

# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-R04

## Is Your Third-Party Service Provider Vendor Management Program Good Enough?

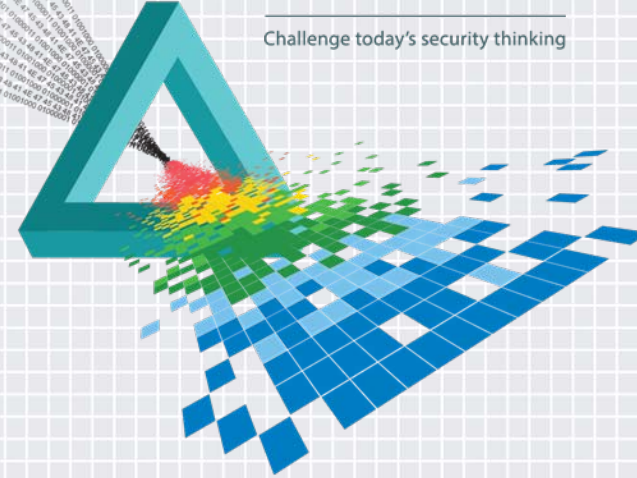
**Patrice Coles**

---

Compliance Manager  
A Global Service Provider  
[patrice@kraasecurity.com](mailto:patrice@kraasecurity.com)

# CHANGE

Challenge today's security thinking



# Why do we care?

OCC BULLETIN 2013-29

Subject: Third-Party Relationships  
Date: October 30, 2013

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

## Description: Risk Management Guidance

### Summary

This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.<sup>1</sup>

The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.<sup>2</sup>

This bulletin rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk." This bulletin supplements and should be used in conjunction with other OCC and interagency



# Piling on!

## PCI SECURITY STANDARDS COUNCIL PUBLISHES THIRD-PARTY SECURITY ASSURANCE GUIDANCE

—PCI Special Interest Group guidance provides merchants with payment security best practices for working with third-party providers—

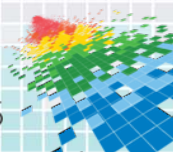
WAKEFIELD, Mass., 7 August 2014 — Businesses are rapidly adopting a third-party operations model that can put payment data at risk. Today, the [PCI](#) Security Standards Council, an open global forum for the development of payment card security standards, published guidance to help organizations and their business partners reduce this risk by better understanding their respective roles in securing card data. Developed by a PCI Special Interest Group ([SIG](#)) including merchants, banks and third-party service providers, the information supplement provides recommendations for meeting PCI Data Security Standard (PCI DSS) requirement 12.8 to ensure payment data and systems entrusted to third parties are maintained in a secure and compliant manner.

Breach reports continue to highlight security vulnerabilities introduced by third parties as a leading cause of data compromise. According to a 2013 study<sup>1</sup> by the Ponemon Institute, the leading mistake organizations make when entrusting sensitive and confidential consumer information to third-party vendors is not applying the same level of rigor to information security in vendor networks as they do in their own.



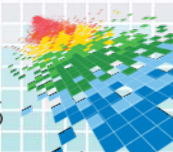
# Observations – Proactive?

- ◆ NOT proactive
  - ◆ Historical
  - ◆ New technologies
  - ◆ 3<sup>rd</sup> party assessments
  - ◆ Performance based metrics



# Observations – Ongoing Competence?

- ◆ Do NOT ensure ongoing competence of third party service providers
  - ◆ Follow up
  - ◆ Status change
  - ◆ Test / Audit / Monitor




# Observations – Alignment?

## RSA Conference 2015

San Francisco | April 20-24 | Moscone Center

- ◆ NOT well aligned to the customer or the provider's objectives and complexity – SCOPING!

- ◆ Type of service
- ◆ Data
- ◆ Scoping “on the hoof”
- ◆ ?s that do no apply

 PCI Standards Council
Information Supplement • Third-Party Security Assurance • August 2014

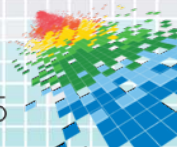
### 3.1 Determining the Scope of the Services Provided

When engaging a TPSP, initially, the entity should consider determining the scope of the TPSP's involvement with regard to storing, processing, or transmission of cardholder data and the resulting effect on the security of the CDE. Because TPSP involvement and services may impact the level of risk assumed by the entity when processing payment transactions, thorough due diligence is critical in determining which TPSP is appropriate and which third-party services may be needed.

