

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

Session ID: ECO-T10

From Cowboys to Sales Engineers: Building Mature Security Services

Julian Mihai

Manager

BlueCross BlueShield of IL, TX, NM, OK, MT

Tom Baltis

VP, Chief Information Security Officer

Blue Cross Blue Shield of Michigan

CHANGE

Challenge today's security thinking



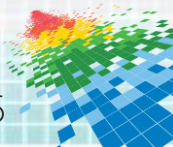
Introduction

Many companies and industries are facing disruptions.

Information security services that worked in stable environments can't meet new demands.

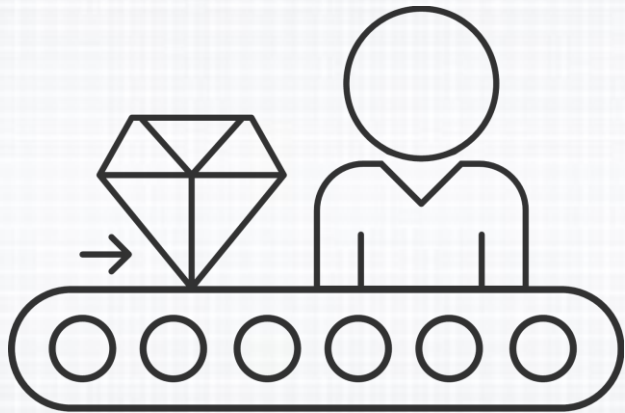
If security services aren't run like a business, 'heroic' individuals will take over with negative consequences.

We will present three case studies to show how to evolve your services and succeed during disruptions.



Information Security in Stable Environments

In stable business and technology environments, process-oriented security services deliver value with:

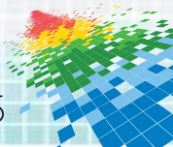


“Production Engineer”

Well-defined objectives and consistent processes

Timely, high-quality deliverables

Enhancement through various frameworks
(e.g. CMMI, ITIL, NIST)



Business and Technology Transformation

Companies are facing dramatic **business & technology disruptions** but traditional security services can't scale or adapt rapidly.



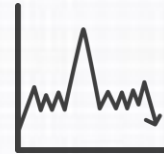
Business
innovation more
pervasive
(e.g. Uber, iWatch)



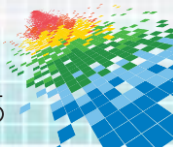
Emerging
technologies
accelerating



Cyber attacks
intensifying
(e.g. healthcare)

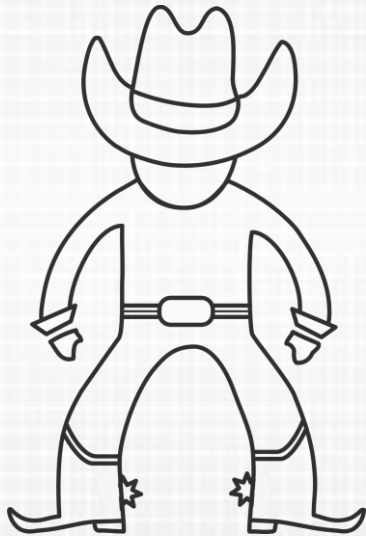


Unpredictable
demand peaks
more common



Cowboys Take Over by Default

As traditional approaches break down in dynamic or disruptive environments, “cowboys” will:



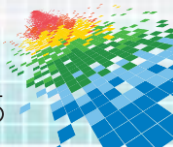
“Renegade Cowboy”

Handle demand spikes through heroics

Hire hotshot experts for each new security domain or technology

Impose inflexible solutions by waving the governance stick

Neglect service improvement and disregard customer feedback



The Problems with Cowboys

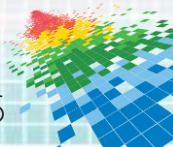
This ad hoc approach may work in the short term but will eventually lead to:

High costs and future rework

Inconsistent or reduced quality

Long ramp-up times during demand spikes

Pushback from stakeholders



Modern Security Services Development

Instead, evolve security services into businesses that scale and adapt.



