RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CXO-W03

CISO Success Strategies:

On Becoming a Security Business Leader

Frank Kim

CISO

SANS Institute

@fykim

#RSAC

Outline

- Build Your Business Case
- Rocket Your Relationships
- Master Your Message

Build Your Business Case

Why Create a Business Case?

- Business case helps
  - Leadership estimate the costs and benefits
  - Management determine resource allocations
  - Put requests in broader organizational context

Security Business Case Traps

- "If we don’t do this we’ll get hacked"
- "It’s the right thing to do"
- "This new technology will solve all our problems”
- "It doesn’t cost that much"
- "Management doesn’t get it"

SANS

Approaches to Building a Security Business Case

Cost Approach

- How much does it cost to recover from a data breach?

Industry Comparison Approach

- What are comparable firms doing and paying?

Business Innovation Approach

- What can I gain from doing this?

SANS

Cost Approach

- Typically calculated using cost-per-record lost
- Ponemon Cost of Data Breach Study
  - $217 per record in 2015
  - $201 per record in 2014
  - $188 per record in 2013
- These numbers include direct & indirect costs
  - Engaging forensics experts, free credit monitoring
  - In-house investigations & communication
  - Extrapolated value of customer loss

Cost Approach Issues

- Not always accurate
  - Overestimates cost of large breaches
  - Underestimates cost of small breaches
- Verizon applied cost-per-record approach to cyber insurance claims data
  - Resulted in an estimated loss of only 58 cents per record

Ranges of Expected Loss

- Verizon developed a modified log-scale approach

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Approaches to Building a Security Business Case

- Cost Approach
  - How much does it cost to recover from a data breach?
- Industry Comparison Approach
  - What are comparable firms doing and paying?
- Business Innovation Approach
  - What can I gain from doing this?

Industry Comparison Approach

- What is reasonable for security based on:
  - Industry
  - Size
  - Region
  - Market position
    - Value of IP and assets
- Can be analyzed via
  - Spending comparison
  - Maturity comparison

Spending Comparison

- Percent of IT budget spent on security
  - Provides only a rough understanding of performance
  - Research from Gartner
    - 5.1% in 2013
    - 4.7% in 2012
    - 4.2% in 2011
- Can be a problematic metric
  - Depends on what is included in the percentage
  - Spending averages may not be a fit for every org
  - Do not make this the sole or primary focus of your business case

Maturity Comparison

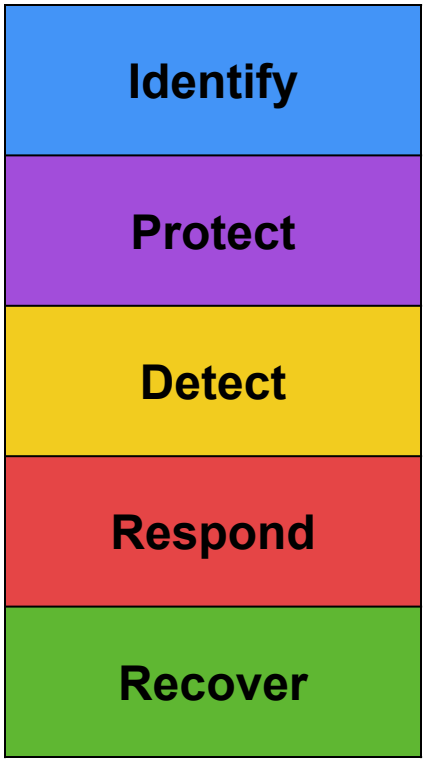
- What are other companies doing?
  - What is a reasonable level of maturity?
  - Can be very qualitative
- Where to get comparable data?
  - Information Sharing & Analysis Centers (ISAC)
    - FS-ISAC, REN-ISAC, etc.
  - Community projects
    - BSIMM, OpenSAMM
  - Research & consulting organizations
    - Gartner, Big 4, security service firms, etc.

Need for 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
  - COBIT
  - ENISA Evaluation Framework
  - NIST Cybersecurity Framework

NIST Cybersecurity Framework

- 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?