Defining the level of involvement of a TPSP is crucial to understanding the overall risk assumed by the entity related to PCI DSS compliance. The entity may elect to engage an outside party to assist with the assessment of the scope of services to be provided by the TPSP and the applicability of those services to the entity's PCI DSS compliance. Questions that may help with this process may include:

- Given the current payment ecosystem and payment channels, what services (security, access, etc.) would affect or impact the CDE and/or CHD? How the services are structured within the TPSP facilities?
- What technology and system components are used by the TPSP for the services provided?
- Are additional third parties used by the TPSP in the delivery of the services provided?
- What other core processes/services are housed in the TPSP facilities that may impact the services provided? What technology is used for those core processes/services?
- How many facilities does the TPSP have where CHD is or will be located?

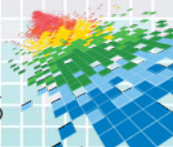
**Note:** The scope and services to be provided by a TPSP will depend on the specific facts and circumstances and services provided. Although the foregoing list of questions may be useful in determining scope and services, this list is not exhaustive. Each organization seeking to engage a TPSP must determine what is relevant in light of the circumstances, the organization's payment environment, the proposed TPSP's role, and other factors determined to be important through thorough due diligence.





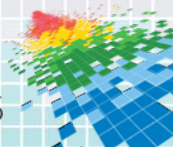
# Observations – Checkboxes / SIGs

- ◆ “Checkbox”
  - ◆ 3rd party assessment timeframes
  - ◆ Forced Y/N
- ◆ “Standardized”
  - ◆ One size fits all
- ◆ Does not produce a clear measure of the effectiveness of the provider



# Observations – When Tools Go Bad

- ◆ Automation is good, but:
- ◆ Inflexible answers – Whether they apply or not
- ◆ Evolving – Imperceptibly, if at all (same questions)
- ◆ Third party risk assessment services
- ◆ Do NOT let Siri drive!





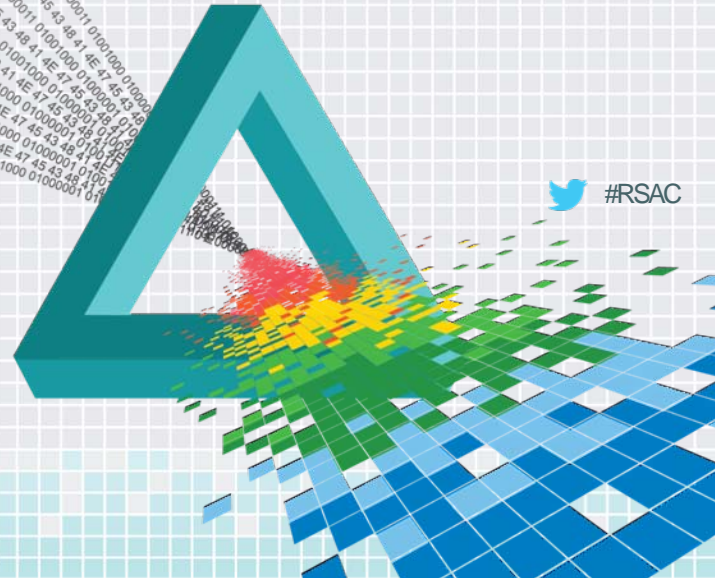
# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

So....

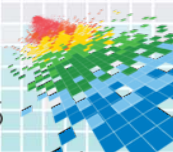


How do we redo the voodoo  
that we do?



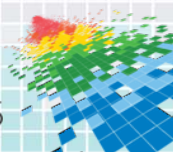
# Redo The Voodoo - Proactive

- ◆ Learn
- ◆ Trends
- ◆ Assess new technologies
- ◆ Monitor
- ◆ KRI
- ◆ Published diligence



# Redo The Voodoo - Evolve

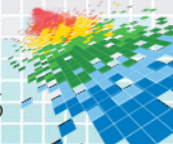
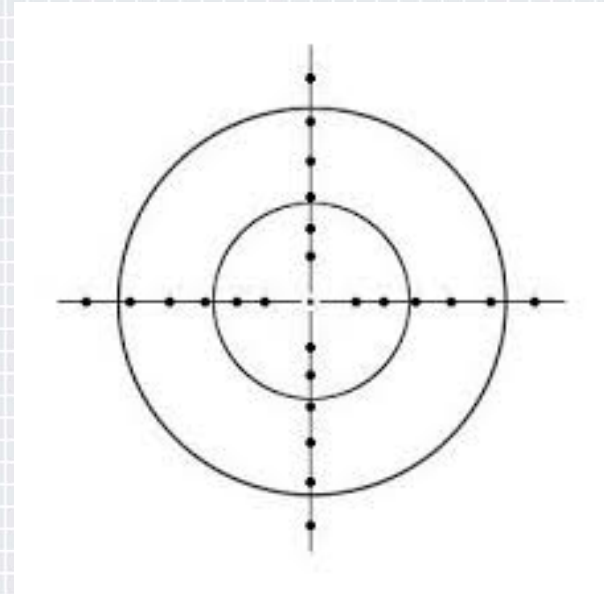
- ◆ Review / Test
  - ◆ Frequency / Maturity
  - ◆ Test / Audit / Monitor
  - ◆ Agreed Upon Procedures / Onsite
  - ◆ TSP Exposure to Evolving Threats
  - ◆ Q:





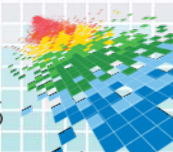
# Redo The Voodoo - Scoping

- ◆ Scoping – (OMG SCOPING!)
  - ◆ Framework
  - ◆ Customer and vendor
  - ◆ Understand the service
  - ◆ Understand the risk



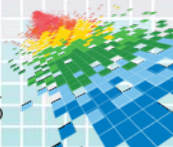
# Redo The Voodoo - Scoping

- ◆ Scoping – (OMG SCOPING!)
  - ◆ Applicable questions
  - ◆ Assess only what matters
  - ◆ Measure / weight



# Redo the Voodoo – Checkboxes / SIGs

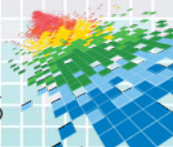
- ◆ Use it where feasible
- ◆ N/A Explain
- ◆ Get the most ! for your \$
- ◆ Choose carefully!





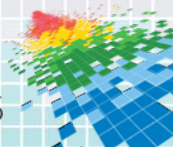
# Redo the Voodoo - Standardized

- ◆ Good starting point
- ◆ Scope
- ◆ Apply the same principles of your own risk management program



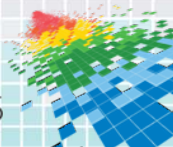
# Redo the Voodoo - Effectiveness

- ◆ Assess only what matters
- ◆ Review frequency
- ◆ Integrate into your risk register where appropriate



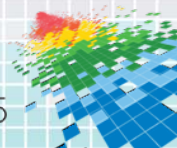
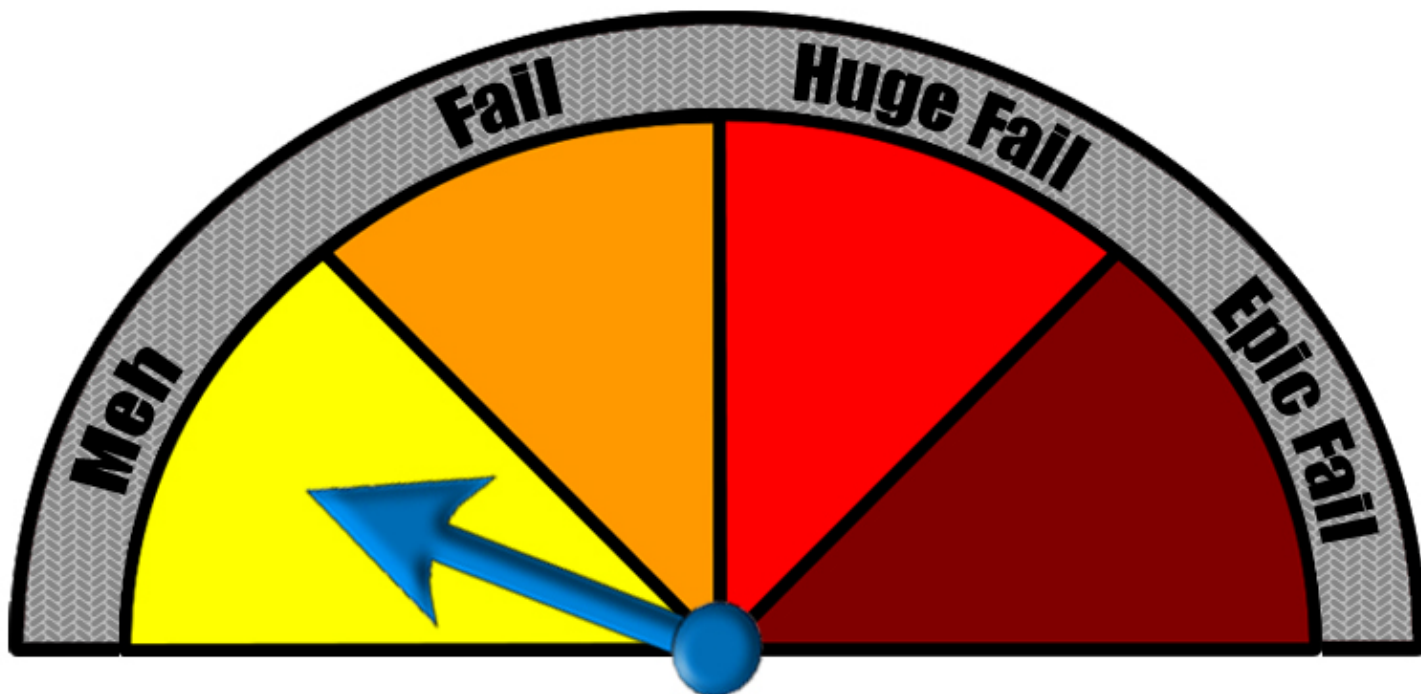
# Redo the Voodoo - Quantify Percentage Complete

