RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAB2-W11

Breaking Out of the Security Metrics Matrix: Steps in the Right Direction

Tim Crothers
Vice President, Security Solutions
Target
@soinull

James Stanger
Chief Technology Evangelist
CompTIA
@jamesstanger

Agenda

- What is the security metrics matrix?
- The contingent value of security controls without metrics
- Demonstrating value for money: Useful metrics
- Moving from the defender's dilemma: A better approach to risk management
- Creating customized metrics

RSAConference2019

The importance of metrics

An overview

Frustrated observations from C-level managers

- “It’s abundantly clear that security companies like to sell their stuff almost as much as my IT department likes to buy it.”
- “We keep having the same discussion every year. The only difference is that the costs keep getting higher.”
- “I keep talking ROI. They keep talking about the latest hack in the news. How is that even relevant?”
- “Isn’t this as simple as just doing more end user training, or even punishing careless actions?”

The problem

- Meaningful cybersecurity metrics are hard to create and use
- There's a disconnect between these three major elements

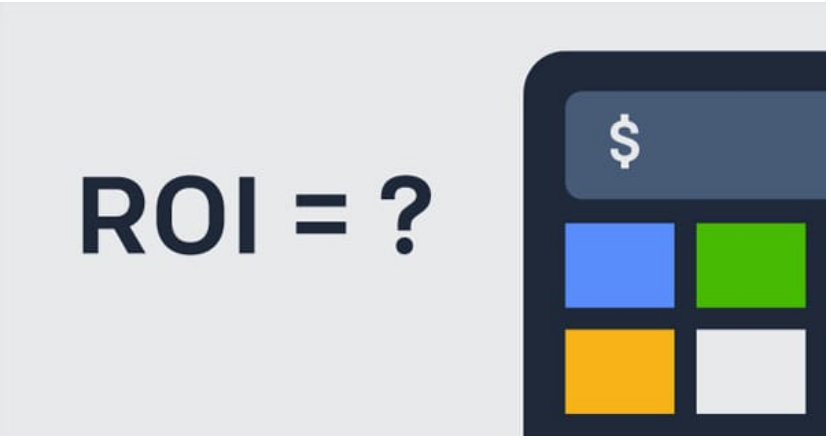
We've seen that security professionals struggle to create and customize meaningful metrics

Lots and lots of questions

- How do I justify spending to leadership?
- Am I spending too little, too much or just right?
- Are my controls effective?
- Are my controls worth the cost?
- How can I improve my operations and controls?
- How do I demonstrate effectiveness of security controls for third parties/regulatory/contractual requirements?
- How do I drive the behavior I want in the organization in regards to security?

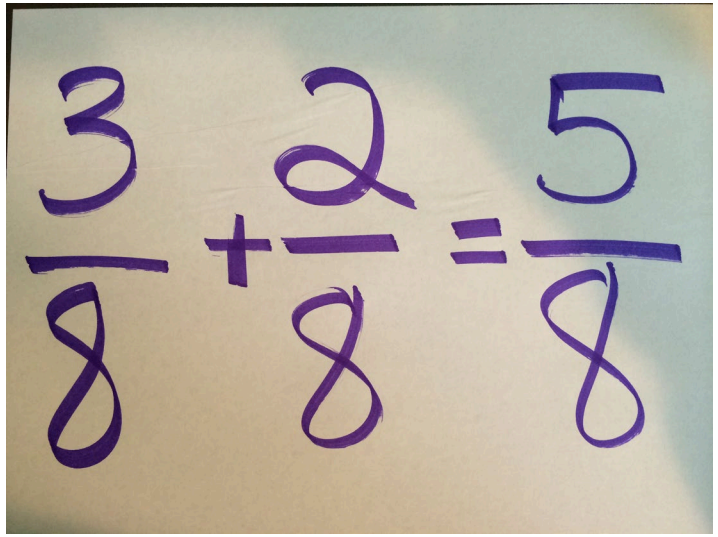
Terms, terms and more terms

- Cloud…
- IoT…
- Risk…
- Breach…
- Response …
- ROI…



Common denominators

- How do I determine/demonstrate value?
- How do I maximize value?
- How do I know and show how well I'm protecting my organization?
- What do I need to do to protect it better and how much will it cost?



RSAConference2019

Group discussion 1: Talking about your environment and situation

What questions are most important for you?

What approaches are working/not working and why?