SANS

Tips on Using the Cybersecurity Framework

- Not everyone can or should implement the full Cybersecurity Framework immediately
  - New programs
  - Small security teams
  - Small and medium-sized businesses (SMBs)
- Useful as a way to frame the high-level components of your security program

Measuring Maturity

- Can't do everything at once
  - Need to define a progression of maturity
- Implementation Tiers
  - Defined in the Cybersecurity Framework
    - Tier 4 - Adaptive
    - Tier 3 - Repeatable
    - Tier 2 - Risk Informed
    - Tier 1 - Partial

"Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective."

- Need a way to measure maturity and determine where to invest

SANS

Maturity Models

- Maturity models provide a standard way to
  - Measure organizational capabilities
  - Identify areas of improvement
- Examples include
  - Capability Maturity Model Integration (CMMI)
  - Enterprise Strategy Group (ESG) Maturity Model
  - Gartner ITScore
  - Cybersecurity Capability Maturity Model (C2M2)
  - Building Security In Maturity Model (BSIMM)
  - Open Software Assurance Maturity Model (OpenSAMM)
  - Capability Immaturity Model (CIMM)

Capability Maturity Model Integration (CMMI)

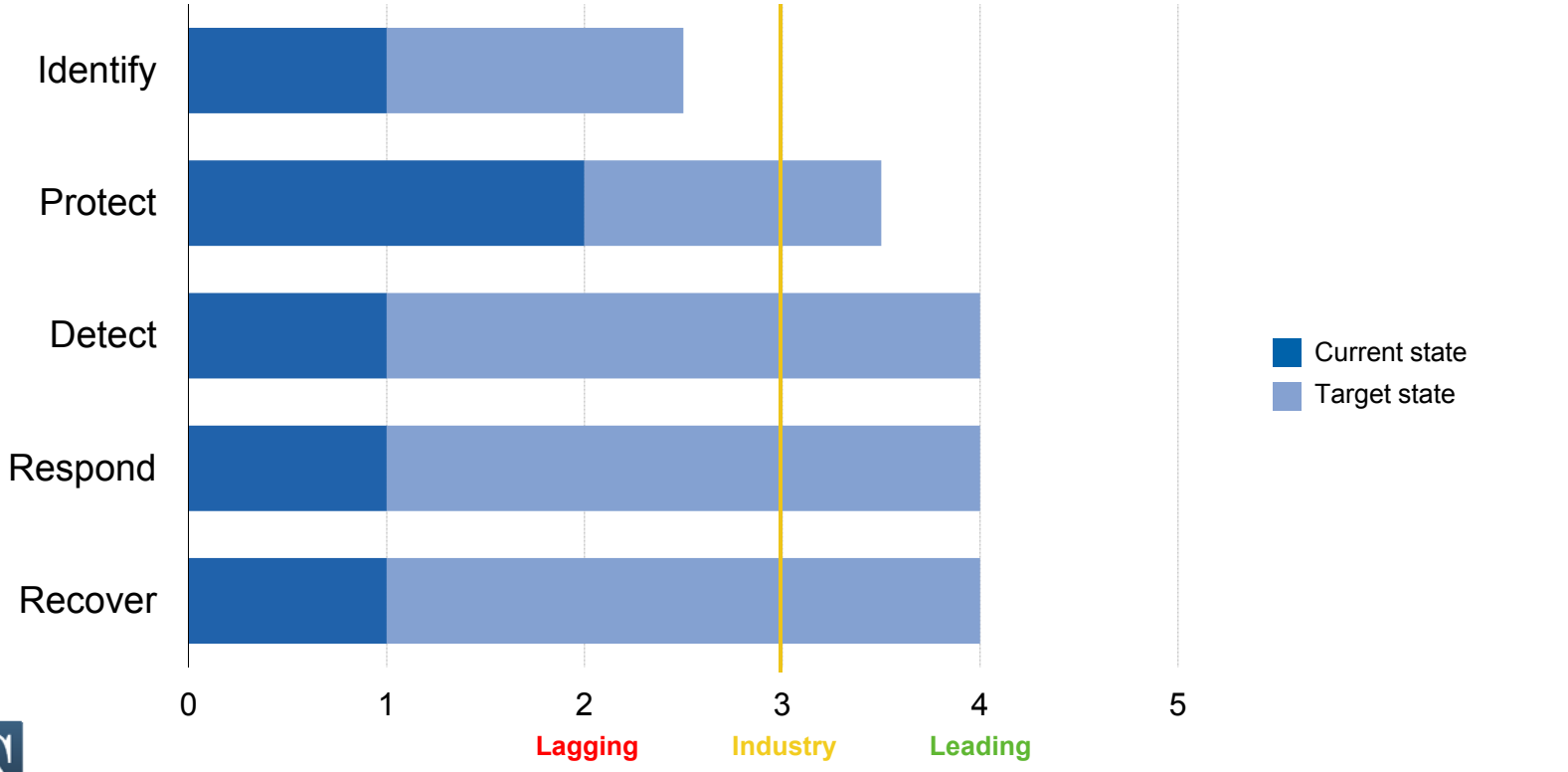
- Process model that defines what should be done to improve performance
  - Originally created to improve software development practices
  - Now expanded to cover development, services, and acquisitions
- Defines five maturity levels
  - Widely recognized and understood by executives, business leaders, and technology managers