<b>Index:</b>	<b>% Comp</b>
<a href="#">Business Information</a>	3%
<a href="#">Documentation Request List</a>	N/A
<a href="#">A. Risk Management</a>	0%
<a href="#">B. Security Policy</a>	0%
<a href="#">C. Organizational Security</a>	0%
<a href="#">D. Asset Management</a>	0%
<a href="#">E. Human Resources Security</a>	0%
<a href="#">F. Physical and Environmental</a>	0%
<a href="#">G. Communications and Ops Management</a>	0%
<a href="#">H. Access Control</a>	0%
<a href="#">I. Information Systems Application Development and Maintenance</a>	0%
<a href="#">J. Information Security Incident Management</a>	0%
<a href="#">K. Business Continuity and Disaster Recovery</a>	0%
<a href="#">KA. Business Continuity and Disaster Recovery Product</a>	0%
<a href="#">L. Compliance</a>	0%
<a href="#">M. Additional Questions</a>	N/A
<a href="#">Glossary</a>	N/A
<a href="#">Overview</a>	N/A
<a href="#">Version History</a>	N/A
<a href="#">Formula Notes</a>	N/A



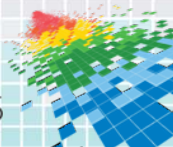


# Redo the Voodoo - Quantify Suck-O-Meter



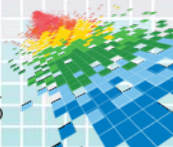
# Redo The Voodoo – Tools R Good!?!

- ◆ Automated processes
- ◆ Workflow
- ◆ Calculations
- ◆ Follow up
- ◆ BUT only the human should drive



# Case Study

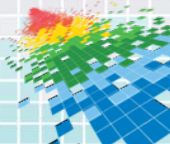
- ◆ Standard diligence questionnaire (DDQ)
- ◆ 500 questions, 20 artifacts
- ◆ Improperly scoped – uh oh!
- ◆ Start again
- ◆ Now under duress





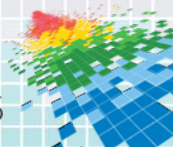
# Take Aways

- ◆ Service Providers:
  - ◆ Self serve
  - ◆ Publish
  - ◆ Help customers learn



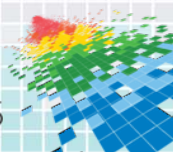
# Take Aways

- ◆ Customers
  - ◆ Conduct initial risk assessment as part of vendor selection process
  - ◆ Ask yourself iteratively:
    - ◆ How can I make the TSP risk management better align with the business's strategy and effectively manage risks?
    - ◆ How can I make the TSP risk management process more efficient and get better value out of the effort?



# Conclusion

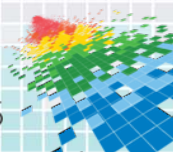
- ◆ You still own the risk
- ◆ Maturity
- ◆ Evolve





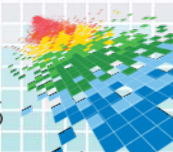
# References and Resources

- ◆ Razient – <http://www.razient.com>
- ◆ Shared Assessments - <https://sharedassessments.org/>
  - ◆ SIG
  - ◆ VMM
  - ◆ AUP
  - ◆ Certification
- ◆ COSO



# References and Resources

- ◆ FFIEC IT Handbook - <http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx>
  - ◆ Program guidance for examination
  - ◆ Work programs
- ◆ CFPB - <http://www.consumerfinance.gov/guidance/supervision/manual/>
  - ◆ Exam Manual