Running Security Services Like a Business



“Sales Engineer”

Sales & Marketing

Build awareness, buy-in, and brand for security services

Service Offerings

Develop and maintain catalog of scalable services based on customer feedback

Delivery Operations

Deliver efficiently, reliably, aligned with demand

Data and Information Technology

Create, manage, and utilize data and systems to optimize all service functions

Human Resources

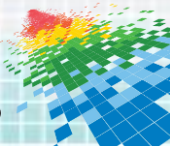
Source and staff with right skills, experience levels, and type (FTE/contractors)

Finance

Obtain internal or external financing to develop and deliver services

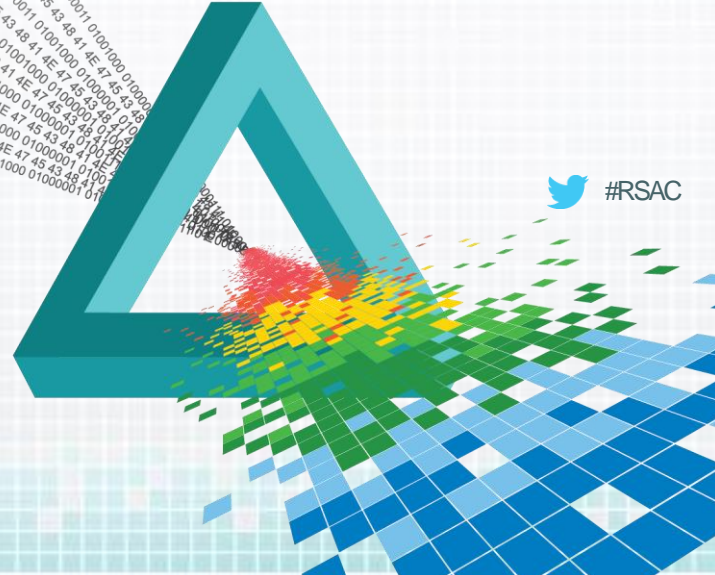
Administrative

Ensure timely execution of all active engagements (consulting engagement manager)







Case Study 1: Product Management

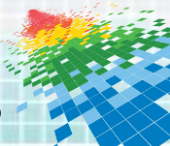


 #RSAC

Product Feature and Stakeholder Gap

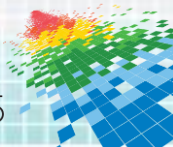
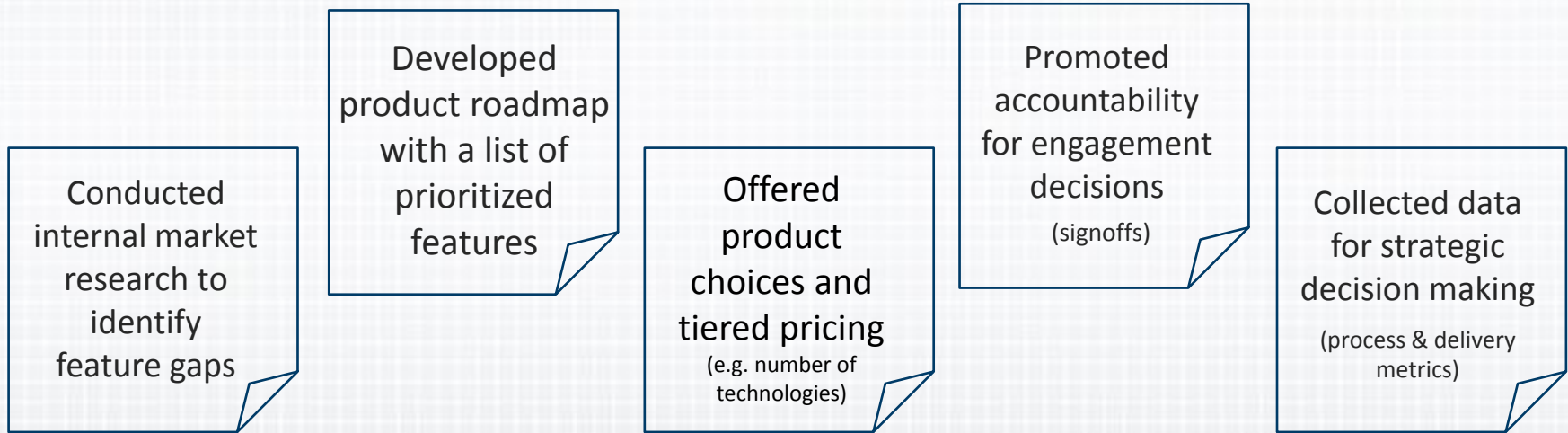
Security services are not managed as products and fail to meet evolving customer needs. Prior to 2012, our security design service was becoming misaligned with stakeholders.

