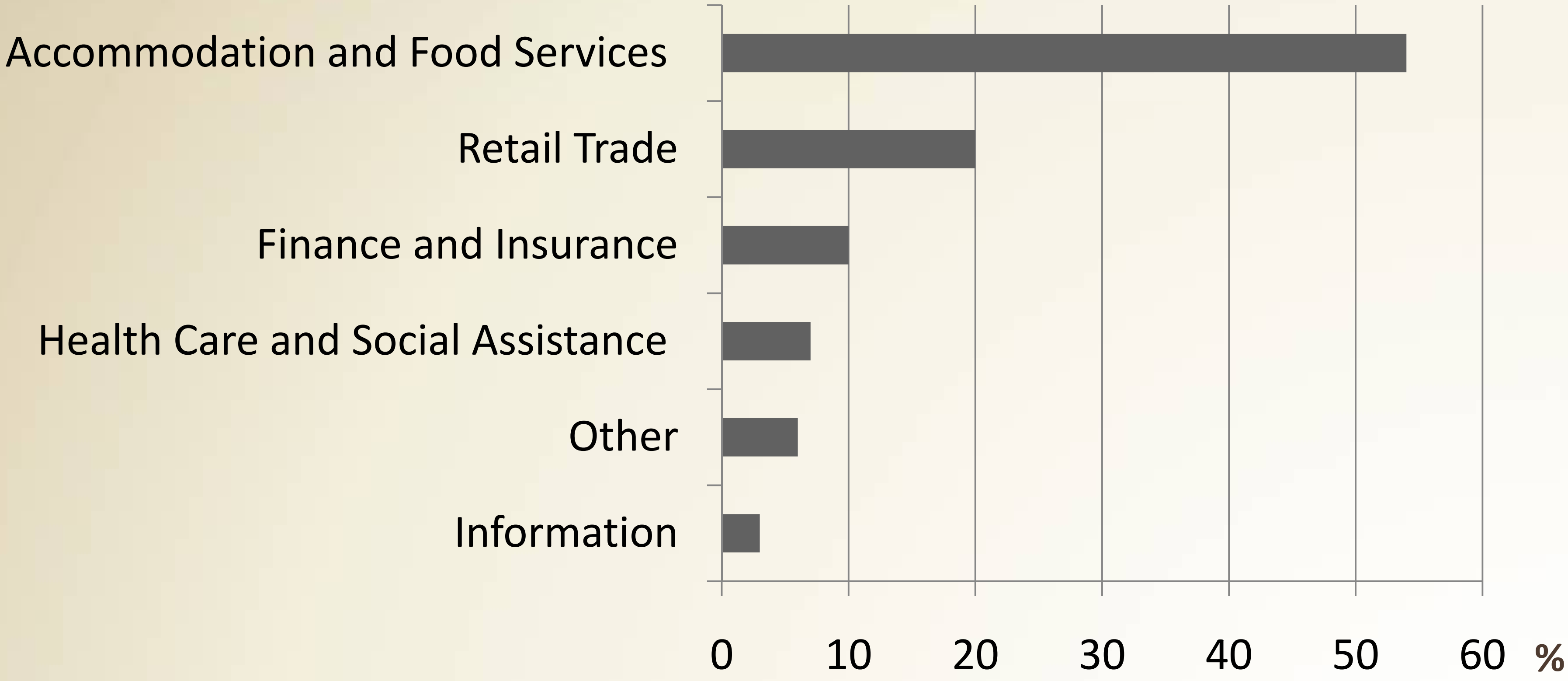
Trust in, and value from, information systems

What is an SQL Injection Attack?



WHO IS THE NEXT TARGET?

New Industry Groups are Targets



By percent of breaches
Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

Follow us @ISACANews
#NACACS

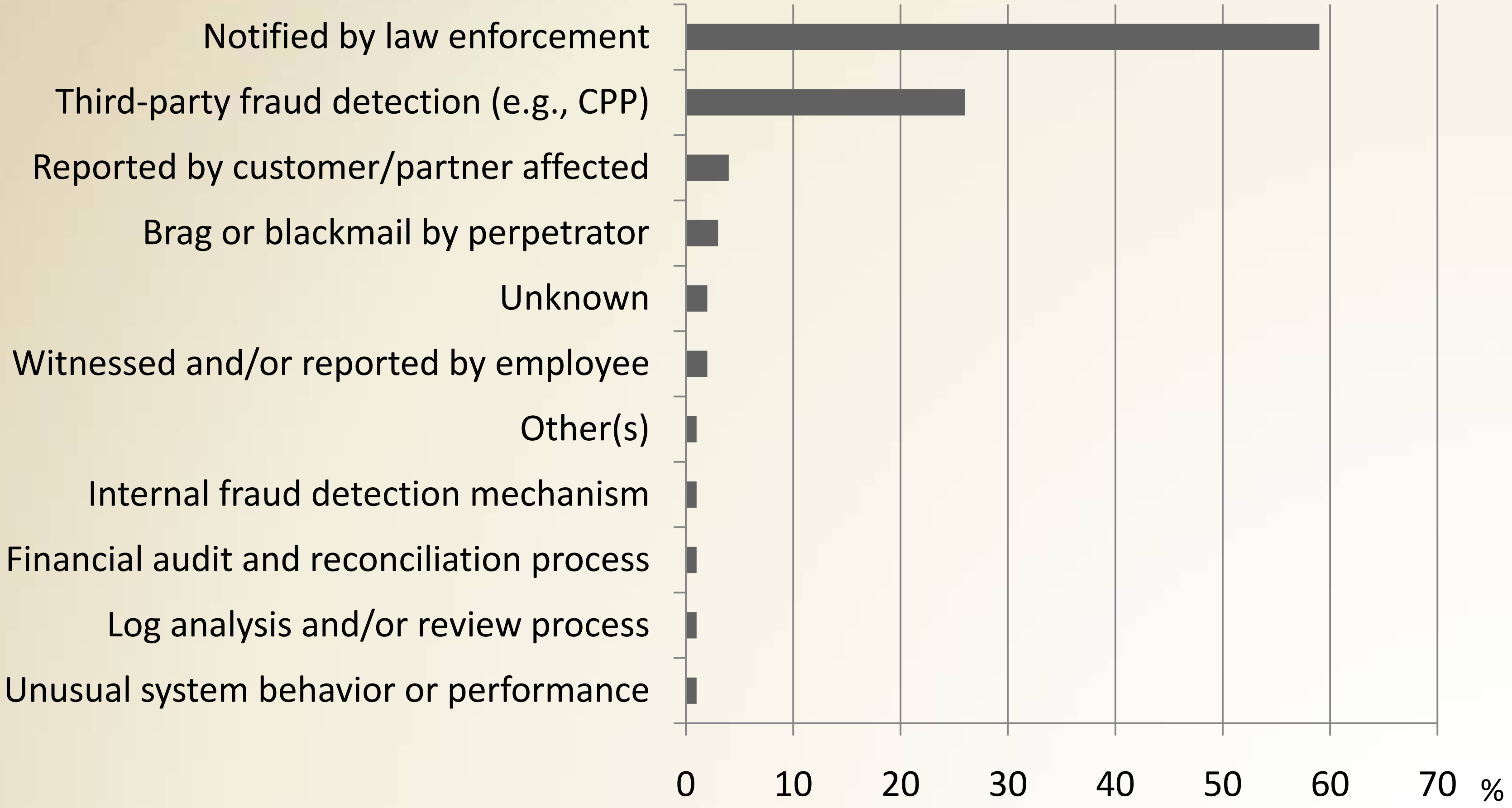
The Changing Threat Landscape

- Some issues have stayed constant:
  - Threat landscape continues to gain sophistication
  - Attackers will always be a step ahead of the defenders
- We are fighting highly organized, well-funded crime syndicates and nations
- Move from detective to preventative controls needed

FORRESTER Forrester Research
MAKING LEADERS SUCCESSFUL EVERY DAY

Source: http://www.csoonline.com/article/602313/the-changing-threat-landscape?page=2

How are Breaches Discovered?



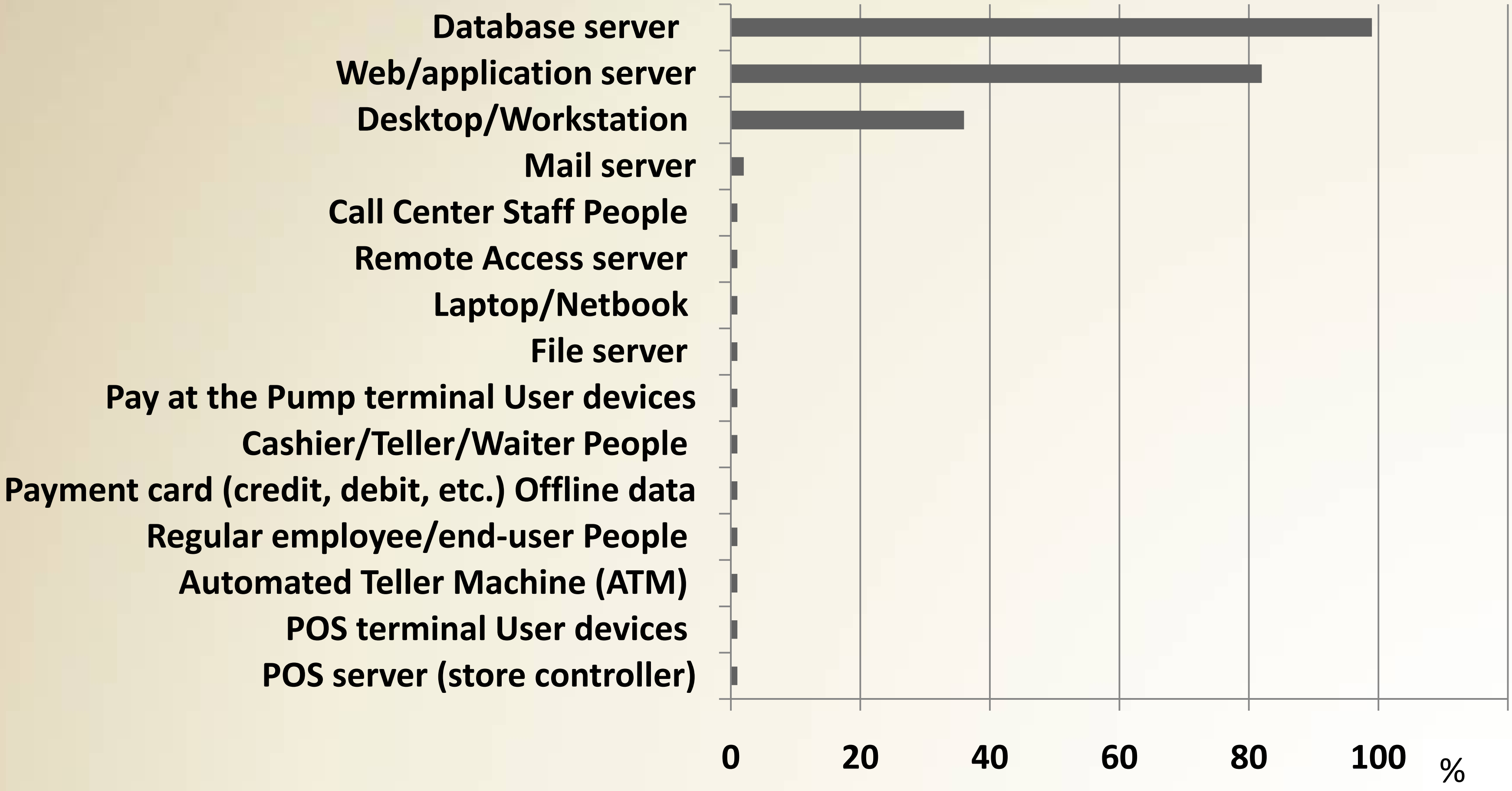
By percent of breaches . Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

Follow us @ISACANews
#NACACS

Trust in, and value from, information systems

WHERE IS DATA LOST?

