RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: CXO-W02F

CISO as Change Agent: Getting to Yes

Frank Kim
Chief Information Security Officer
SANS Institute
@fykim

Outline

- Catch the Culture
- Shape the Strategy
- Build the Business Case

RSAConference2017

#1 Catch the Culture

Organizational Culture

"Culture eats strategy for breakfast."

- Peter Drucker

Ability to Change

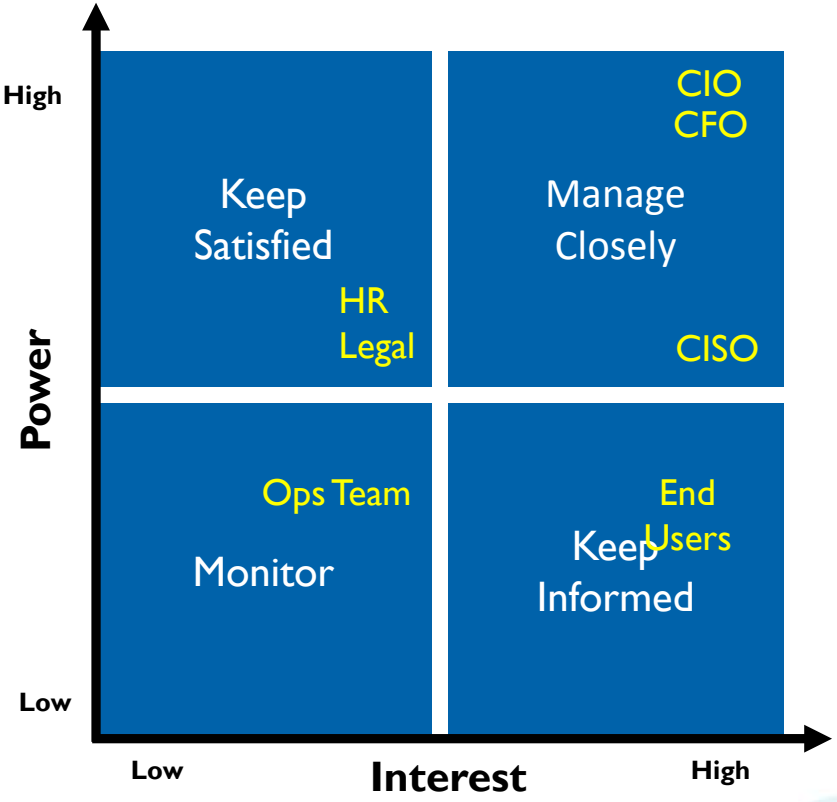
"What makes companies great is inevitably what makes companies fail, whenever that day comes."

- Ben Thompson

Security Culture

- Introduce change
  - At the rate the organization can accept it
- Examples
  - Phishing click through rates
  - Security exception requests

Stakeholders and Culture



From mindtools.com

RSAConference2017

#2 | Shape the Strategy

Establish a Vision

- Stakeholders don't value expertise
  - They value results
- By understanding what they value
  - We can learn to innovate with the business

"If I asked people what they wanted they would have said faster horses."

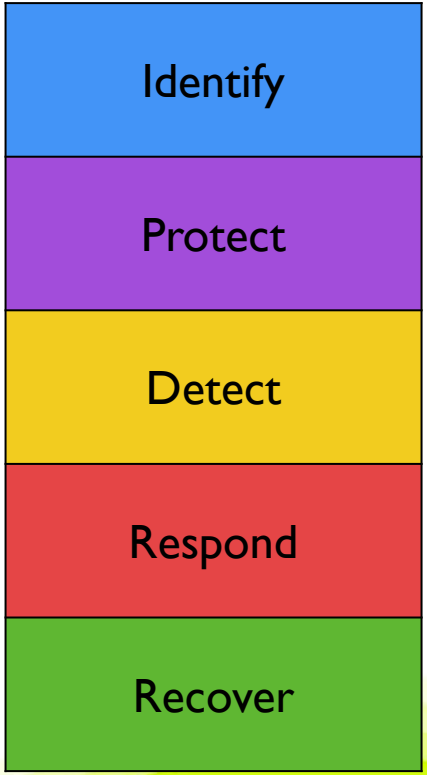
- Henry Ford

Identify a Security Framework

- Security frameworks provide a blueprint for
  - Building security programs
  - Managing risk
  - Communicating about security
- Many frameworks share common security concepts
- Examples include
  - ISO 27000 Series
    - 27001 – ISMS requirements
    - 27002 – Code of practice
    - 27003 – Implementation guidance
    - 27004 – Measurement
    - 27005 – Risk management
  - COBIT
  - ENISA Evaluation Framework
  - NIST Cybersecurity Framework