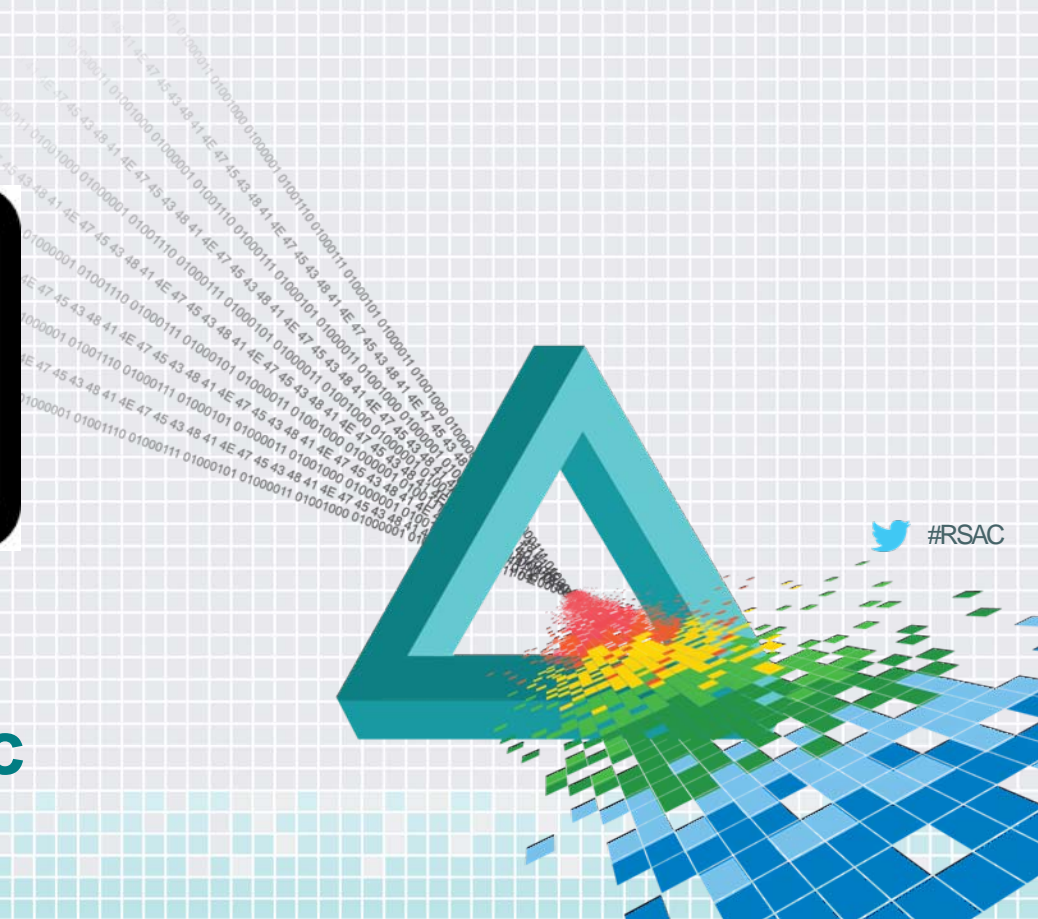
# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

## Questions



Contact me.....  
LinkedIn or  
Twitter @BabyBearSec



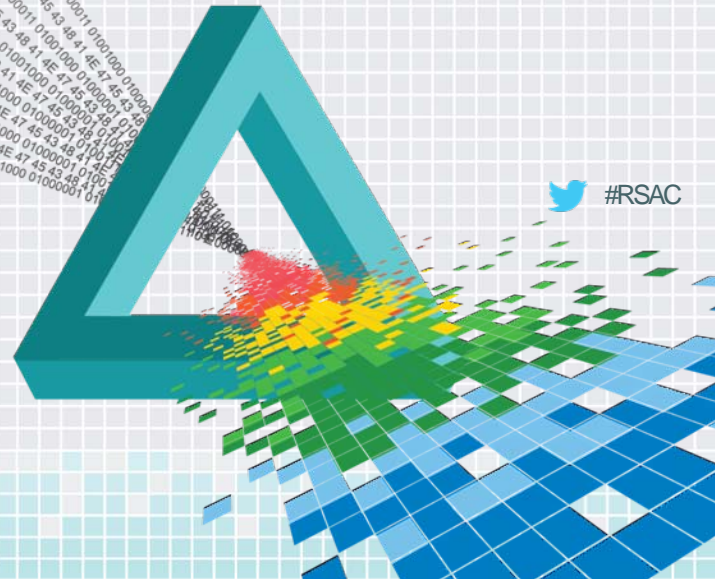


# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

If you want to contact me.....

LinkedIn or  
[patrice@kraasecurity.com](mailto:patrice@kraasecurity.com)



 #RSAC