CMMI Maturity Levels

Level 5 Optimizing	Focus on continuous process improvement
Level 4 Managed	Processes are measured and controlled
Level 3 Defined	Processes defined for the organization and are proactive
Level 2 Repeatable	Processes defined for projects but are reactive
Level 1 Initial	Processes are ad-hoc, chaotic, not repeatable Success requires competence and heroic effort

SANS

Maturity Comparison Example



Approaches to Building a Security Business Case

- Cost Approach
  - How much does it cost to recover from a data breach?
- Industry Comparison Approach
  - What are comparable firms doing and paying?
- Business Innovation Approach
  - What can I gain from doing this?

SANS

Business Innovation Approach

- Plan security investments based on:
  - Business opportunities
    - Key enterprise initiatives
    - Process improvement opportunities
    - New product support
  - Business requirements
    - Compliance, regulatory
  - Business risk
    - Annualized Loss Expectancy

Rocket Your Relationships

Stakeholder Management Strategy

- Understanding the business is not just about understanding the goals of the company
  - It's also about understanding key stakeholders, their motivations, interests, and power
- As you become more successful in your career, the initiatives you run will affect more people
  - It's likely your work will impact people who have power and influence over your projects
  - These people can support or block you

Understand Stakeholder Motivations

- Stakeholders are both organizations & people
  - Identify the specific individuals within each group
  - They may have different views of your project
  - So you need to tailor your approach
- Stakeholders can affect your efforts because they have:
  - Power to “veto”, “vote”, or “voice” their opinions
  - Interest in the work performed
- Understand stakeholders by following a three-step process

Understand Stakeholders

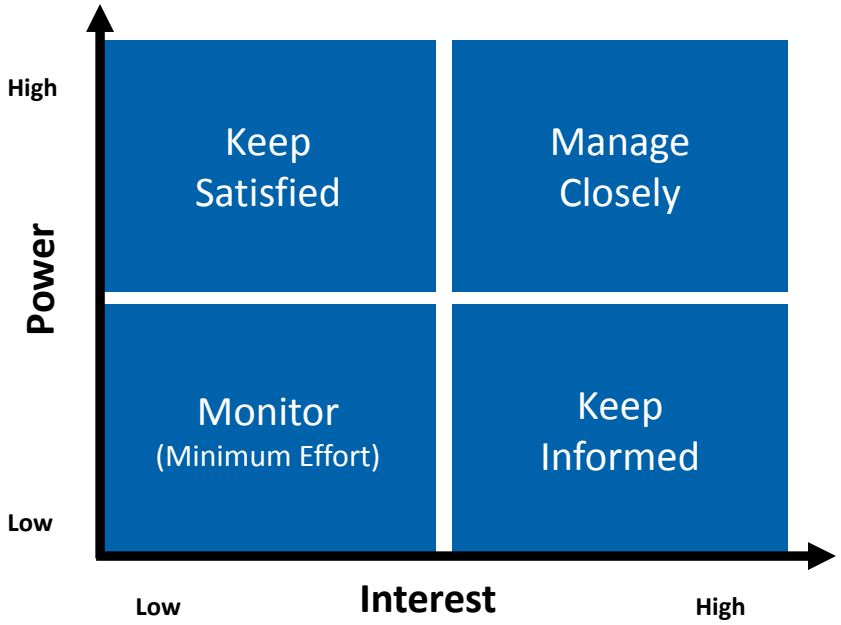
- Meet with them and others who know them to understand
  - What motivates them?
  - What do they want from you?
  - What interest do they have in your work?
  - What can you provide to them?
  - Who do they trust? Who advises them?