NIST Cyber Security Framework

- Composed of three parts
  - Core, Implementation Tiers, Profiles
- Defines a common language for managing security risk
  - Core has five Functions that provide a high-level, strategic view of the security life cycle
- Helps organizations ask:
  - What are we doing today?
  - How are we doing?
  - Where do we want to go?



Critical Security Controls (CSC)

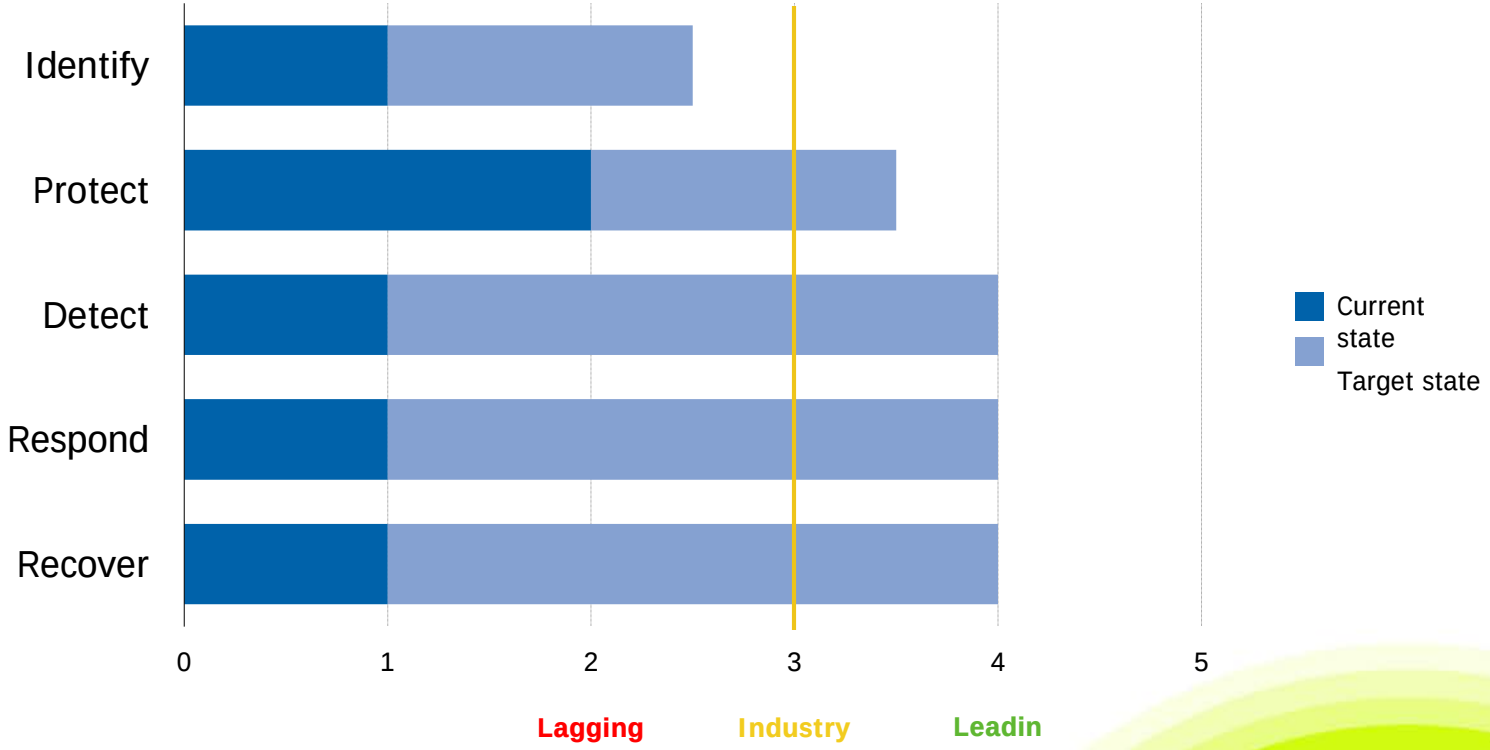
- Maintained by the Center for Internet Security (CIS)
  - Subset of the comprehensive catalog in NIST SP 800-53
  - Prioritizes a smaller number of actionable controls that mitigate the most pervasive attacks