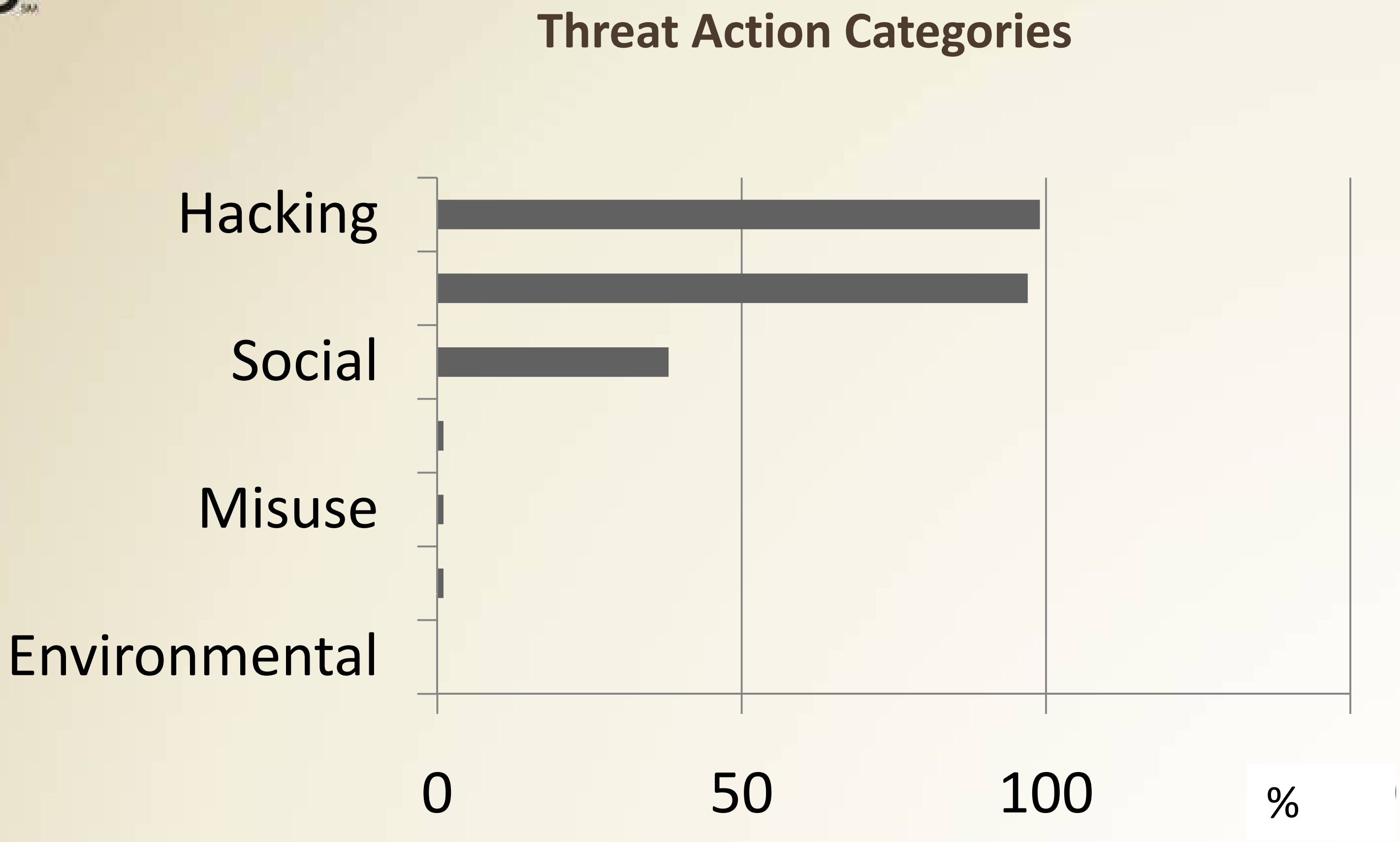
What Assets are Compromised?



By percent of records

Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

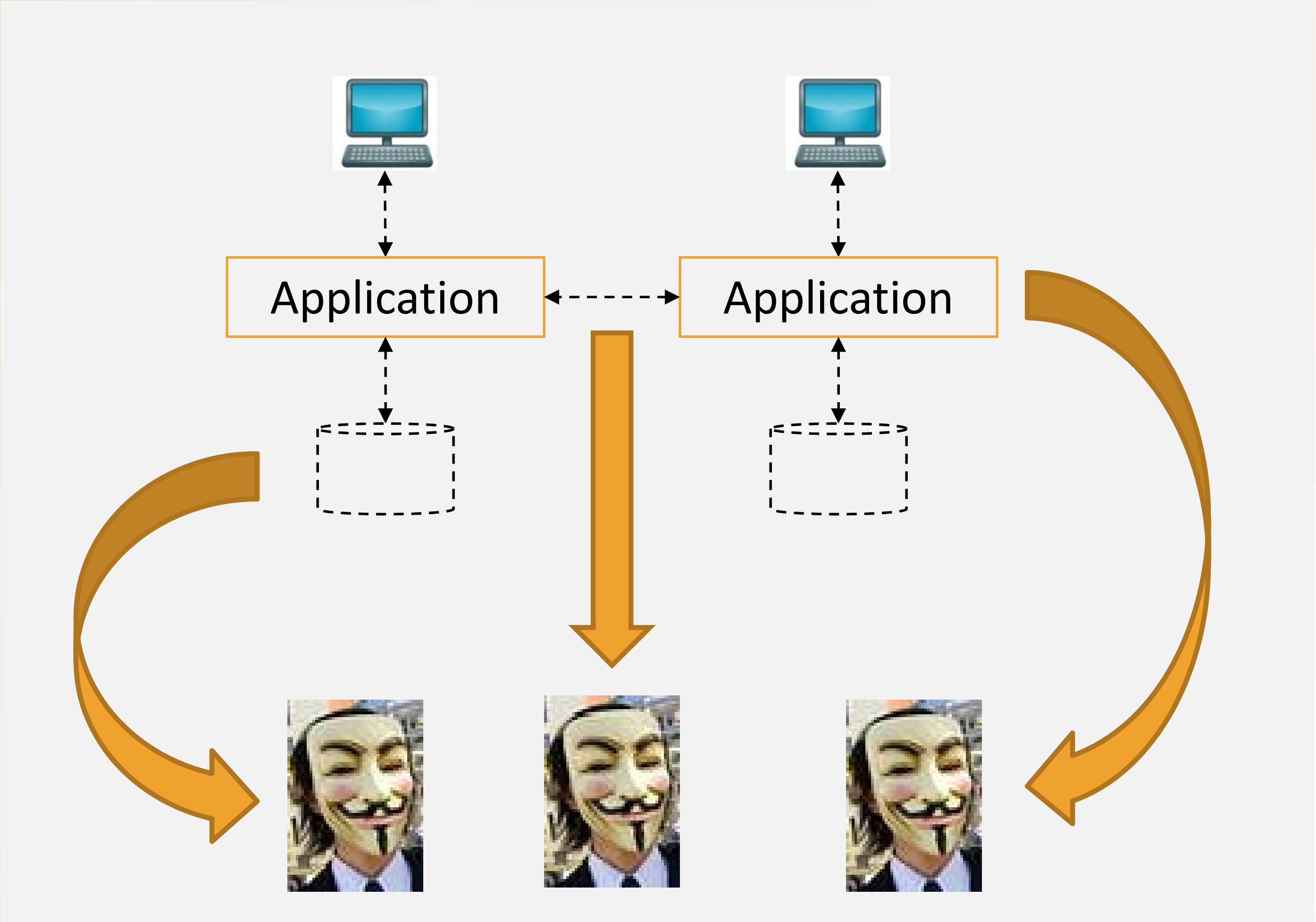
Hacking and Malware are Leading



By percent of records

Source: 2012, http://www.verizonbusiness.com/Products/security/dbir/

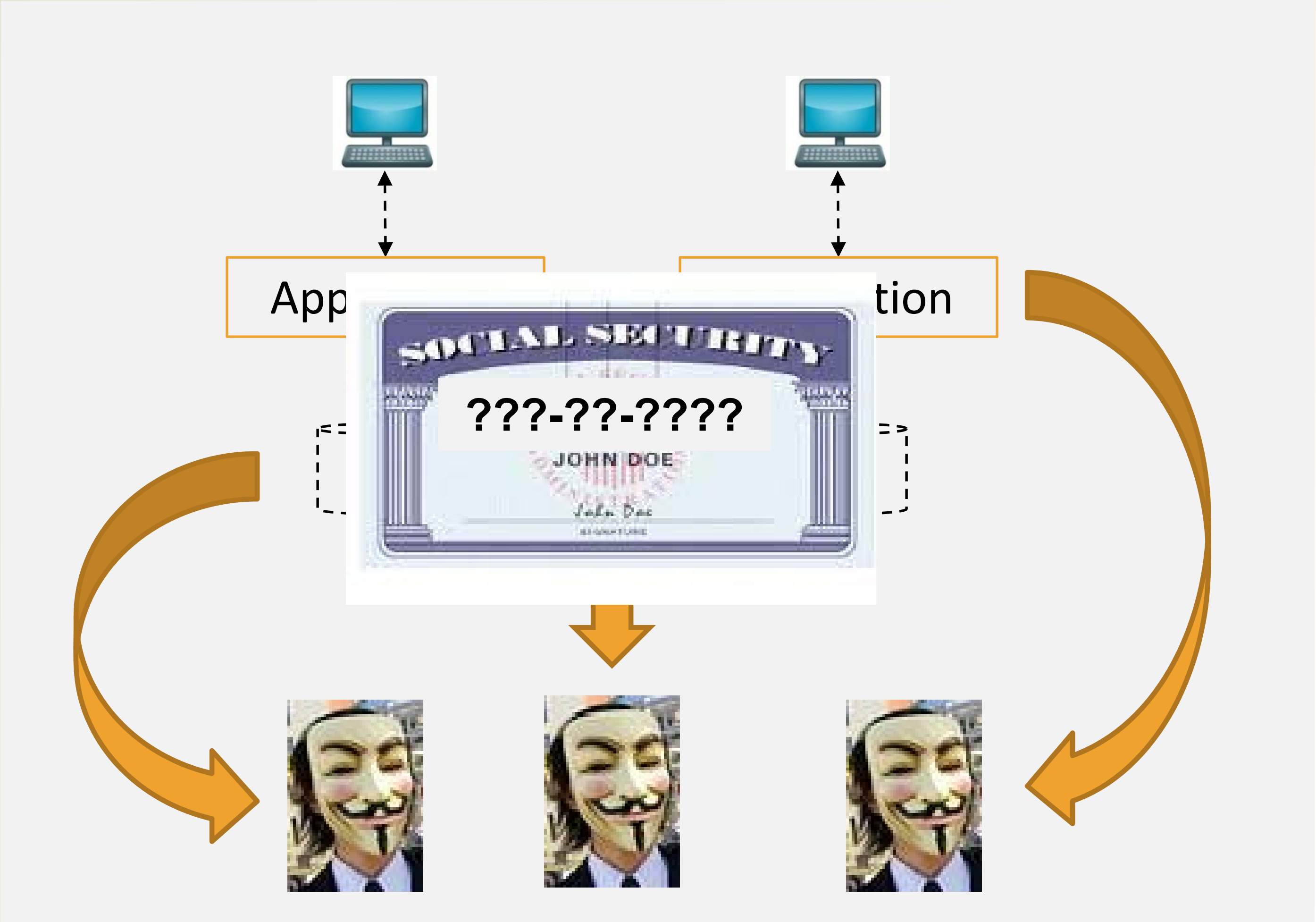
Thieves Are Attacking the Data Flow



Follow us @ISACANews
#NACACS

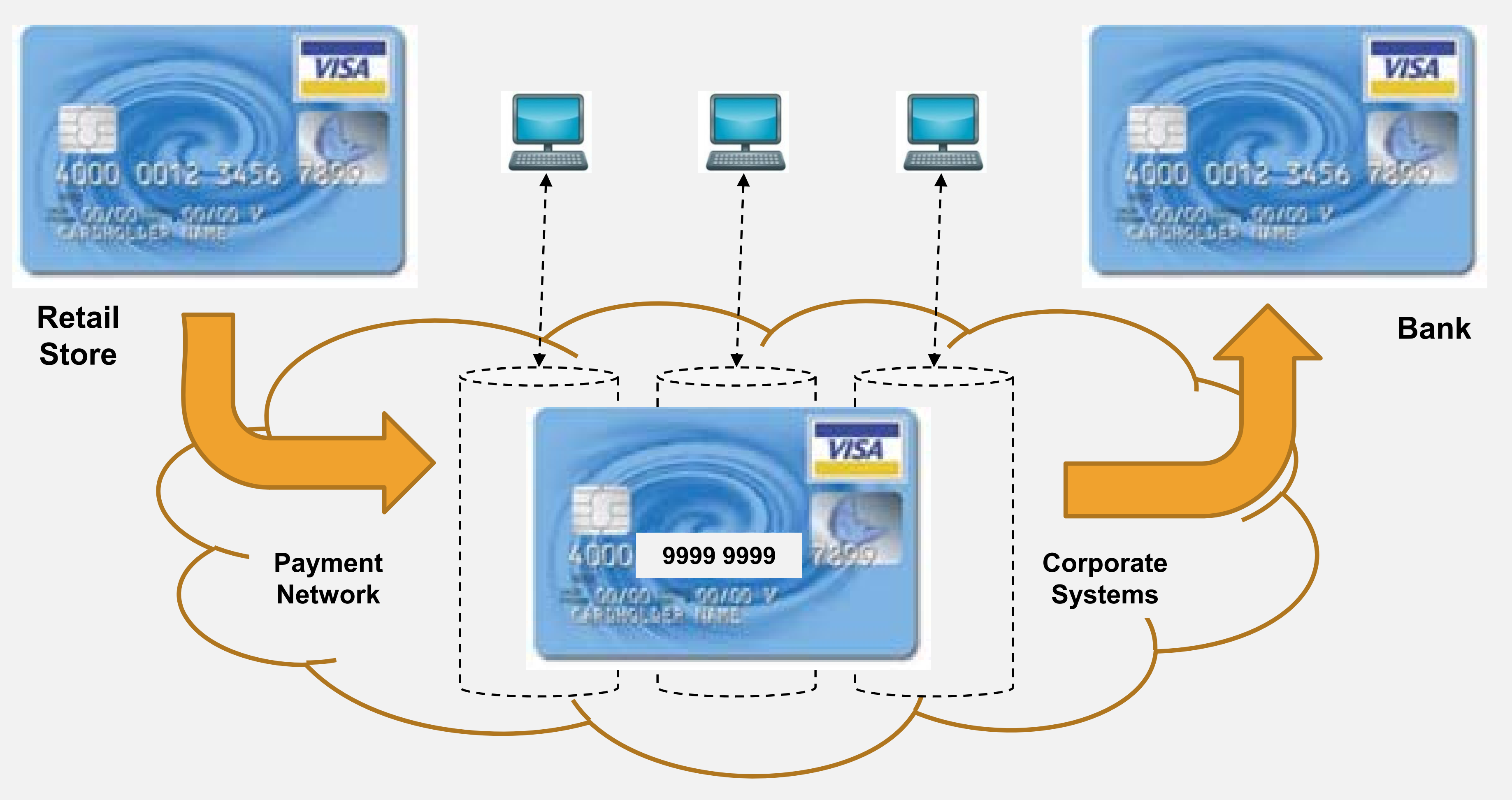
THIS IS A CATCH 22!