 	Reduced Effectiveness
	Pushback from Stakeholders
	Low Satisfaction & Bad Publicity
	One size fits all pricing model



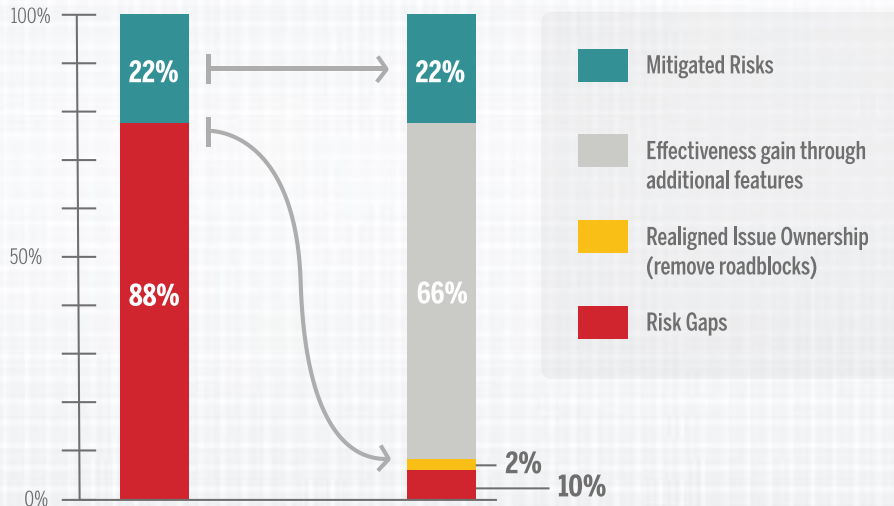
Product Management Approach

We treated the design service as a product and applied product management techniques to better meet stakeholder needs, e.g. moving away from single design and pricing model.



Benefits of Security Product Management

The new security design service offered multiple size and pricing levels, resulting in increased coverage and a dramatic decrease in risks.

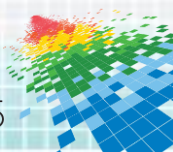


Other benefits:

Early adoption of security solutions

Reduced rework

Improved operational visibility



Lessons Learned

1

Adapt service features to stakeholder needs using frequent feedback

2

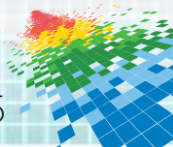
Provide only realistic design options with tiered cost and risk levels

3

Hold stakeholders accountable for their decisions

4

Conduct customer experience surveys



Passive Demand Management

Security services can't manage demand effectively without marketing.

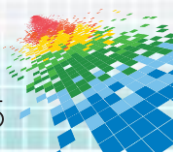
Prior to 2013, IT leaders at my organization lacked awareness of the design service or understanding of its value proposition, resulting in:

Sporadic
or delayed
engagements

Low or
variable
security
utilization

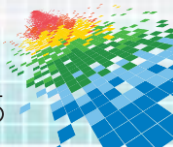
Risk of
being
replaced

Excessive
security
risks



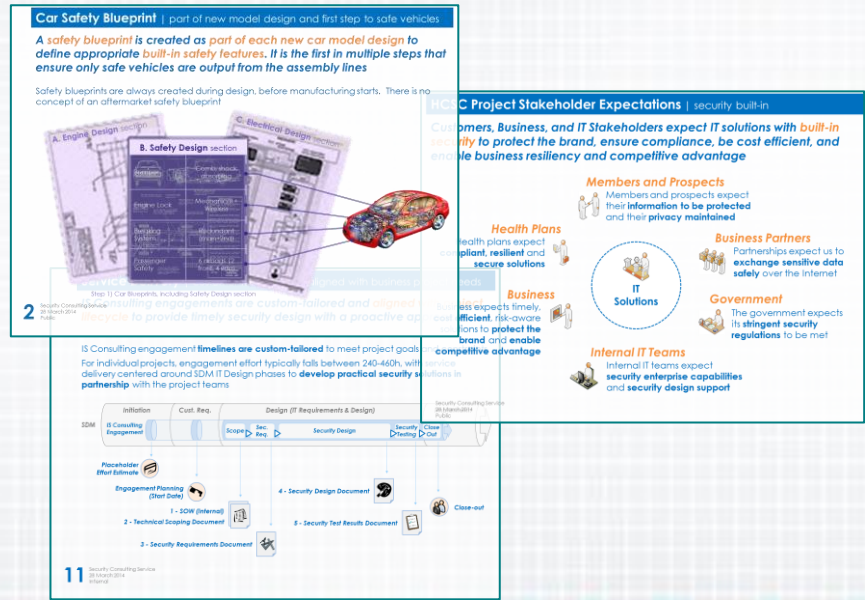
Marketing Development Approach

In 2012, we started to actively market to better manage demand and resource utilization.



Sample 'Pre-Sales' Marketing Collateral

We customized messages to each stakeholder, e.g. ease of technical integration for IT or recurring costs for business. The presentations:



Car Safety Blueprint | part of new model design and first step to safe vehicles

A safety blueprint is created as part of each new car model design to define appropriate built-in safety features. It is the first in multiple steps that ensure only safe vehicles are output from the assembly lines

Safety blueprints are always created during design, before manufacturing starts. There is no concept of an aftermarket safety blueprint

IT Project Stakeholder Expectations | security built-in

Customers, Business, and IT Stakeholders expect IT solutions with built-in security to protect the brand, ensure compliance, be cost efficient, and enable business resiliency and competitive advantage

- Members and Prospects**: Members and prospects expect their information to be protected and their privacy maintained
- Business Partners**: Partnerships expect us to exchange sensitive data safely over the internet
- Government**: The government expects its stringent security regulations to be met
- Internal IT Teams**: Internal IT teams expect security enterprise capabilities and security design support
- Health Plans**: Health plans expect compliant, resilient and secure solutions
- Business**: Business expects timely, efficient, risk-aware solutions to protect the brand and enable competitive advantage

IS Consulting engagement **timelines** are custom-tailored to meet project goals. For individual projects, engagement effort typically falls between 240-460h, with delivery centered around SDM IT Design phases to develop practical security partnership with the project teams

SDM IT Design Phases: Initiation, Cust. Req., Design (IT Requirements & Design), Security Design, Security Testing, Close-out

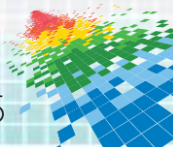
Placeholder Effort Estimate

Engagement Planning (Effort Only)

- 1 - SOW (Internal)
- 2 - Technical Scoping Document
- 3 - Security Requirements Document
- 4 - Security Design Document
- 5 - Security Test Results Document

Close-out

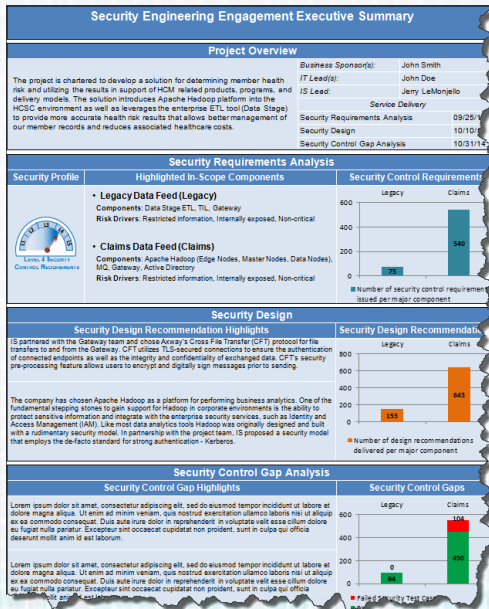
- Used non-IT metaphors
- Addressed misconceptions
- Proactively answered questions
- Invested in visuals