Mapping Power and Interest

- Full understanding of stakeholder power and interest can be achieved through stakeholder mapping
- Stakeholders have:
  - Three levels of power
    - Those with a “veto”
    - Those with a “vote”
    - Those with a “voice”
  - Three levels of interest
    - High
    - Medium
    - Low

Prioritize Stakeholders

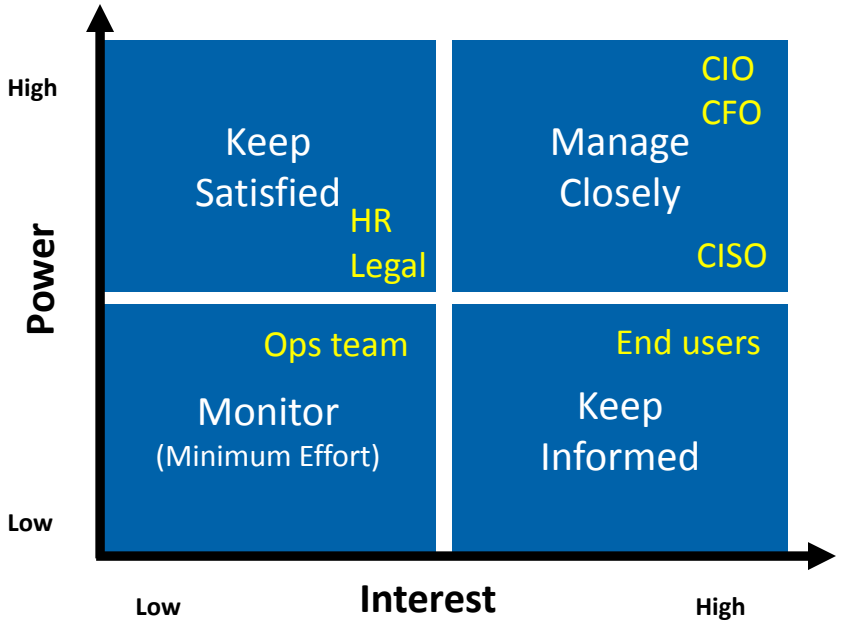
- Power/Interest Grid can be used to prioritize your stakeholders



From mindtools.com

Prioritize Stakeholders - Example

- Power/Interest Grid



From mindtools.com

Master Your Message

Example #1: Heartbleed - Bad

Heartbleed is a bug in the **OpenSSL** cryptography library, the widely used **TLS** protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or client. It results from **improper input validation** in the implementation of the **TLS heartbeat extension**. This vuln is classified as a **buffer over-read**.

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

Example #1: Heartbleed - Better

A security vulnerability called "Heartbleed" was disclosed Monday night, which could impact our **websites**. This bug allows private data such as **usernames**, **passwords**, and **credit card numbers** to be stolen from the memory of a website's server.

Our security team immediately began scanning our environment for potential impact. At this time, there is no indication that our company is at risk, or has been compromised.

Example #2: DMARC - Bad

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

Example #2: DMARC - Better

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**.

Example #3: DDoS - Bad

DDoS is an attack where multiple **compromised systems**, which are often infected with a **Trojan**, are used to target a single system causing a Distributed Denial of Service (DDoS) attack. Victims of a DDoS attack consist of both the end targeted system and all **systems maliciously used** and controlled by the hacker in the distributed attack. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via **botnets**.

Source: http://www.webopedia.com/TERM/D/DDoS_attack.html

Example #3: DDoS - Better

On Friday night our **primary web site** was **unavailable** for **two minutes** because it was **flooded** with traffic from the Internet by cyber attackers. We immediately instituted our incident response and recovery procedures and the web site was **made available** with **zero customer impact**.

Summary

Key Takeaways

- Build Your Business Case
  - Don't just ask for the money
  - Sell a vision on how you will solve business problems
- Rocket Your Relationships
  - Prioritize using the Power/Interest Grid
  - Engage stakeholders with a stakeholder management strategy
- Master Your Message
  - Make security understandable to business leaders using plain language
  - Market and promote your accomplishments

RSAConference2016

#RSAC

Frank Kim
fkim@sans.org
@fykim

Material based on SANS MGT514
Security Strategic Planning, Policy & Leadership