Thieves Can't Steal What's Not There: Fake Data



HOW CAN WE SECURE THE DATA FLOW?

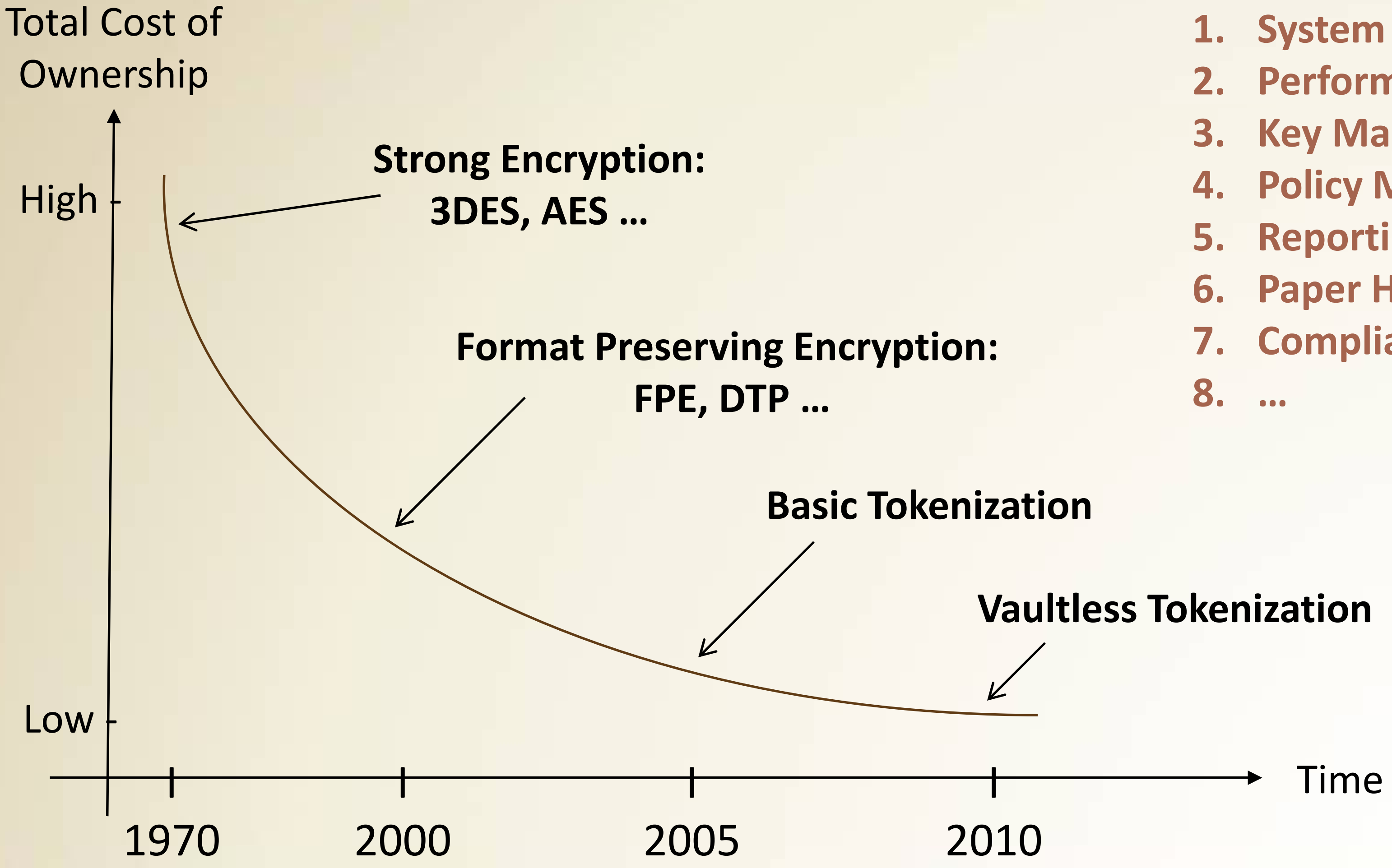
Securing The Data Flow with Tokenization



Follow us @ISACANews
#NACACS

WHAT HAS THE INDUSTRY DONE TO SECURE DATA?

What Has The Industry Done?



Total Cost of Ownership

1. System Integration
2. Performance Impact
3. Key Management
4. Policy Management
5. Reporting
6. Paper Handling
7. Compliance Audit
8. …

Follow us @ISACANews
#NACACS

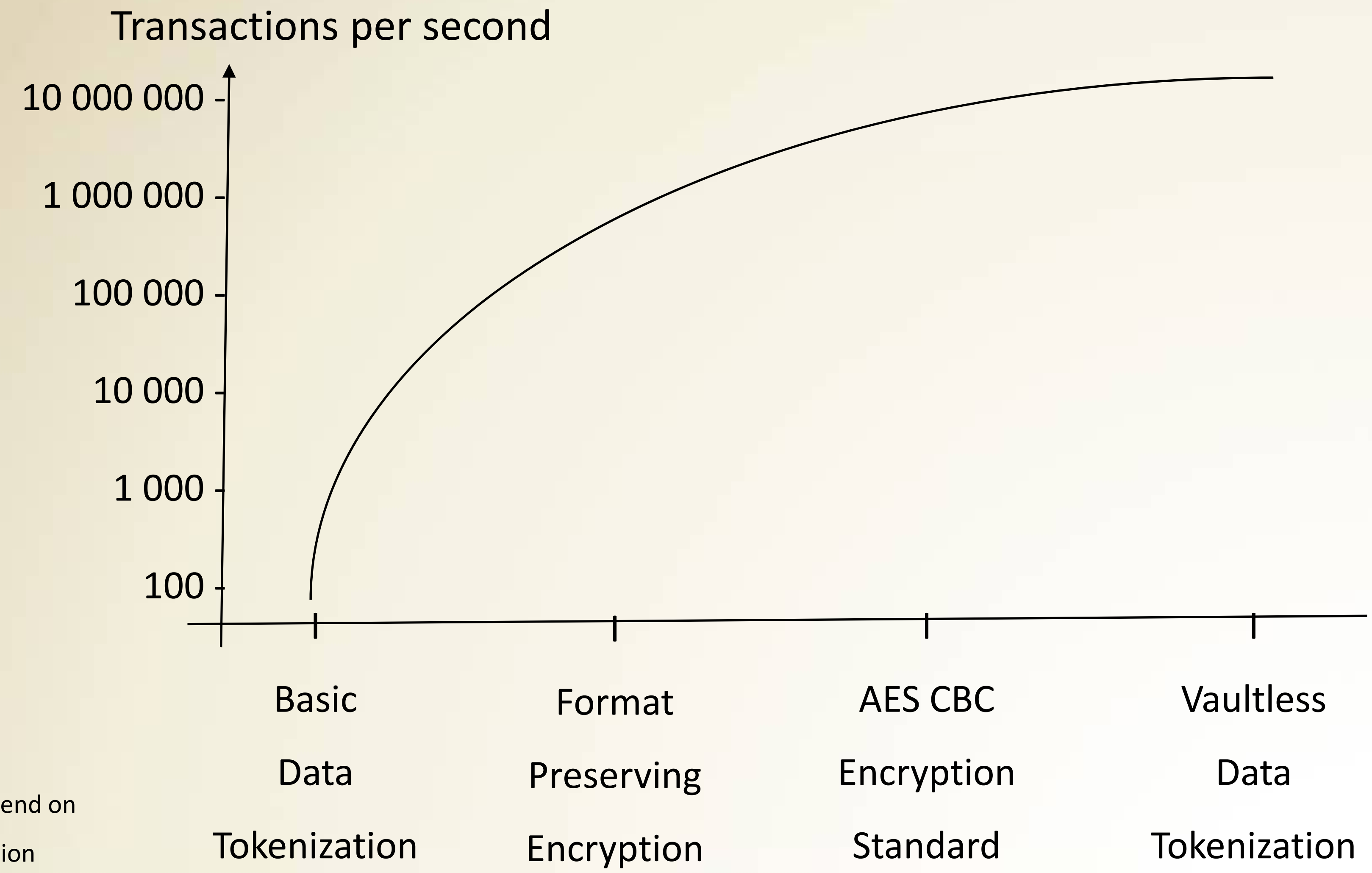
Case Study: Large Chain Store

Why? Reduce compliance cost by 50%

- 50 million Credit Cards, 700 million daily transactions
- Performance Challenge: 30 days with Basic to 90 minutes with Vaultless Tokenization
- End-to-End Tokens: Started with the D/W and expanding to stores
- Lower maintenance cost – don't have to apply all 12 requirements
- Better security – able to eliminate several business and daily reports
- Qualified Security Assessors had no issues
  - "With encryption, implementations can spawn dozens of questions"
  - "There were no such challenges with tokenization"

HOW CAN WE POSITION DIFFERENT SECURITY OPTIONS?

Speed of Different Protection Methods



Speed will depend on the configuration

WHAT IS VAULT-LESS DATA TOKENIZATION?