Sample 'Post-Sales' Marketing Collateral

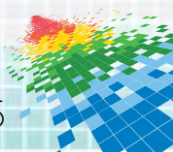
We connected deliverables to specific business benefits.

Executive Summary & Thank You emails



Created 1-page visual summary supported by hard data

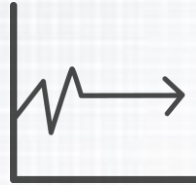
Thanked all our stakeholders to gain future support



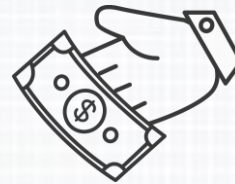
Benefits of Service Marketing



Reduced pushback
and clear value
proposition



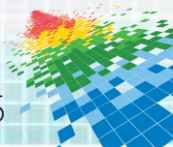
More predictable
demand



Pre-allocated
budget instead of
variable



Enhanced product
features through
feedback



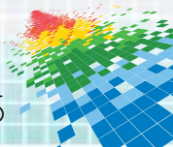
Lessons Learned

1 Develop clear value proposition for the service

2 Build visually appealing, concise, and relevant service marketing materials

3 Always Be Closing (ABC)

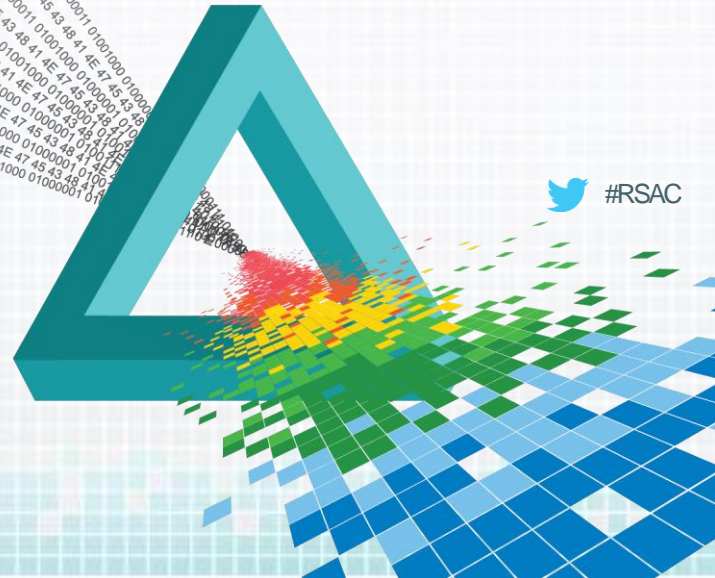
4 Enhance customer engagement by building long-term relationships





Case Study 3:

Scalable Operations



Security Design Services Difficult to Scale

Major business changes driven by healthcare reform triggered a IT implementation spike from 2011-2013. Initially, my organization thought security architecture could not scale.



Typical responses and outcomes:

Hire many contract architects

Overload existing staff

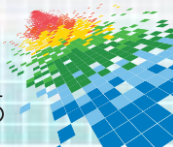
Take shortcuts on standards and process



Inconsistent quality

High cost or future rework

Resource burnout, turnover,
and lost institutional knowledge



Building Security Scalability Approach

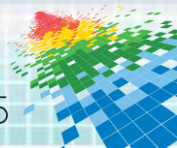
We maximized service scalability by using a predefined set of product components rather than building custom deliverables.

