Security in knowledge

PRIVATE VS. PUBLIC SECTOR: FUNDING A SUCCESSFUL SECURITY PROGRAM

Stefan Richards, CISSP

President & CTO, Fulcum Security

Rick Gilmore, CISSP

CISO, State Of California, County Of Yuba

RSACONFERENCE2013

Session ID: GRC-R35B

Session Classification: Intermediate

Overview

- Funding A Successful Security Program
  - Obtaining the funds
  - Retaining the funds

Getting the Money

You need money, so what?

Make a Business Case

- Answer "so what?" in dollars where possible
  - Make $
  - Save $
  - Mitigate $ loss
- Always tie to business objectives
- Avoid
  - Gloom & doom
  - Tech talk

Keeping the money

What about next year?

Keeping the money

Care and feeding for your security program.

- Treat it as a living entity…because it is.
- Know it intimately.
- Efficiently communicate its “health” to management.

Communication

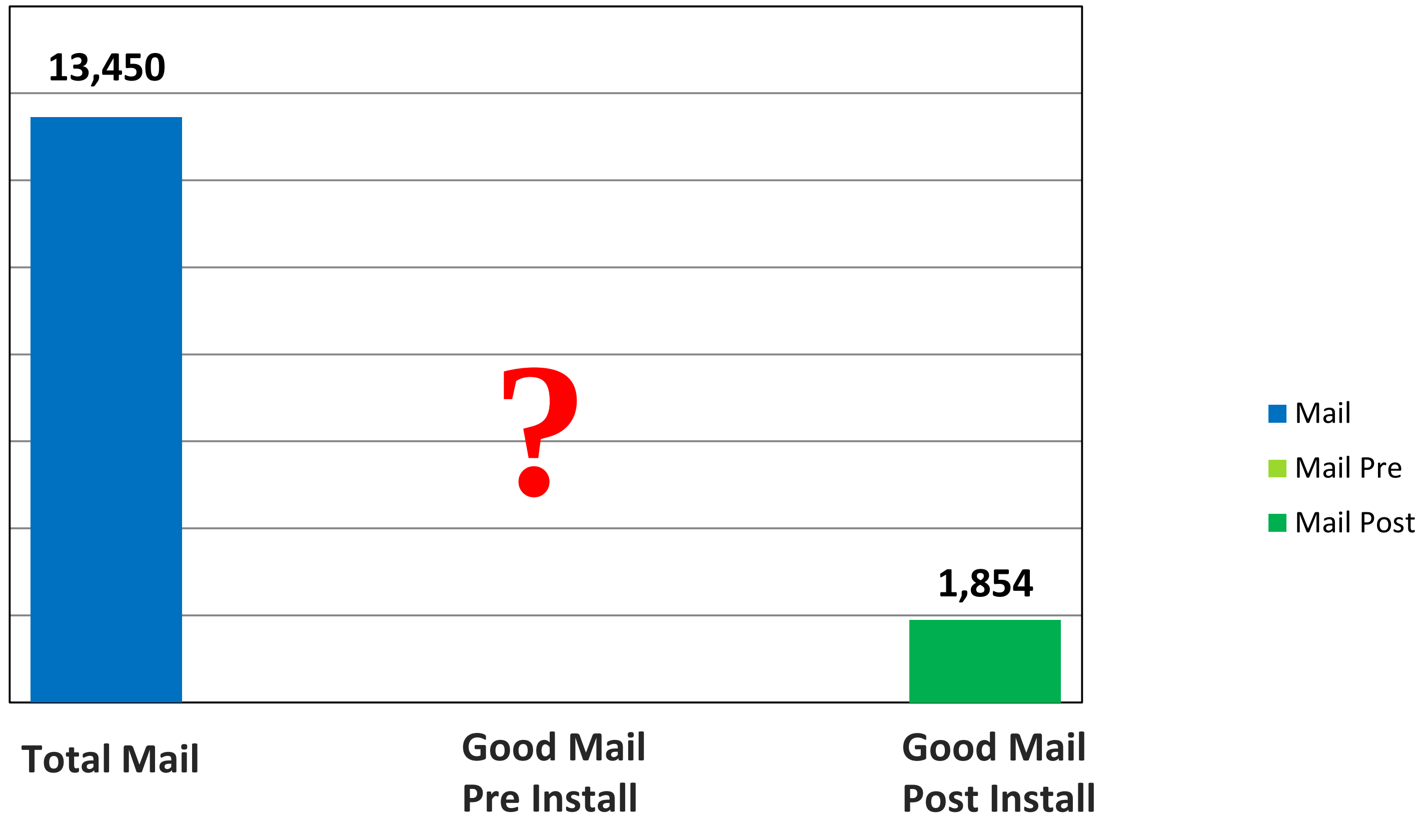
- Meet with Mgt. to understand their concerns.
  - Stay tuned-in throughout the life of your program
- Develop a good metrics program in order to communicate the status and health of the program.
  - Security Awareness Bulletins
  - Email with 3 indicators designed to address risk appetite.
- Correlate a previous decision for support with success.