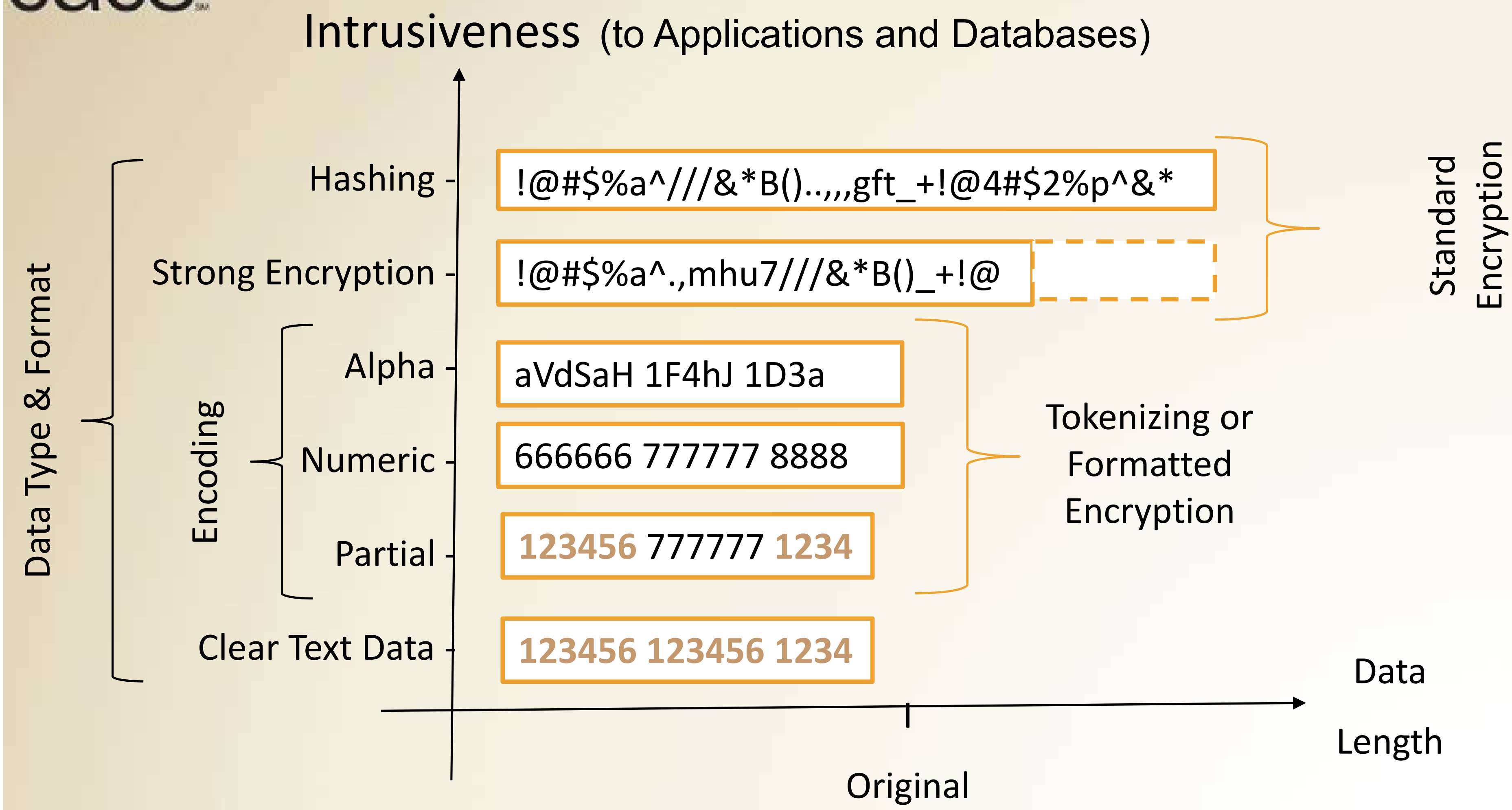
Different Tokenization Approaches

	Basic Tokenization	Vault-less Tokenization*
Footprint	Large, Expanding.	Small, Static.
High Availability, Disaster Recovery	Complex, expensive replication required.	No replication required.
Distribution	Practically impossible to distribute geographically.	Easy to deploy at different geographically distributed locations.
Reliability	Prone to collisions.	No collisions.
Performance, Latency, and Scalability	Will adversely impact performance & scalability.	Little or no latency. Fastest industry tokenization.
Extendibility	Practically impossible.	Unlimited Tokenization Capability.

*: Validated by 3rd party experts

HOW IMPORTANT IS COST?

Impact of Different Protection Methods



Intrusiveness (to Applications and Databases)

Data Type & Format

Hashing - !@#$%a^///&*B()..,,,gft_+!@4#$2%p^&*

Strong Encryption - !@#$%a^.,mhu7///&*B()_+!@

Encoding

Alpha - aVdSaH 1F4hJ 1D3a

Numeric - 666666 777777 8888

Partial - 123456 777777 1234

Clear Text Data - 123456 123456 1234

Standard Encryption

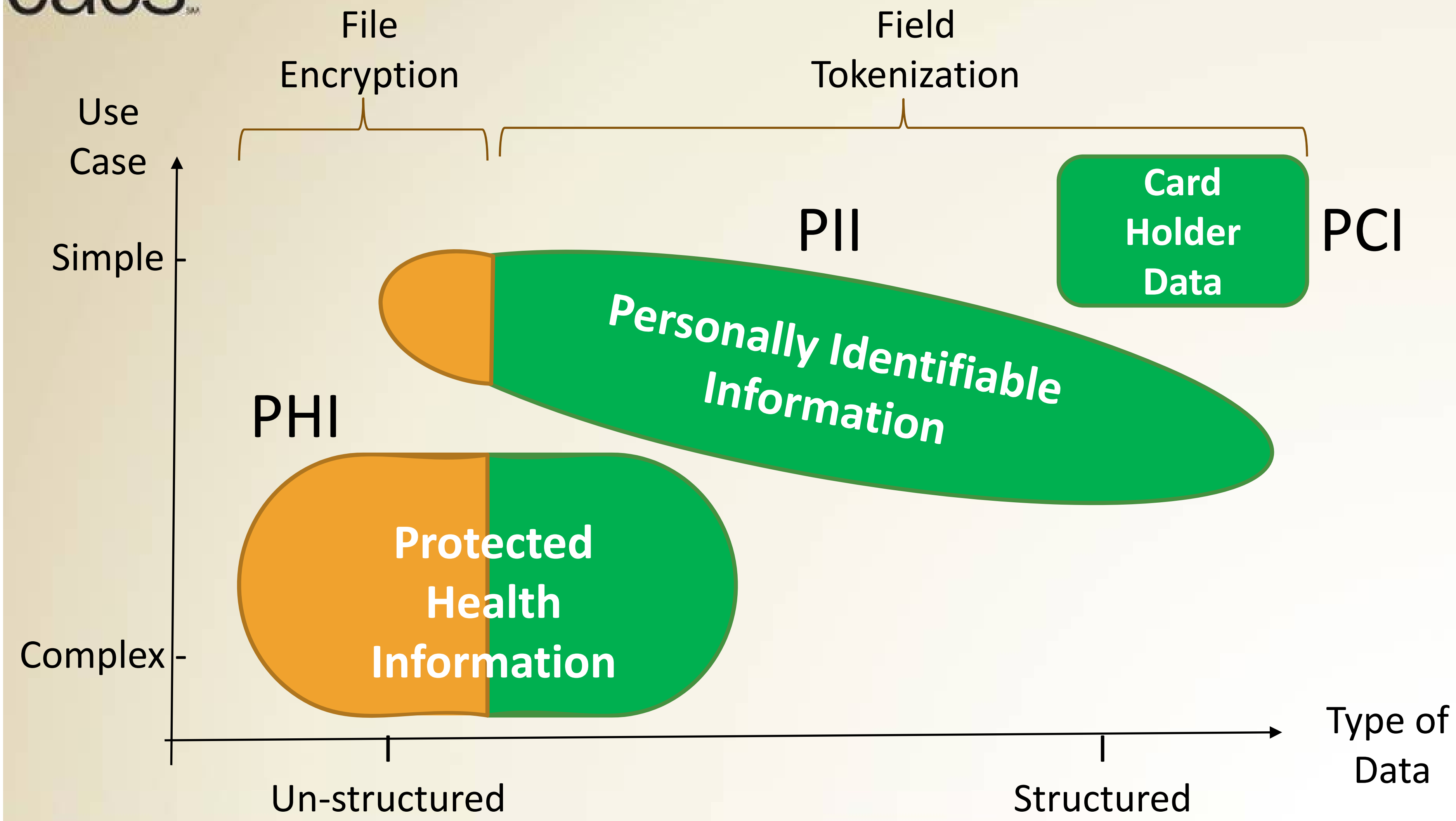
Tokenizing or Formatted Encryption

Original

Data Length

WHEN CAN I USE TOKENIZATION?

How Should I Secure Different Data?



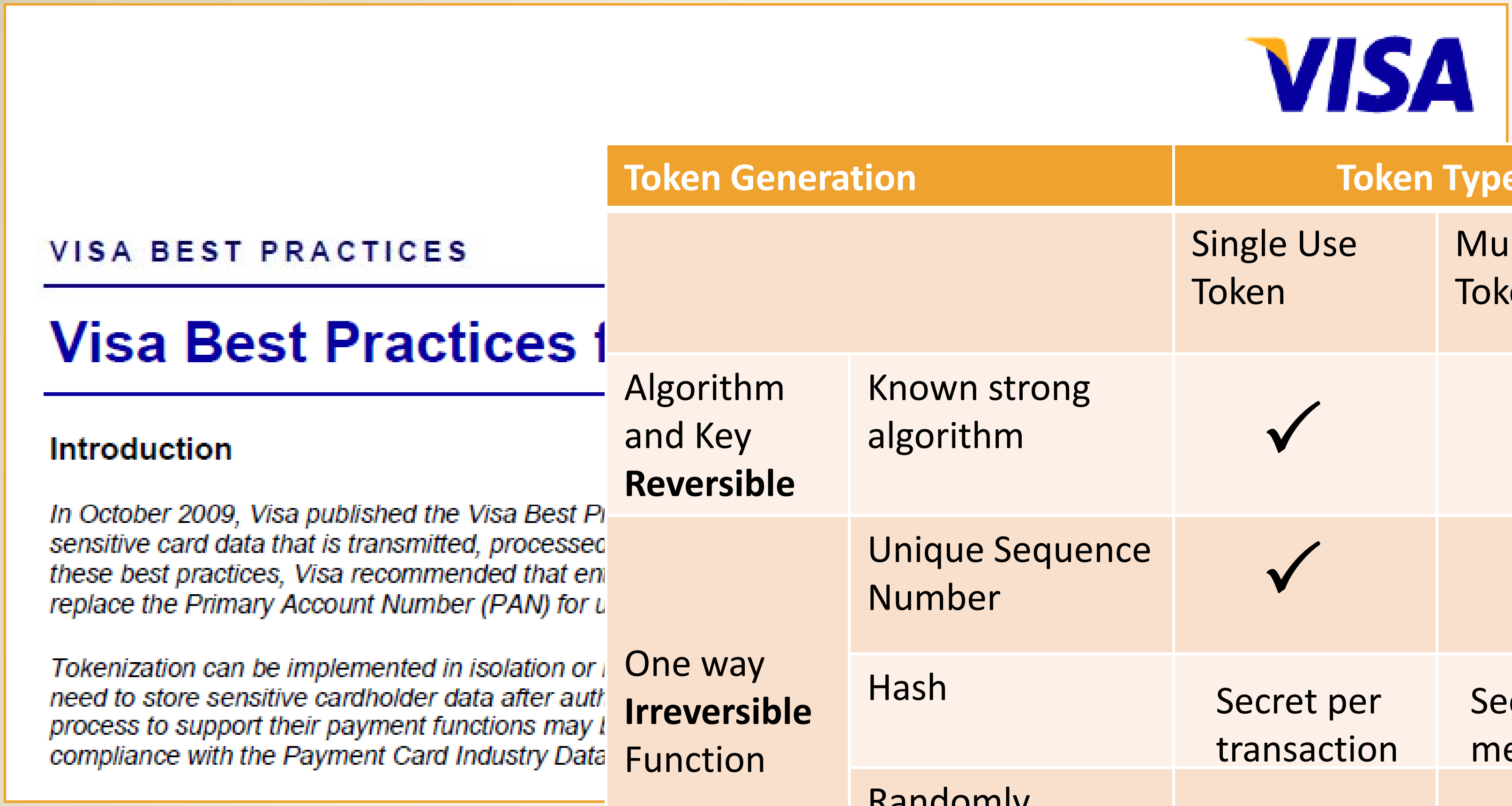
Follow us @ISACANews
#NACACS

Tokenizing Different Types of Data

Type of Data	Input	Token	Comment
Credit Card	3872 3789 1620 3675	8278 2789 2990 2789	Numeric
Medical ID	29M2009ID	497HF390D	Alpha-Numeric
Date	10/30/1955	12/25/2034	Date
E-mail Address	Ulf.mattsson@protegrity.com	empo.snaugs@svtiensnni.snk	Alpha Numeric, delimiters in input preserved
SSN delimiters	075-67-2278	287-38-2567	Numeric, delimiters in input
Credit Card	3872 3789 1620 3675	8278 2789 2990 3675	Numeric, Last 4 digits exposed

ANY TOKENIZATION GUIDELINES?