Mature architecture process to analyze, design, and make specific technical security recommendations

Technology-agnostic security systems analysis to create **technical security recommendations**

Prebuilt repository of custom requirements, test cases, and communications

Resource pool of generalist security experts with a process mindset



Sample Process Artifacts

We used libraries of prebuilt artifacts to automate tasks that can be executed without architectural expertise.

Stakeholder	Communication Objectives
Project Manager	<ul style="list-style-type: none"> Request distribution deliverable Request agreement to incorporate Provide assurance that the security cooperation with the IA and SA Provide assurance that the requirements scope Provide high level progress report
Solution Architect	<ul style="list-style-type: none"> Request agreement to incorporate Request review of the Requirements Request feedback on the technical Understand why we do not provide Requirements to cut-and-paste in

To: <Solution Architect(s)>, <Infrastructure/Application Architects>
 Cc: <Project Manager(s)>, <Service Lead>

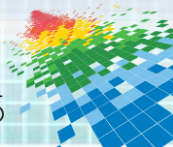
Subject: Security Engineering Engagement - <Project Name>
 Document <version#>

Program Stakeholders

Communication plan with predefined messages and communication objectives for each expert SME interaction

Requirement ID	Requirement
1	Authentication to the component or interface requires transaction present a digital certificate or security token (individual or component) for the lifetime of the transaction.
2	SR-CL4-AN1 The digital certificates or security tokens used for authentication and verifiable by a trusted third party.
3	SR-CL4-AN2 The digital certificates or security tokens used for authentication and verifiable by a trusted third party.
4	SR-CL4-AN3 The private key used to verify the issuance of the certificate is strongly resistant to brute force attacks.
5	SR-CL4-AN4 The digital certificate or security token used for authentication periodically limit the time available for an attack.
6	SR-CL4-AN5 The private key used to verify the issuance of the certificate be shared, and must never be transmitted across a network.
7	SR-CL4-AN6 The authentication private keys or passwords must be stored on a secure disk or in a database.
8	SR-CL4-AZ1 Authorization to access the component or interface requires, by the association of trusted attributes, a minimum, by the association of trusted attributes.
9	SR-CL4-AZ2 The trusted attributes (e.g., username) used to authenticate must be explicitly approved through a workflow process.
10	SR-CL4-AZ3 The trusted attributes (e.g., username) used to authenticate must be explicitly used in the definition granting or denying access to the component or interface.

Security requirements, design patterns, and test scenarios for common use cases



Benefits of Operationalized Architecture

-80%

**Reduced ramp up time
for new resources**
(12 weeks to 2)

\$500k

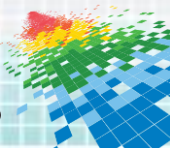
Lowered costs

30-40%

Improved delivery time

60%

Increased time to market
(1.5 months > 2 Weeks)



Lessons Learned

1

Hire highly skilled experienced professionals to make decisions

2

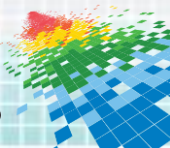
Combine repeatable process and security experts— not technology experts

3

Use work artifact templates (SOW, requirements, design, etc.) not just for final deliverables

4

Develop communications plan





Conclusions



Summary

To meet the challenges of profound business and technology transformations, security services must be run like a business. We illustrated the benefits of applying product development, marketing and operations concepts:

1

Scalable delivery with increased responsiveness and consistent quality

2

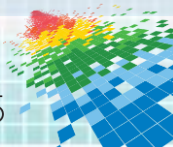
Higher satisfaction and engagement through customer focus

3

Relevant options to meet every internal need

4

Rapid investment reprioritization and strategic agility



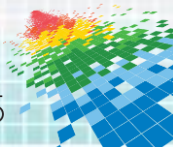
Takeaways and Next Steps

Prepare your organization to embrace demand variability through standardization and repeatable processes

Incorporate sales and marketing techniques to better manage demand and resources

Use metrics and customer feedback mechanisms to continuously improve your engagement model and process artifacts

Establish an appropriate engagement and pricing model



Questions?

Julian Mihai
julian.us@outlook.com

Tom Baltis
tbaltis@bcbsm.com