Critical Security Controls (CSC) Matrix

CSC 1 Inventory of Authorized and Unauthorized Devices	**CSC 2** Inventory of Authorized and Unauthorized Software	**CSC 3** Secure Configurations for Hardware and Software	**CSC 4** Continuous Vulnerability Assessment and Remediation
CSC 5 Controlled Use of Administration Privileges	**CSC 6** Maintenance, Monitoring, and Analysis of Audit Logs	**CSC 7** Email and Web Browser Protections	**CSC 8** Malware Defenses
CSC 9 Limit & Control of Network Ports, Protocols, Services	**CSC 10** Data Recovery Capability	**CSC 11** Secure Configurations for Network Devices	**CSC 12** Boundary Defense
CSC 13 Data Protection	**CSC 14** Controlled Access Based on the Need to Know	**CSC 15** Wireless Access Control	**CSC 16** Account Monitoring and Control
CSC 17 Security Skills Assessment	**CSC 18** Application Software Security	**CSC 19** Incident Response and Management	**CSC 20** Penetration Tests and Red Team Exercises

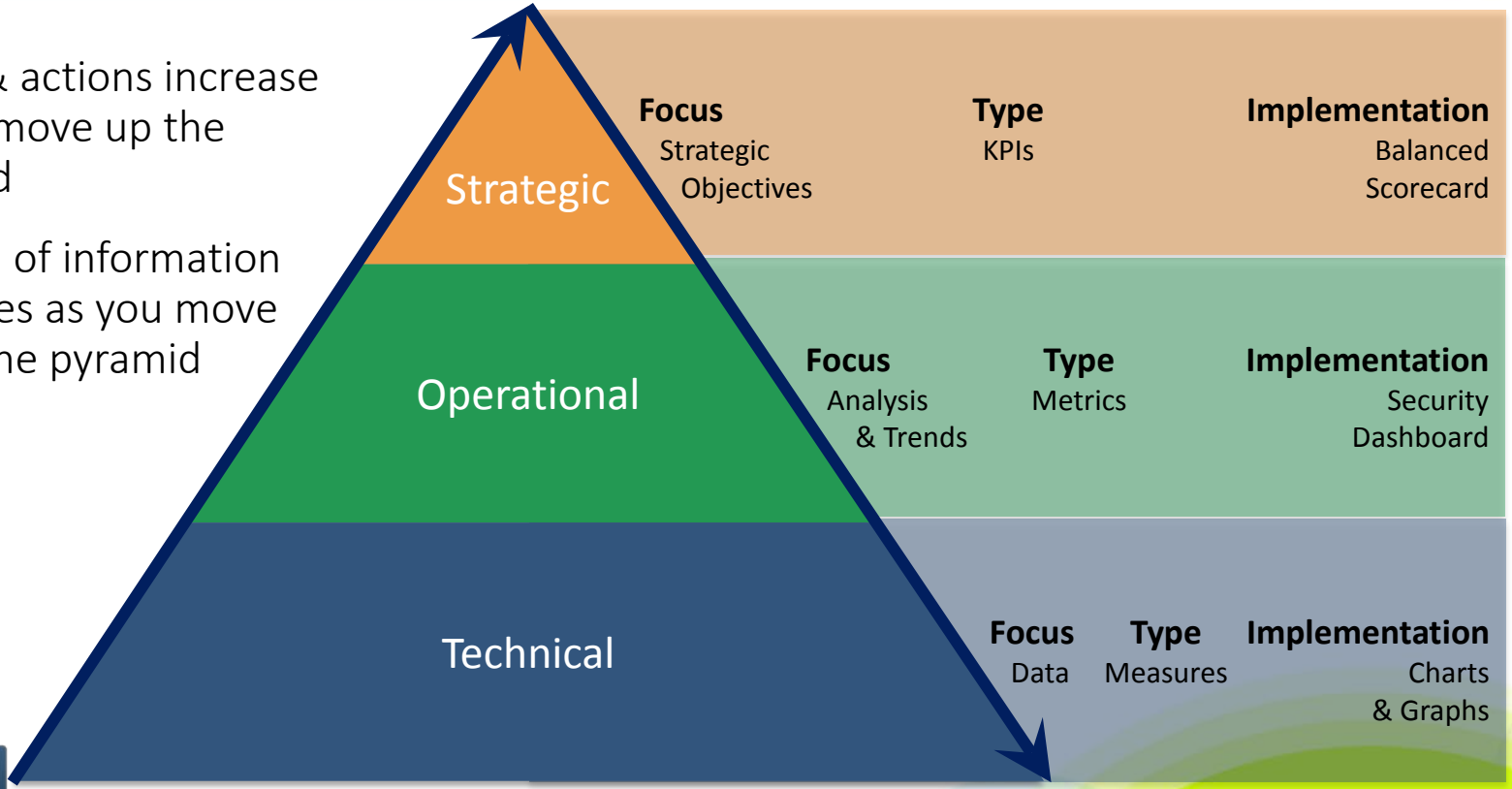
SANS

Maturity Comparison Example



Metrics Hierarchy

- Focus & actions increase as you move up the pyramid
- Volume of information increases as you move down the pyramid



Security Program Dashboard – Example

Financial/Stewardship

% Budget Allocated to Security

Target 5% ✓
Trend ➔

5%

YTD Security Budget Allocation

	Q1	Q2	Q3	Q4	YTD
Products	$575,000	$597,000	$425,000	$732,000	
Services	$1,590,000	$1,320,000	$1,190,000	$1,090,000	
Training	$326,000	$315,000	$427,000	$301,000	
Actuals	$2,491,000	$2,232,000	$2,042,000	$2,123,000	
Budget	$2,190,000	$2,211,900	$2,234,019	$2,256,359	
$ Variance	-$301,000	-$20,100	$192,019	$133,359	