Tokenization Guidelines, Visa



VISA

VISA BEST PRACTICES

Visa Best Practices f

Introduction

In October 2009, Visa published the Visa Best Pr sensitive card data that is transmitted, processed these best practices, Visa recommended that en replace the Primary Account Number (PAN) for u

Tokenization can be implemented in isolation or need to store sensitive cardholder data after auth process to support their payment functions may b compliance with the Payment Card Industry Data

Token Generation		Token Types	
		Single Use Token	Multi Use Token
Algorithm and Key **Reversible**	Known strong algorithm	✓	**No**
One way **Irreversible** Function	Unique Sequence Number	✓	✓
	Hash	Secret per transaction	Secret per merchant
	Randomly generated value	✓	✓

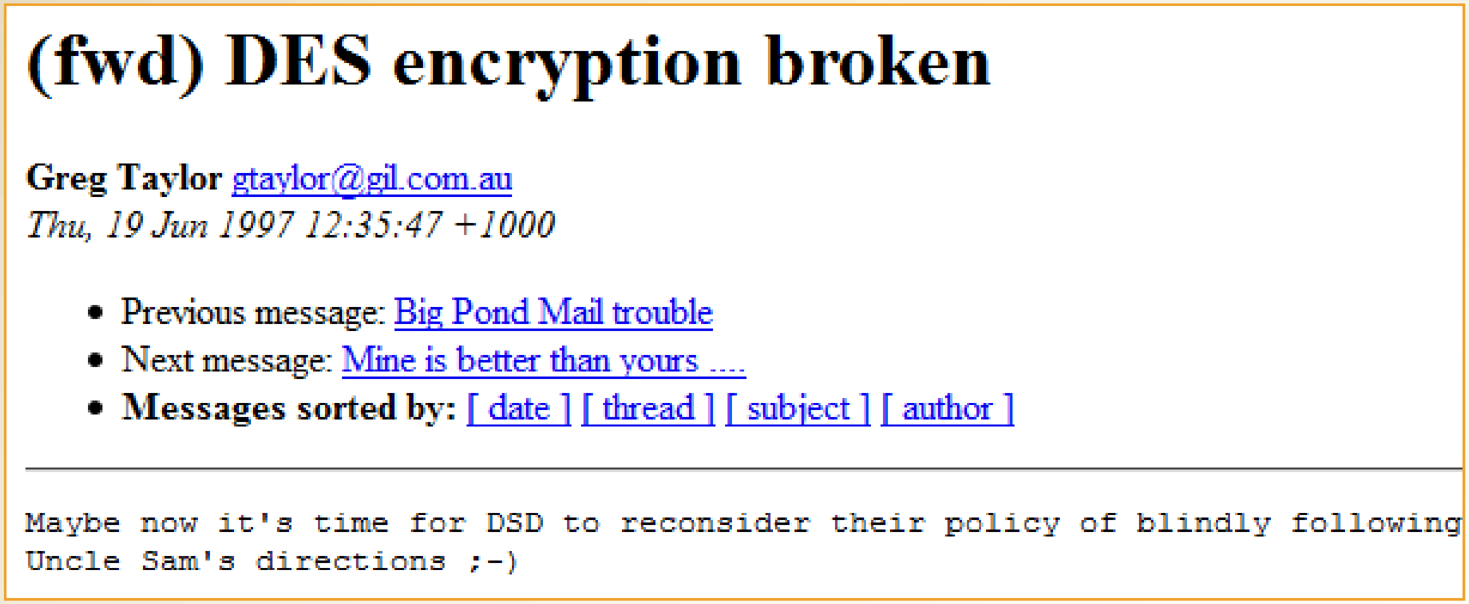
Tokenization vs. Encryption

	Encryption	Tokenization
Used Approach	**Cipher System**	**Code System**
Cryptographic algorithms	●	
Cryptographic keys	●	
Code books		●
Index tokens		●

Source: McGraw-HILL ENCYPLOPEDIA OF SCIENCE & TECHNOLOGY

HOW SECURE IS ENCRYPTION?