Sample Scenario

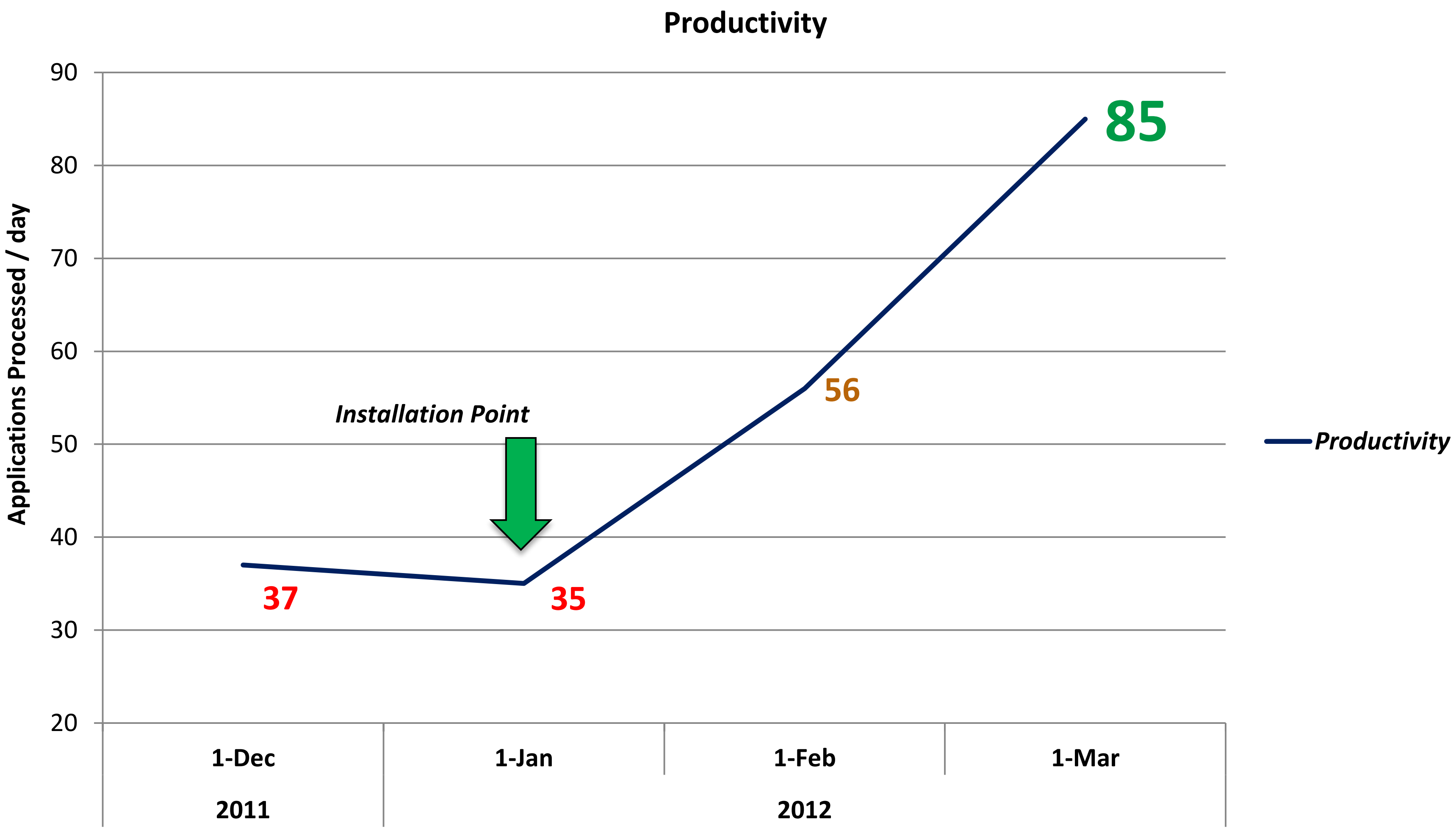
The problem statement:

Productivity could be impacted by spam & malware.

Security Audit Impact



Productivity Impact



Function of metrics

- Information Security Metrics, when done well:
  - Enables better decision making
    - You're there to help them make better decisions
  - Indicates program performance, both good and bad
    - Show them you can be objective, even with yourself
  - Justifies resource allocation
    - Spending their money in the right place for the right reason
  - Gauges control implementation
    - Are you safer now?
  - All information MUST address their concerns
    - Remember: Associate a result with a decision

Summary

- Speak the language of business!
- Get funded – Make a grounded business case
  - Prove need in <u>business</u> terms – efficiency, profit & loss, $$
  - Save tech talk for engineers, gloom & doom for the bars
- Stay funded – Show your worth it!
  - Understand management concerns up-front
  - Demonstrate program effectiveness with good metrics
  - Correlate a successful result with a decision for support

Thanks!

For questions or more information, please don’t hesitate to look us up

Stefan Richards
stefan@fulcum.com
http://fulcum.com

Rick Gilmore
rgilmore@co.yuba.ca.us

Backup

Security in knowledge

Do's and Do not's

- DO NOT
  1. Use doom and gloom strategy or scare tactics
  2. Use chaotic graphs and information
  3. Use questionable information
  4. Throw associates under a bus
  5. Criticize past decision, even if they were catastrophic
- DO
  1. Treat a security program like a living entity
  2. Talk their language via metrics (ROI, TCO, Cost Benefit, etc.)
  3. Brevity, Sincerity, and Accuracy
  4. Use relevant and intelligible information
  5. Associate a successful outcome with a decision for support

Resources

- Available resources on metrics
    - *SANS*
    - *NIST 800-55*
    - *"Security Metrics" by Andrew Jaquith*

Make a Business Case - Example

- Justifying purchase of Threat Intelligence/Security Patch Information Service
- Before:

Borderline
To technical

Improper patching is easily detected and exploited by hackers using automated scanning techniques and existing packaged exploits. We need this service to reduce the amount of work required to keep our platforms up to date as well as to eliminate potential errors of doing this manually. If we don't use this service, a serious breach is likely, which could put us out of business or irreparably blight our reputation.

Gloom &
doom

Make a Business Case - Example

- After:

Quantify risks mitigated in $

Quantify $ saved

*This service reduces operations costs by **~$10k/year (30%)** while reducing errors and improving timeliness of corrective action. Failure to patch in a correct and timely manner exposes us to **assessment of regulatory fines** for non-compliance (**$100 – 1.5M per incident**) as well as potential breach of customer data (**avg. cost $200+/ record**). Funding this program **supports our strategic business objectives** of reduced operational costs, zero regulatory findings and maintaining the high levels of customer trust.*

Tie to Business objectives