Customer / Stakeholder

% of Products Delivered On Time

Target 95% ✓
Trend ↑

95%

Customer Satisfaction

Target 90% ✗
Trend ↑

85%

Internal Business Process

% of Developers Trained

Target 95% ✓
Trend ↑

97%

% of Developers with Certification

Target 95% ✗
Trend ↑

42%

Security Status – Example

Security Capability	Status	Trend	Highlights

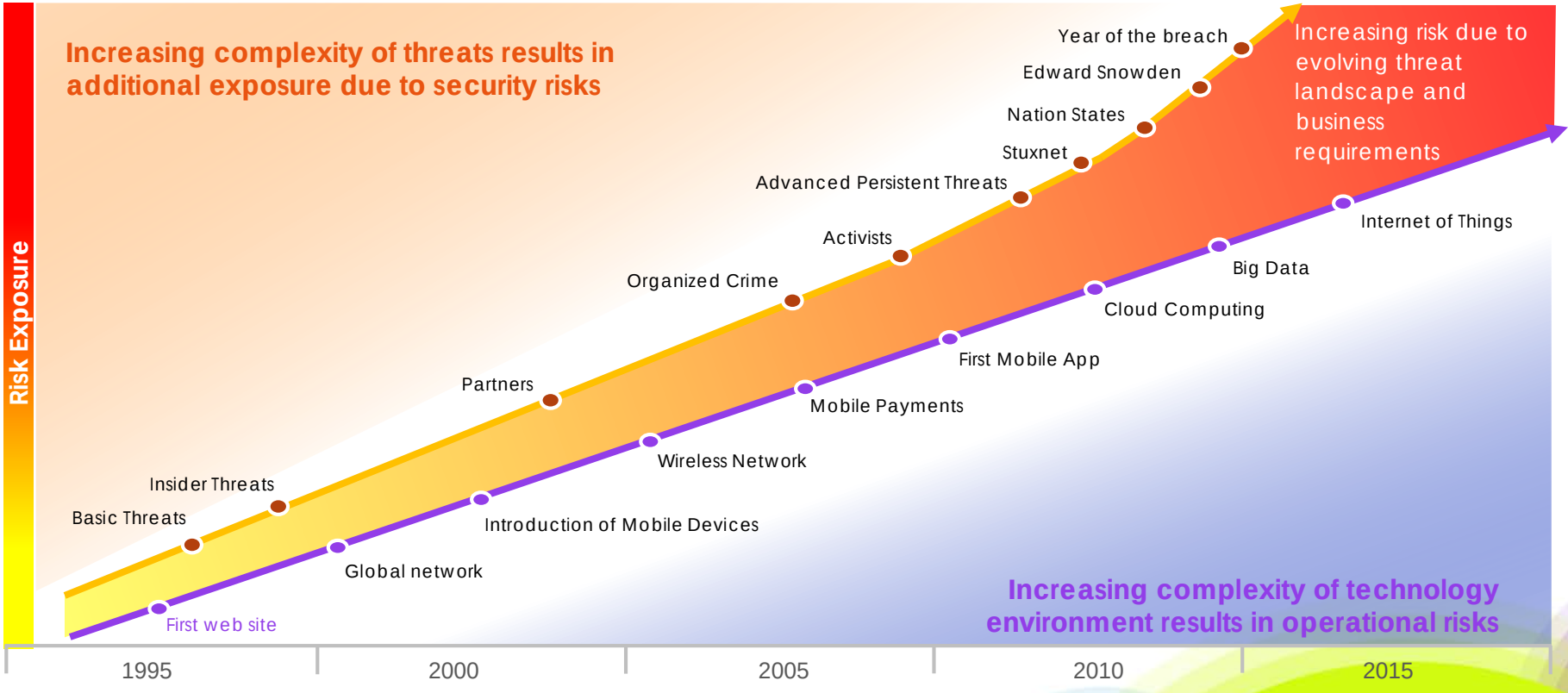
Identify: Manage risk to systems, assets, data, and capabilities	Yellow	↑	• 32% increase in unauthorized devices
			  • 29% IT
			  • 3 % HR
			• 27% increase in unauthorized software
			• Attributed to Q4 BYOD pilot

Protect: Ensure delivery of critical infrastructure services	Green	→	• 12% of users failed sponsored email phishing tests • 15% of employees have not passed security awareness assessments
Detect: Identify occurrence of a cybersecurity event	Green	↓	• 27% decrease in elevated access accounts • 275 total elevated access accounts
Respond: Take action regarding a detected cybersecurity event	Green	→	• 5% of database systems with sensitive information have not been scanned by vulnerability scanners
Recover: Maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event	Red	↑	• 34% of systems not enabled with up to date anti-malware • Attributed to Q4 BYOD pilot

RSAConference2017

#3 Build the Business Case

Risk Landscape



Bad Business Justification (DMARC)

DMARC is an email validation system designed to detect **email spoofing** by providing a mechanism to allow receiving **mail exchangers** to check that incoming mail from a domain is authorized by that domain's administrators and that the email (including attachments) has not been modified during transport.