Many Broken Algorithms

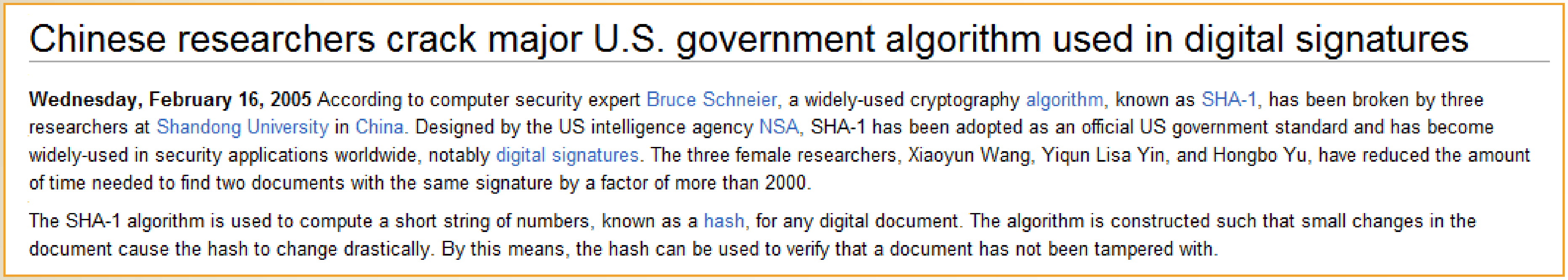


(fwd) DES encryption broken

Greg Taylor gtaylor@gil.com.au
Thu, 19 Jun 1997 12:35:47 +1000

- Previous message: Big Pond Mail trouble
- Next message: Mine is better than yours ....
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Maybe now it's time for DSD to reconsider their policy of blindly following
Uncle Sam's directions ;-)
```



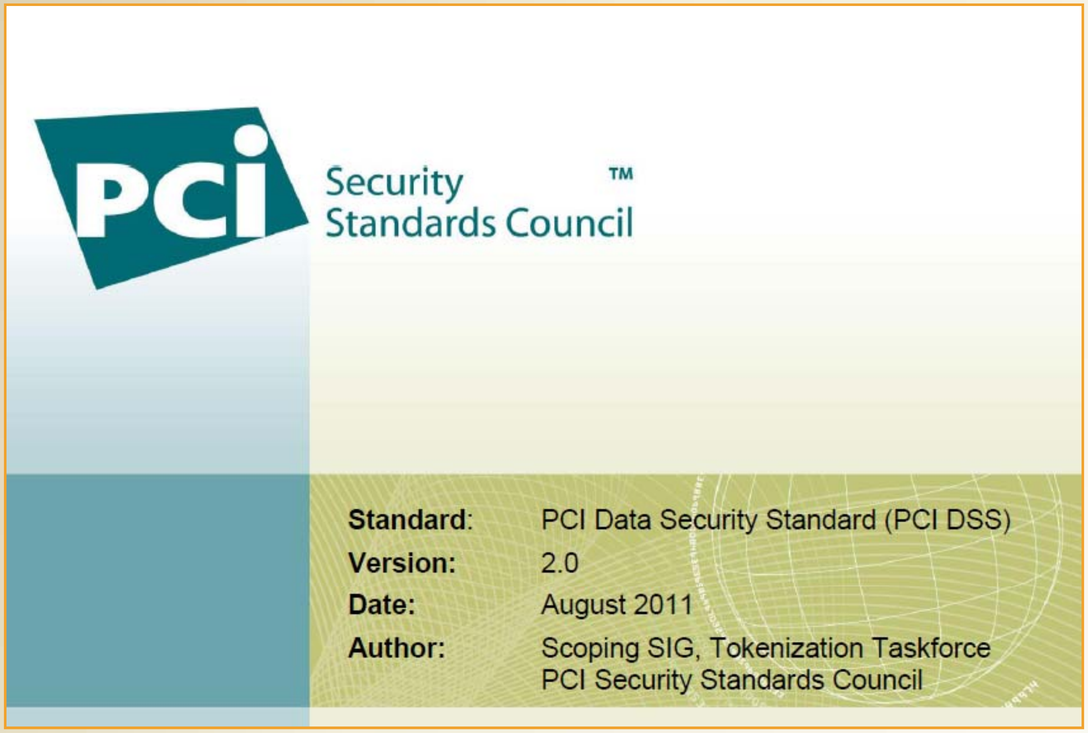
Chinese researchers crack major U.S. government algorithm used in digital signatures

Wednesday, February 16, 2005 According to computer security expert Bruce Schneier, a widely-used cryptography algorithm, known as SHA-1, has been broken by three researchers at Shandong University in China. Designed by the US intelligence agency NSA, SHA-1 has been adopted as an official US government standard and has become widely-used in security applications worldwide, notably digital signatures. The three female researchers, Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, have reduced the amount of time needed to find two documents with the same signature by a factor of more than 2000.

The SHA-1 algorithm is used to compute a short string of numbers, known as a hash, for any digital document. The algorithm is constructed such that small changes in the document cause the hash to change drastically. By this means, the hash can be used to verify that a document has not been tampered with.

KEYS EVERYWHERE!

PCI DSS : Tokenization and Encryption are Different



Security Standards Council™

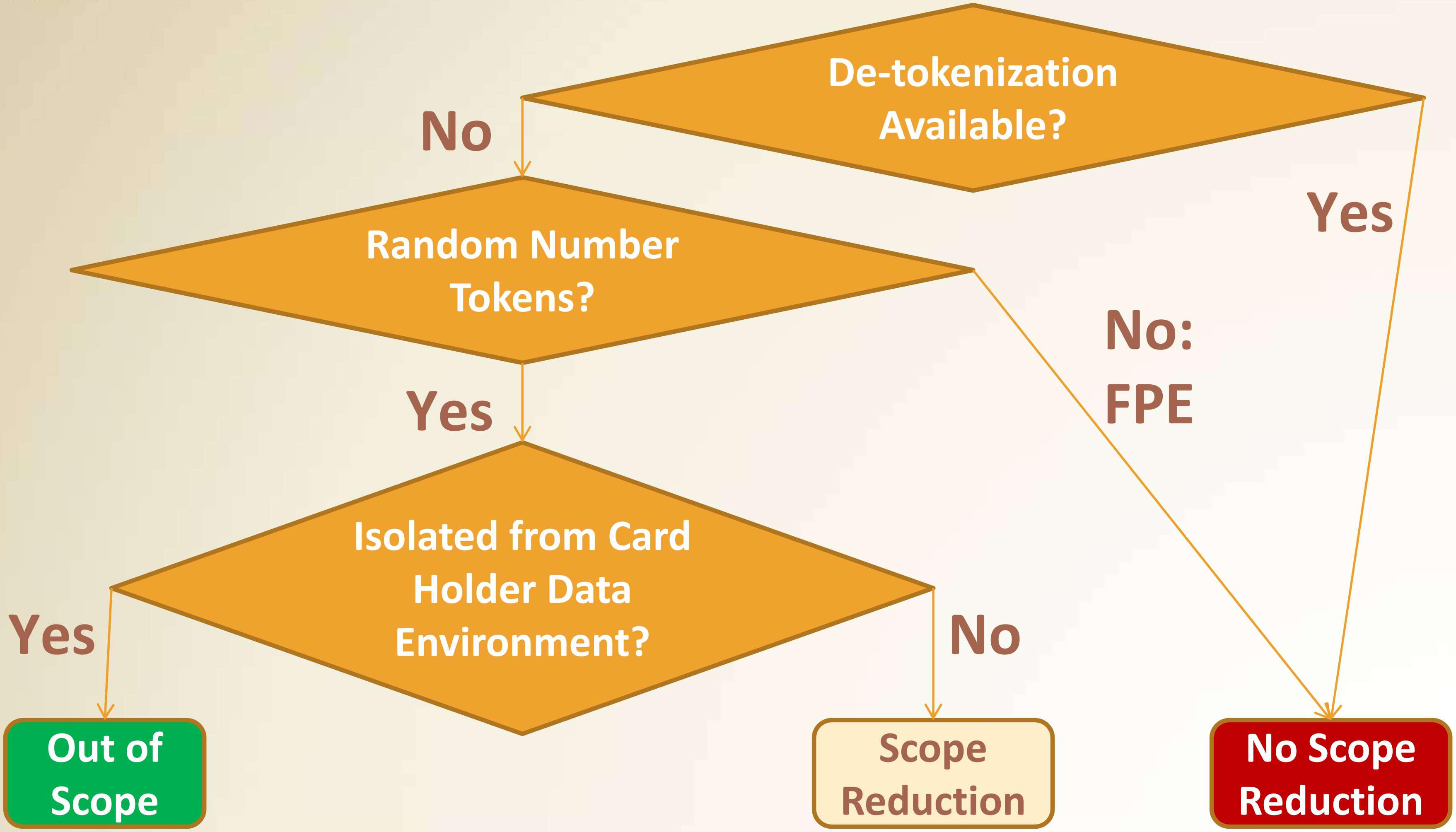
Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: August 2011
Author: Scoping SIG, Tokenization Taskforce
PCI Security Standards Council

If the token is mathematically derived from the original PAN through the use of an encryption algorithm and cryptographic key

No Scope Reduction

TOKENS ARE RANDOM

Tokenization and "PCI Out Of Scope"



Source: http://www.securosis.com

Follow us @ISACANews
#NACACS

Case Study: Energy Industry

Why? Reduce PCI Scope

- Best way to handle legacy, we got most of it out of PCI
- Get rid of unwanted paper copies
- No need to rewrite/redevelop or restructure business applications
- A VERY efficient way of PCI Reduction of Scope
- Better understanding of your data flow
- Better understanding of business flow
- Opportunity to clean up a few business oddities

Evaluating Encryption & Tokenization

Area	Criteria	Database File Encryption	Database Column Encryption	Basic Tokenization	Vaultless Tokenization
Scalability	Availability	●	●	○	●
	Latency	◔	◒	○	●
	CPU Consumption	○	◒	◒	●
Security	Data Flow Protection	○	◒	◕	●
	Compliance Scoping	◒	◕	●	●
	Key Management	○	○	●	●
	Data Collisions	●	●	◒	●
	Separation of Duties	◔	◒	●	●

Best ●

Case Studies: Retail

Customer 1: Why? Three major concerns solved

- Performance Challenge; Initial tokenization
- Vendor Lock-In: What if we want to switch payment processor
- Extensive Enterprise End-to-End Credit Card Data Protection

Customer 2: Why? Desired single vendor to provide data protection

- Combined use of tokenization and encryption
- Looking to expand tokens beyond CCN to **PII**

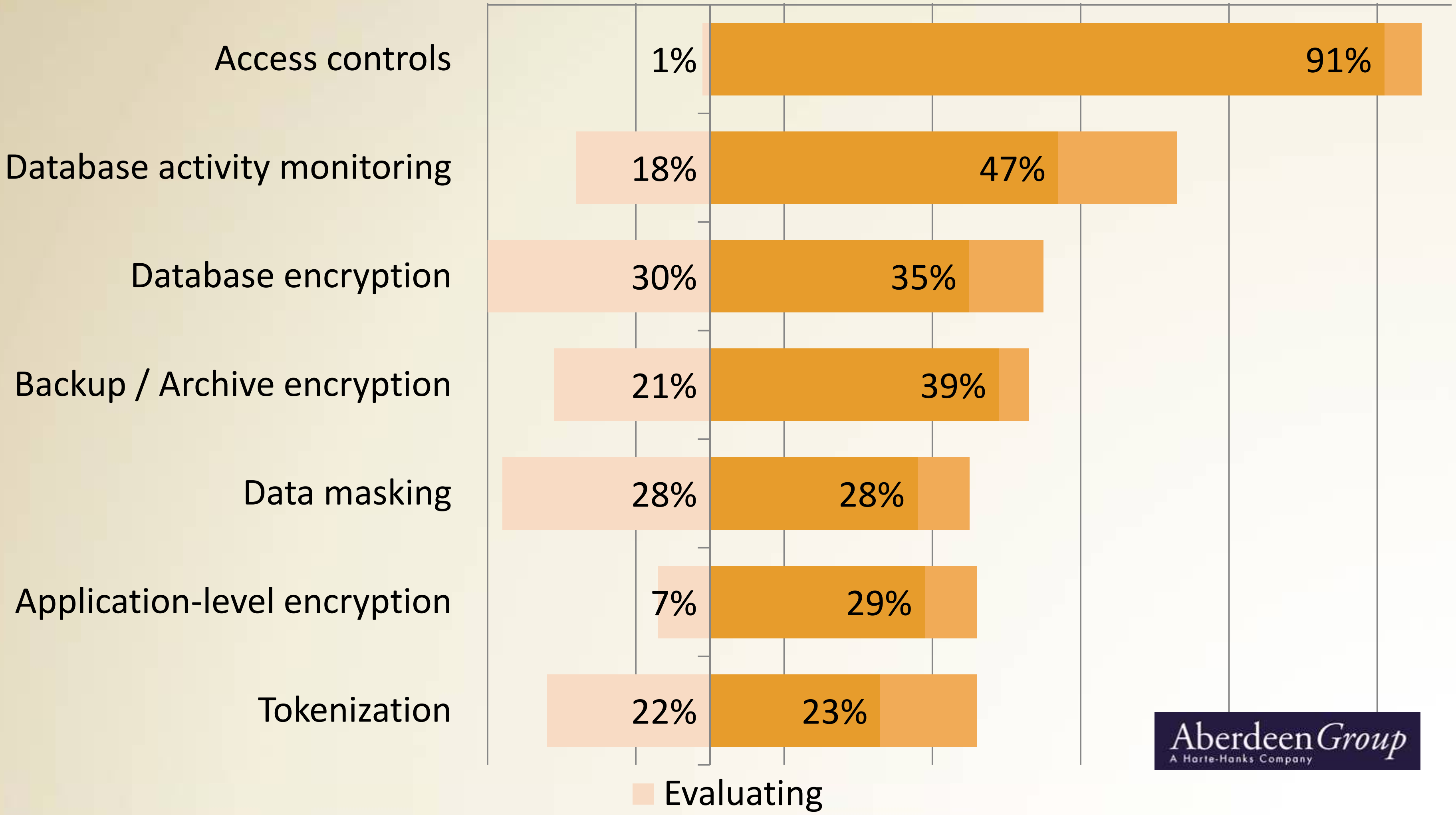
Customer 3: Why? Remove compensating controls from the mainframe

- Tokens on the mainframe to avoid compensating controls

WHAT IS THE CURRENT USE OF ENABLING TECHNOLOGIES?

Follow us @ISACANews
#NACACS

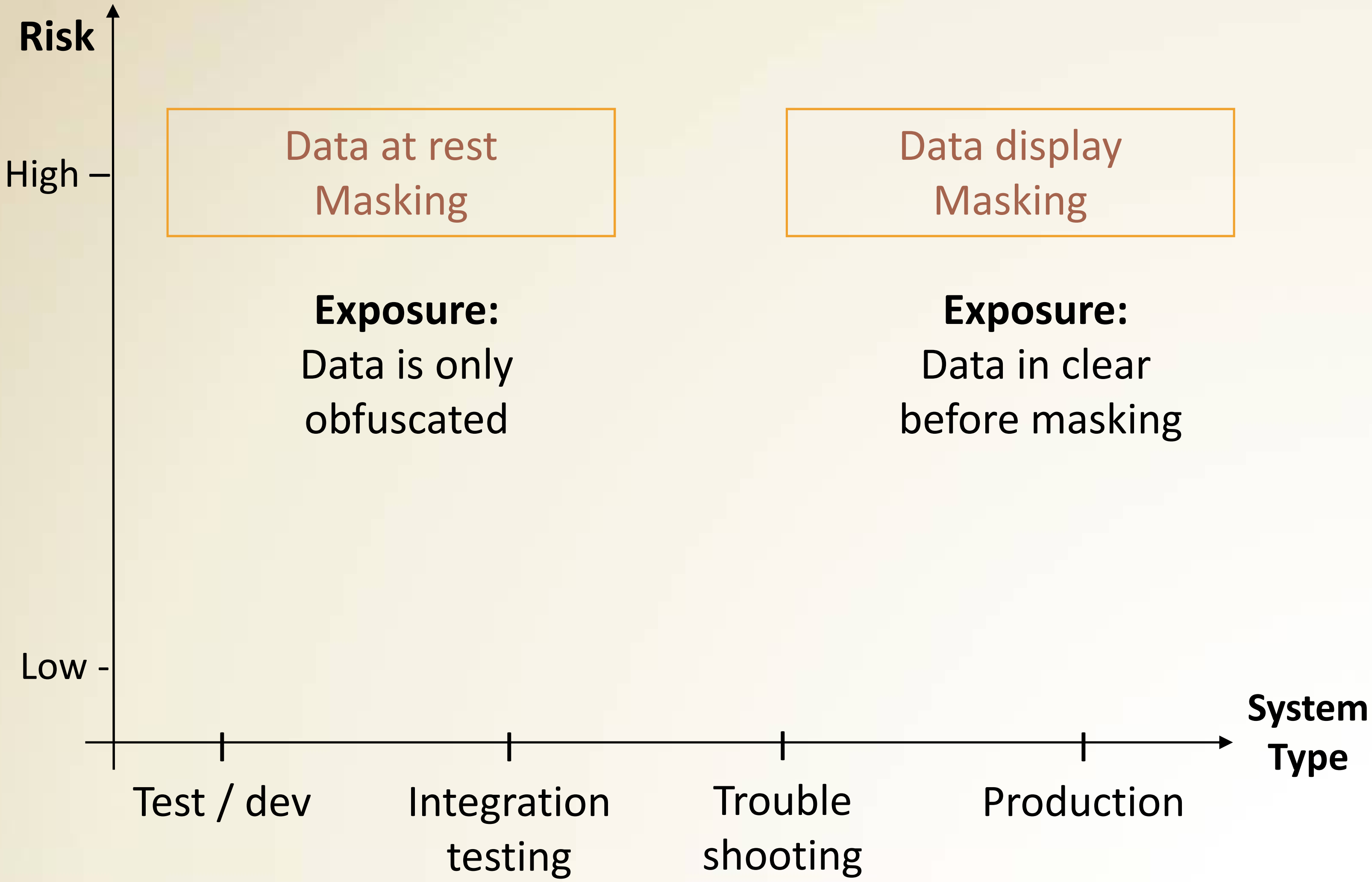
Use of Enabling Technologies



AberdeenGroup
A Harte-Hanks Company

Follow us @ISACANews
#NACACS

Is Data Masking Secure?



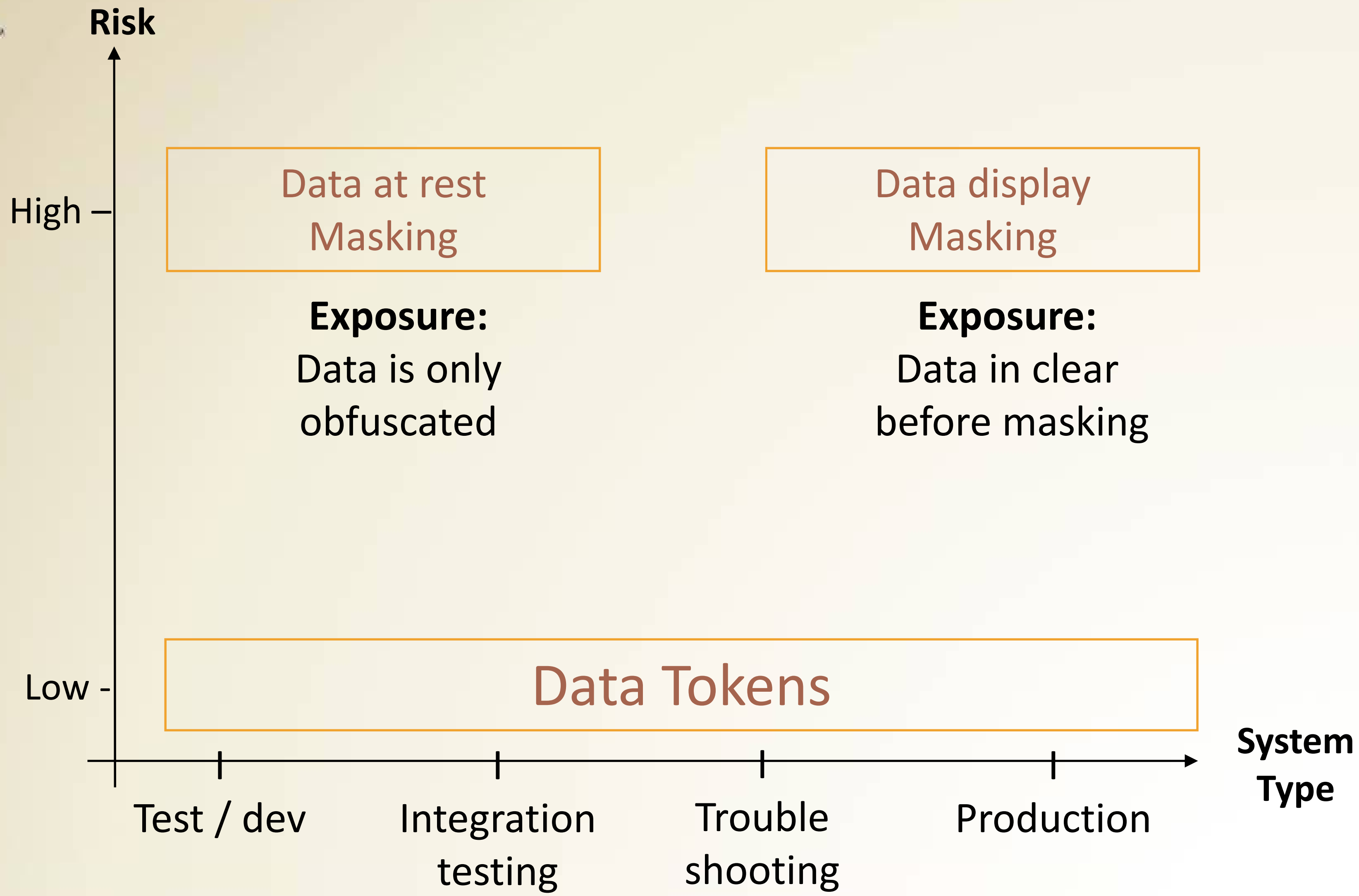
Data at rest Masking

Exposure:
Data is only obfuscated

Data display Masking

Exposure:
Data in clear before masking

Data Tokens = Lower Risk



Risk

High –

Low -

Data at rest Masking

Exposure:
Data is only obfuscated

Data display Masking

Exposure:
Data in clear before masking

Data Tokens

System Type

Test / dev

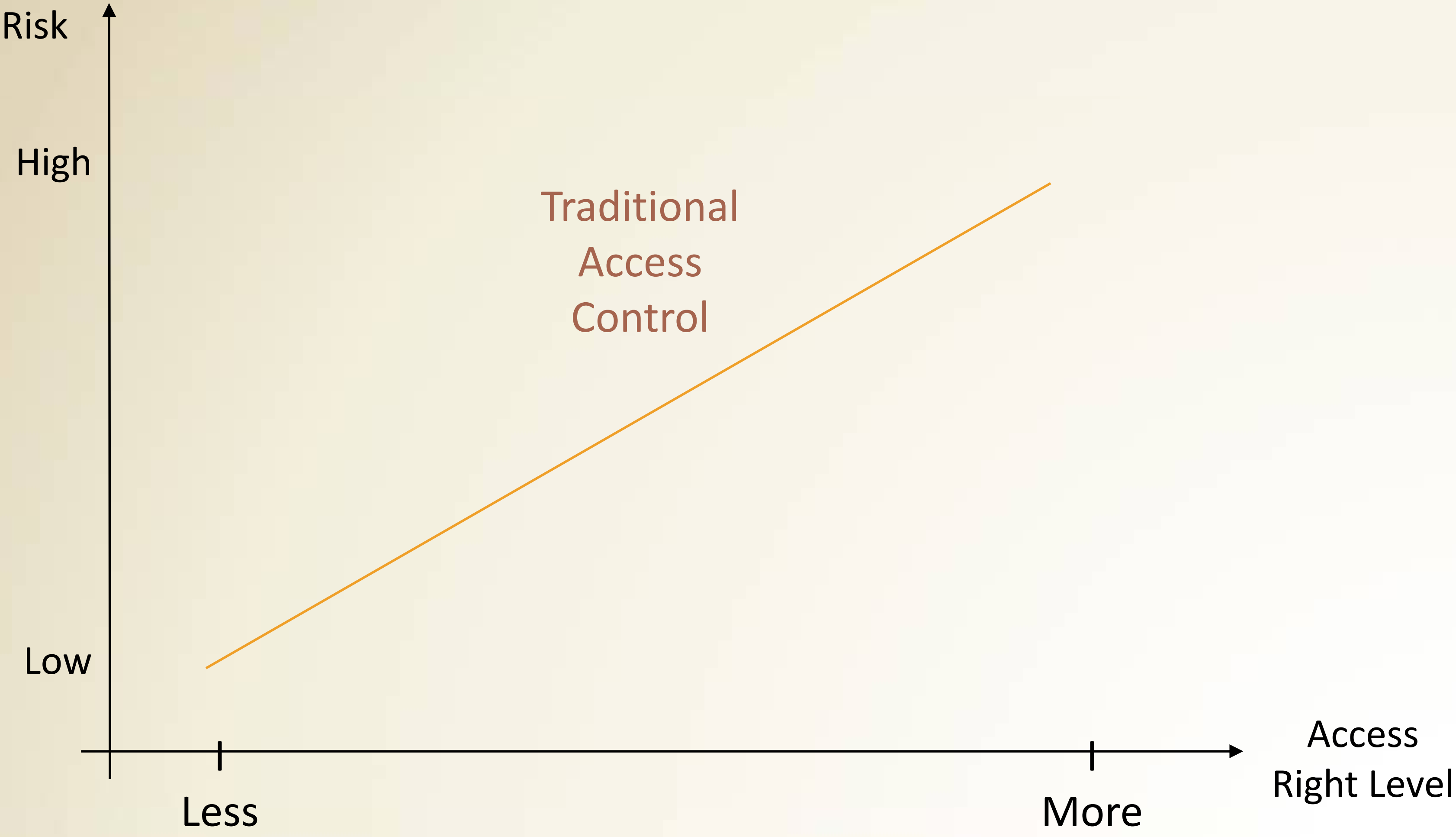
Integration testing

Trouble shooting

Production

CAN SECURITY HELP CREATIVITY?

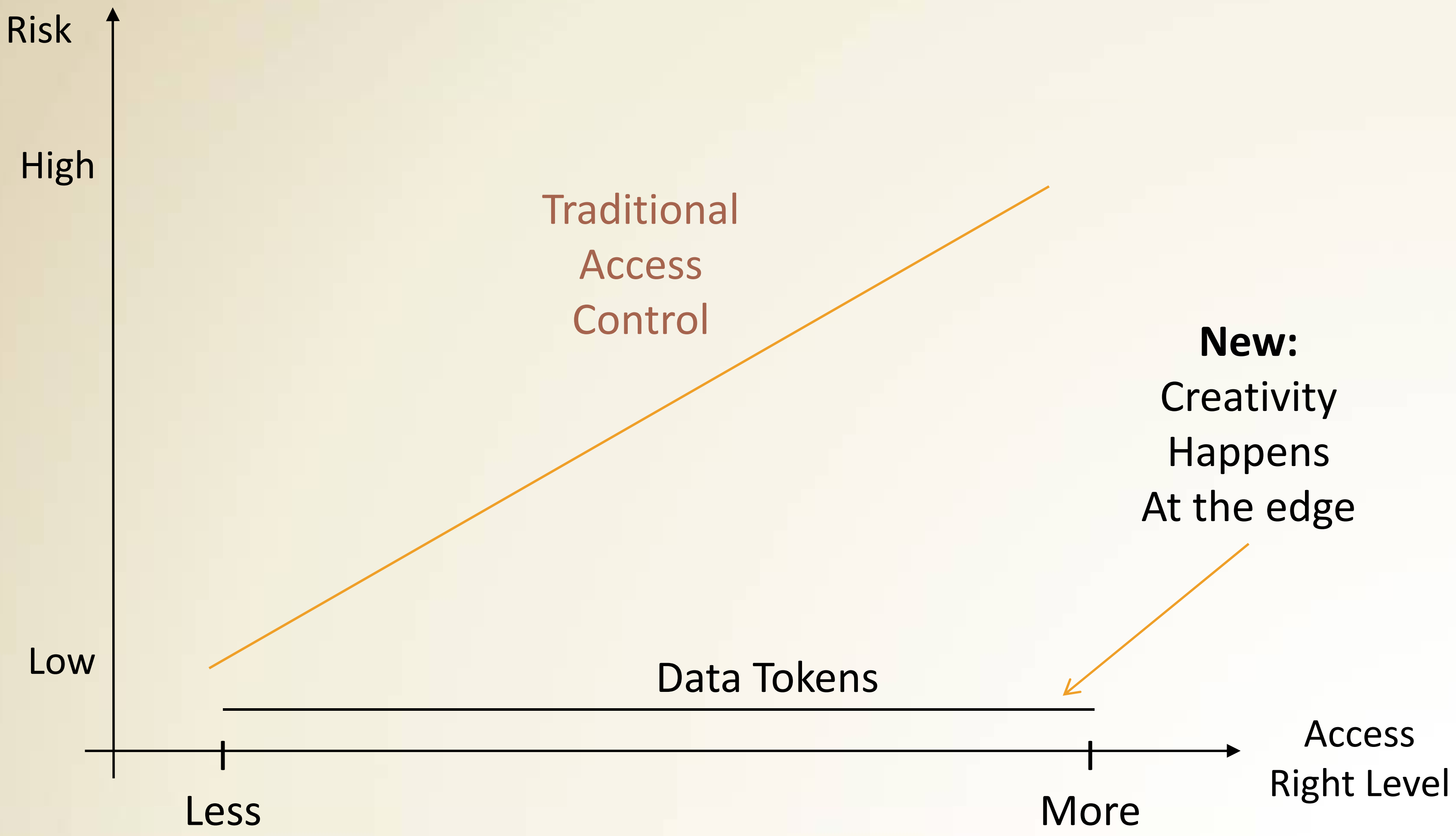
Old Security = Less Creativity



Source: InformationWeek Aug 15, 2011

Follow us @ISACANews
#NACACS

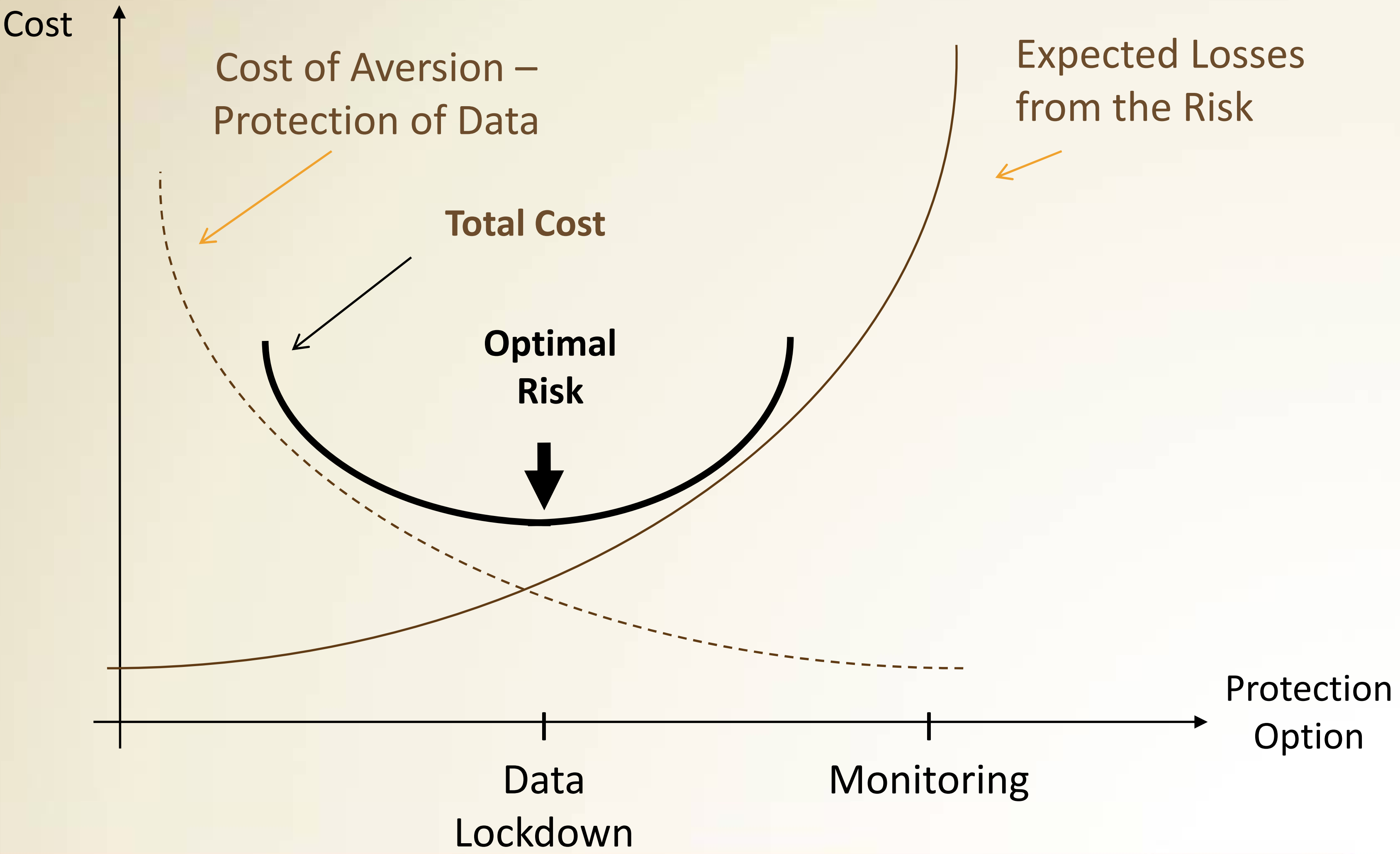
New Data Security = More Creativity



Source: InformationWeek Aug 15, 2011

WHAT IS THE IMPACT ON RISK MANAGEMENT?

Choose Your Defenses



DATA SECURITY ADVANCES ARE CHANGING THE BALANCE

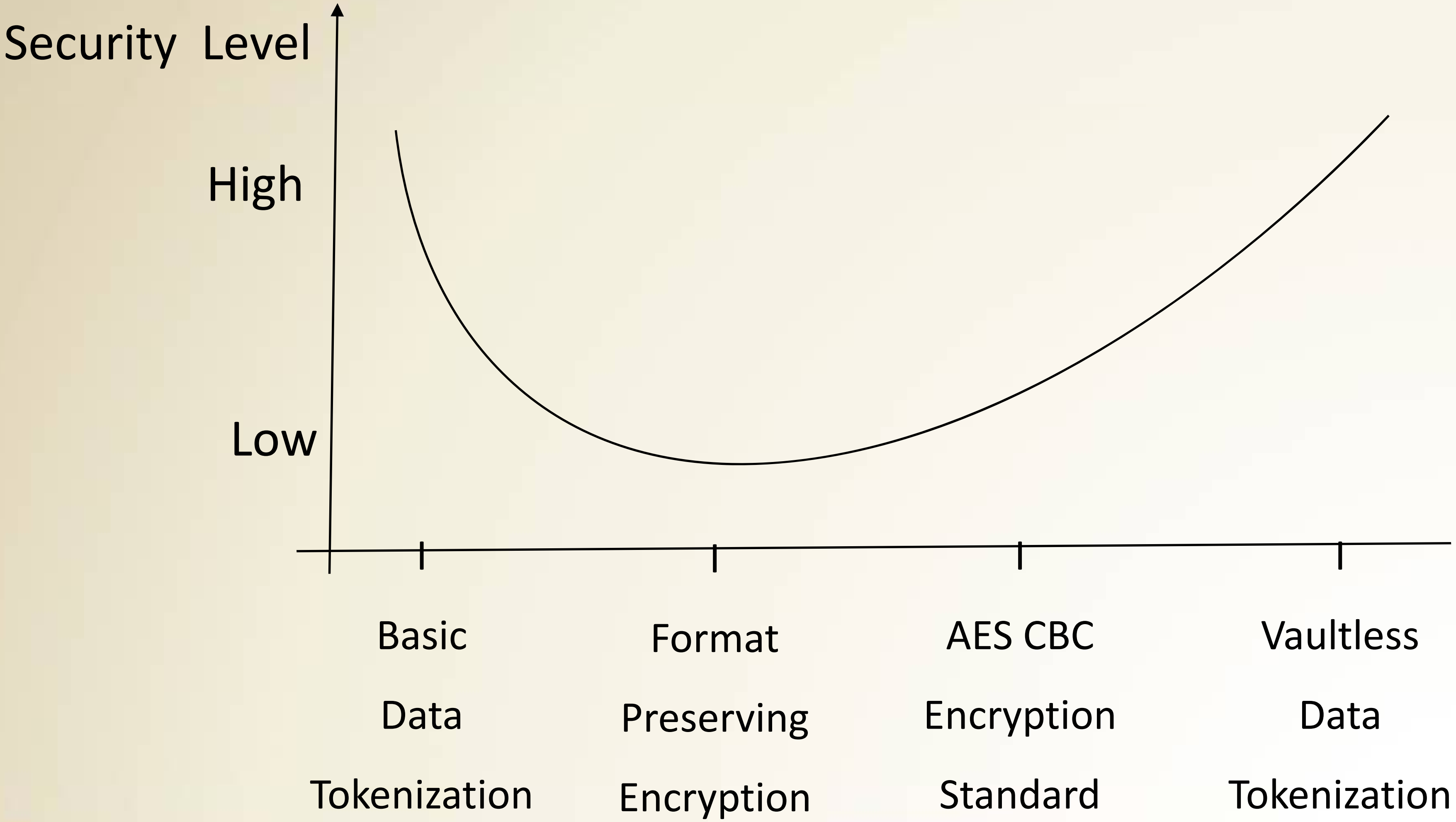
Matching Data Protection with Risk Level

Data Field	Risk Level
Credit Card Number	25
Social Security Number	20
Email Address	20
Customer Name	12
Secret Formula	10
Employee Name	9
Employee Health Record	6
Zip Code	3

Risk Level		Solution
High Risk (16-25)	🟥	Tokenization, strong encryption
Medium Risk (6-15)	🟨	Monitoring, masking, format controlling encryption
Low Risk (1-5)	🟩	Monitoring

SEPARATION OF DUTIES!

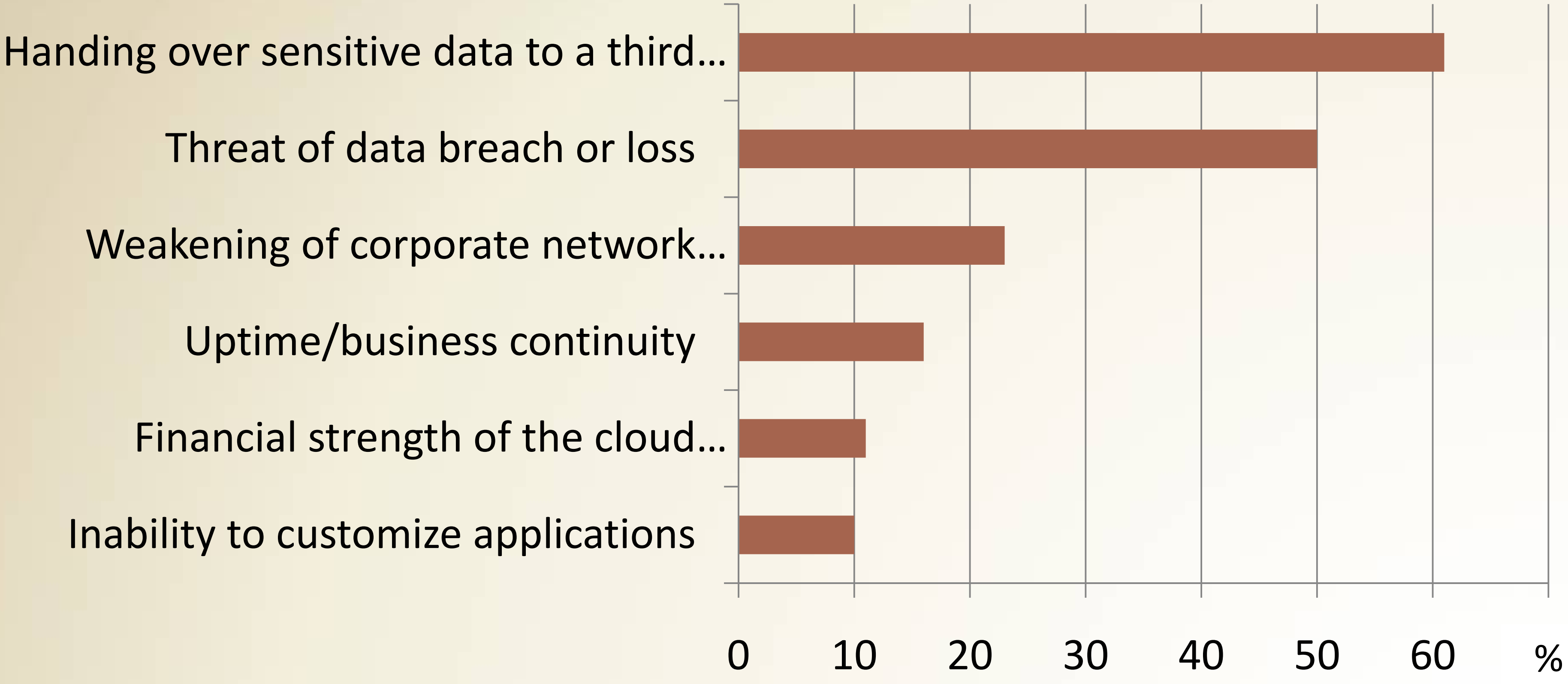
Security of Different Protection Methods



Follow us @ISACANews
#NACACS