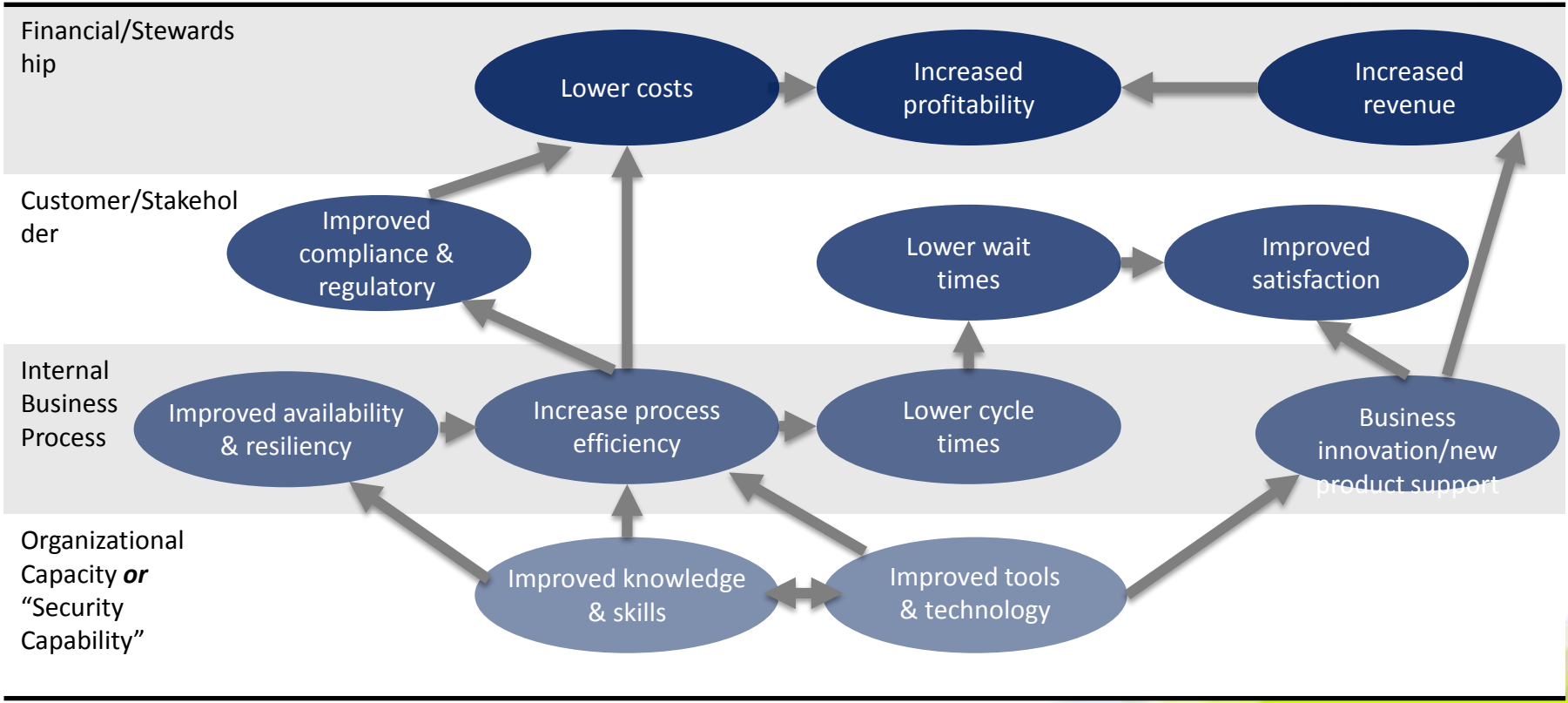
It expands on two existing mechanisms, the well-known Sender Policy Framework (**SPF**) and DomainKeys Identified Mail (**DKIM**), coordinating their results on the alignment of the domain in the **From: header** field, which is often visible to end users. It allows specification of policies (the procedures for handling incoming mail based on the combined results) and provides for reporting of actions performed under those policies.

Source: https://en.wikipedia.org/wiki/DMARC

Better Business Justification (DMARC)

The solution prevents scammers from sending **fraudulent email** to our customers. These fraudulent emails result in **stolen usernames, passwords**, and **fraudulent transactions**. The solution reduces the number of stolen accounts by 20%, **account fraud** by 10%, and the total amount of fraudulent transactions by **$1 million** per year.

Mapping to Strategic Objectives



Build Your Business Case

- As a manager and leader you are expected to
  - Understand the vision and mission of the company
  - Make security understandable to business leaders
- Don't just ask for the money
  - Sell the vision and how you will solve business problems
- Let the case speak for itself
  - Allow decision makers to come to their own conclusion
  - Outline three options with various pros and cons
    - Let them pick one

Provide Options

- Highlight trade-offs with business value, risk reduction, cost

	Option A	Option B	Option C
Business value	✓	✓✓	✓✓✓
Risk reduction			
Cost	$	$$	$$$

Summary

Leading Change

"It's not the strongest that survive or
the most intelligent that survive.
It's the ones that are most adaptable to change."

- Charles Darwin

Key Takeaways

- Catch the Culture
  - Understand culture and stakeholder motivations
  - Introduce change one step at a time
- Shape the Strategy
  - Utilize an industry recognized framework
  - Provide metrics that matter
- Build the Business Case
  - Don't just ask for the money
  - Sell a vision on how you will solve business problems

RSAConference2017

Frank Kim
fkim@sans.org
@fykim