HOW CAN I SECURE DATA IN CLOUD?

Risks with Cloud Computing



Source: The evolving role of IT managers and CIOs Findings from the 2010 IBM Global IT Risk Study

Follow us @ISACANews
#NACACS

PCI & Cloud

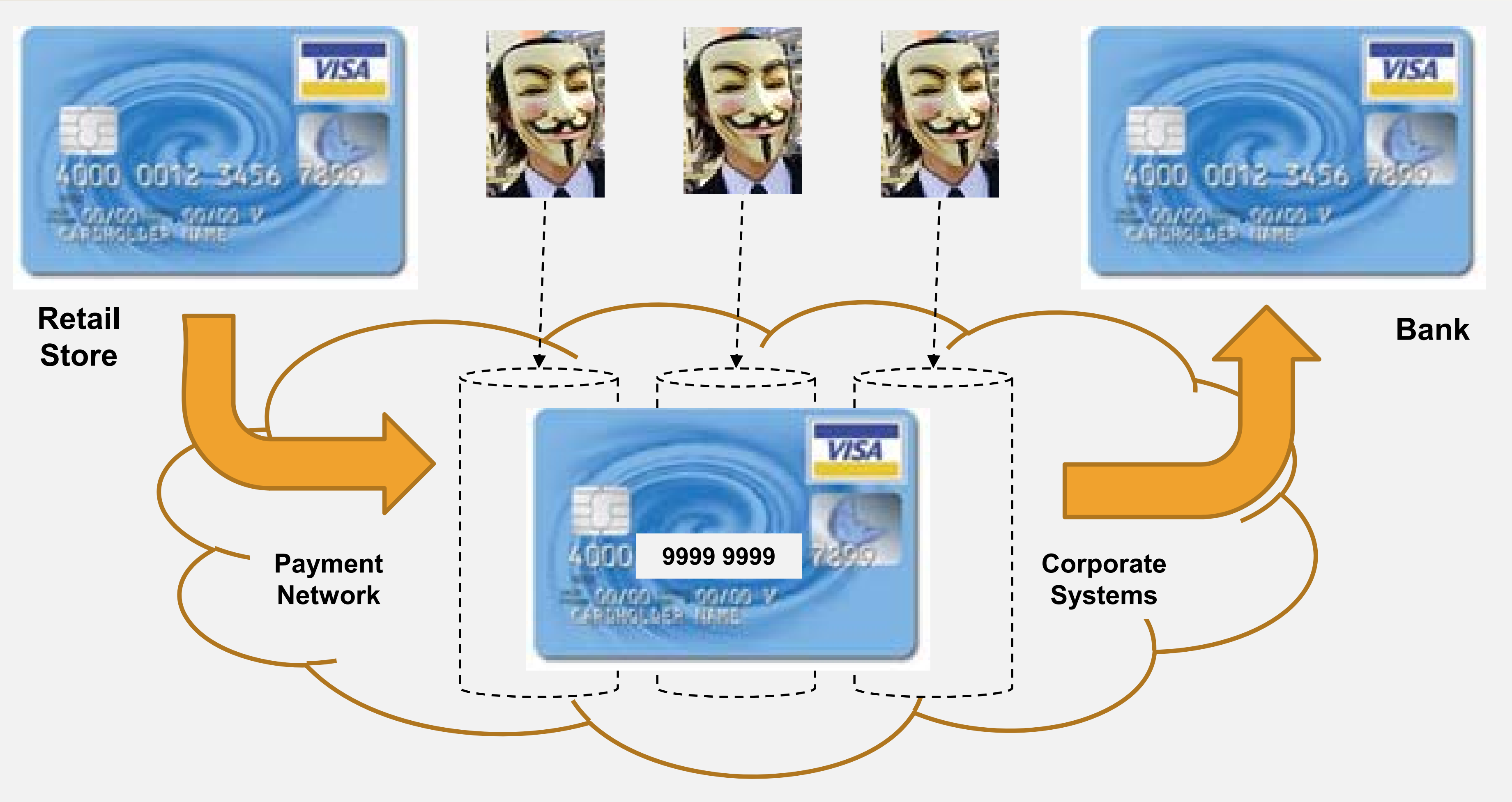
- The PCI council's security caution over virtualization is justified, because virtualized environments are susceptible to types of attacks not seen in any other environment
  - Bob Russo, general manager of the PCI Security Standards Council

Amazon’s PCI Compliance

- PCI-DSS 2.0 doesn't address multi-tenancy concerns
- You can store PAN data on S3, but it still needs to be encrypted in accordance with PCI-DSS requirements
  - Amazon doesn't do this for you -- it's something you need to implement yourself; including key management, rotation, logging, etc.
  - If you deploy a server instance in EC2 it still needs to be assessed by your QSA
- Your organization's assessment scope isn't necessarily reduced
  - It might be when you move to something like a tokenization service where you reduce your handling of PAN data

Source: securosis.com

Securing The Data Flow with Tokenization



Why Tokenization?

Why Tokenization

1. No Masking
2. No Encryption
3. No Key Management

$

Why Vaultless Tokenization

1. Lower Cost / TCO
2. Better
3. Faster

Conclusion

- Organizations need to understand their data flow and current security technologies
  - Determine most significant security exposures
  - Target budgets toward addressing the most critical issues
  - Strengthen security and compliance profiles

- Achieve the right balance between business needs and security demands
  - I increasingly important as companies are changing their security strategies to better protect sensitive data
  - Following continuing attacks

About Protegrity

- Proven enterprise data security software and innovation leader
  - Sole focus on the protection of data
  - Patented Technology, Continuing to Drive Innovation
- Growth driven by compliance and risk management
  - PCI (Payment Card Industry), PII (Personally Identifiable Information), PHI (Protected Health Information)
  - US State and Foreign Privacy Laws, Breach Notification Laws
- Cross-industry applicability
  - Retail, Hospitality, Travel and Transportation
  - Financial Services, Insurance, Banking
  - Healthcare, Telecommunications, Media and Entertainment
  - Manufacturing and Government

Thank you!

Q&A

ulf.mattsson@protegrity.com

www.protegrity.com

203-326-7200

Trust in, and value from, information systems