RSAConference2019

Setting the stage

A starting point… Detection and Response/SOC operations

Foundations and core beliefs

- Value people & skills over technology & prioritize my investments accordingly
- Prevention failures are inevitable.
  - The trick is to contain them before they become breaches
  - Define your terms
- Measuring the effectiveness of everything and constantly improving it is critical

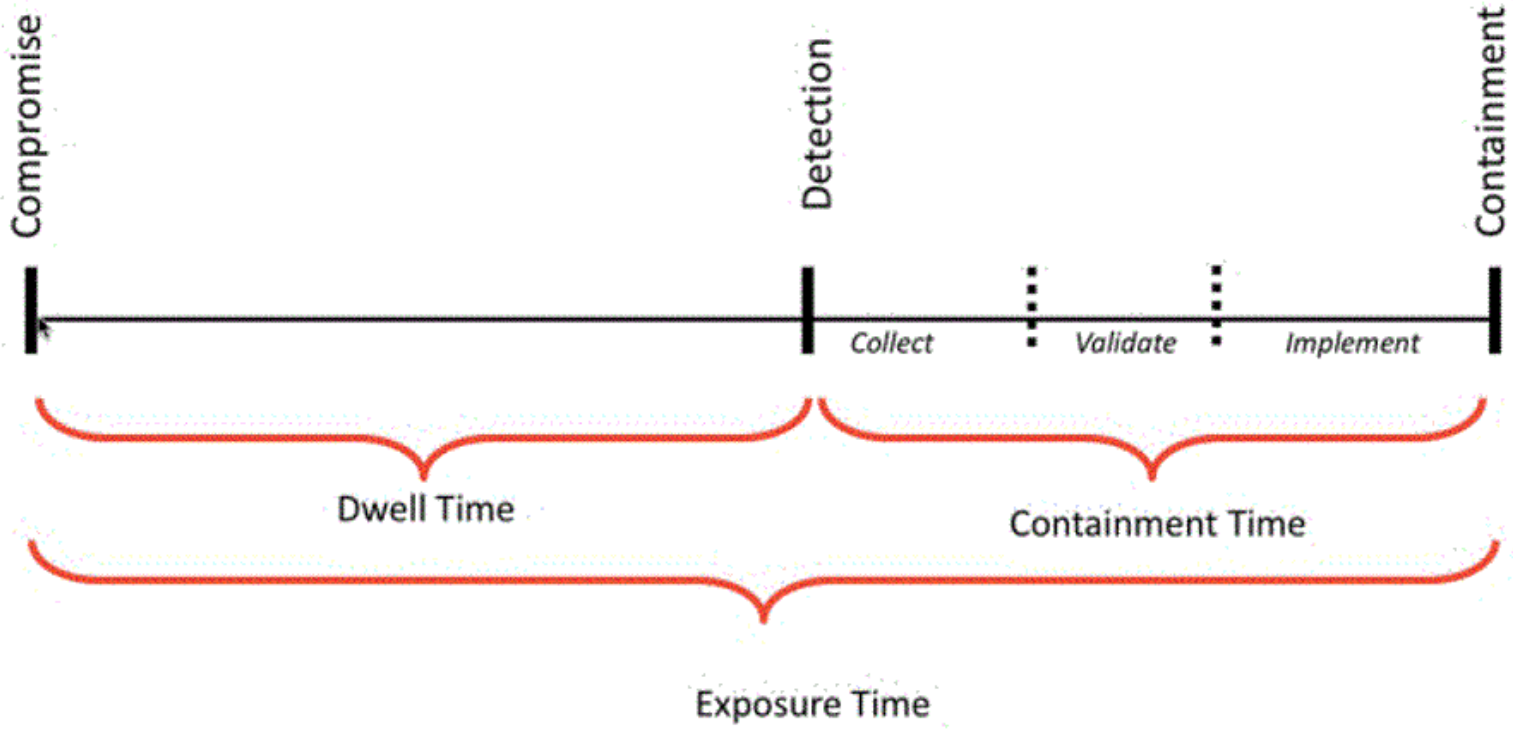
Essential terms and approaches

- Business
  - Value for money vs. Return on investment (ROI)
  - Risk management
- Technical
  - Sensors
  - Threat hunting
  - Root cause analysis

Root cause analysis and exploits – using consistent terms

- Compromise / prevention failure
  - When the system protection files
  - For example, antivirus doesn't catch the exploit
- Detection
  - Secondary control
  - Individual
- Containment
  - Not exposure time
  - How long it takes to manage the attack

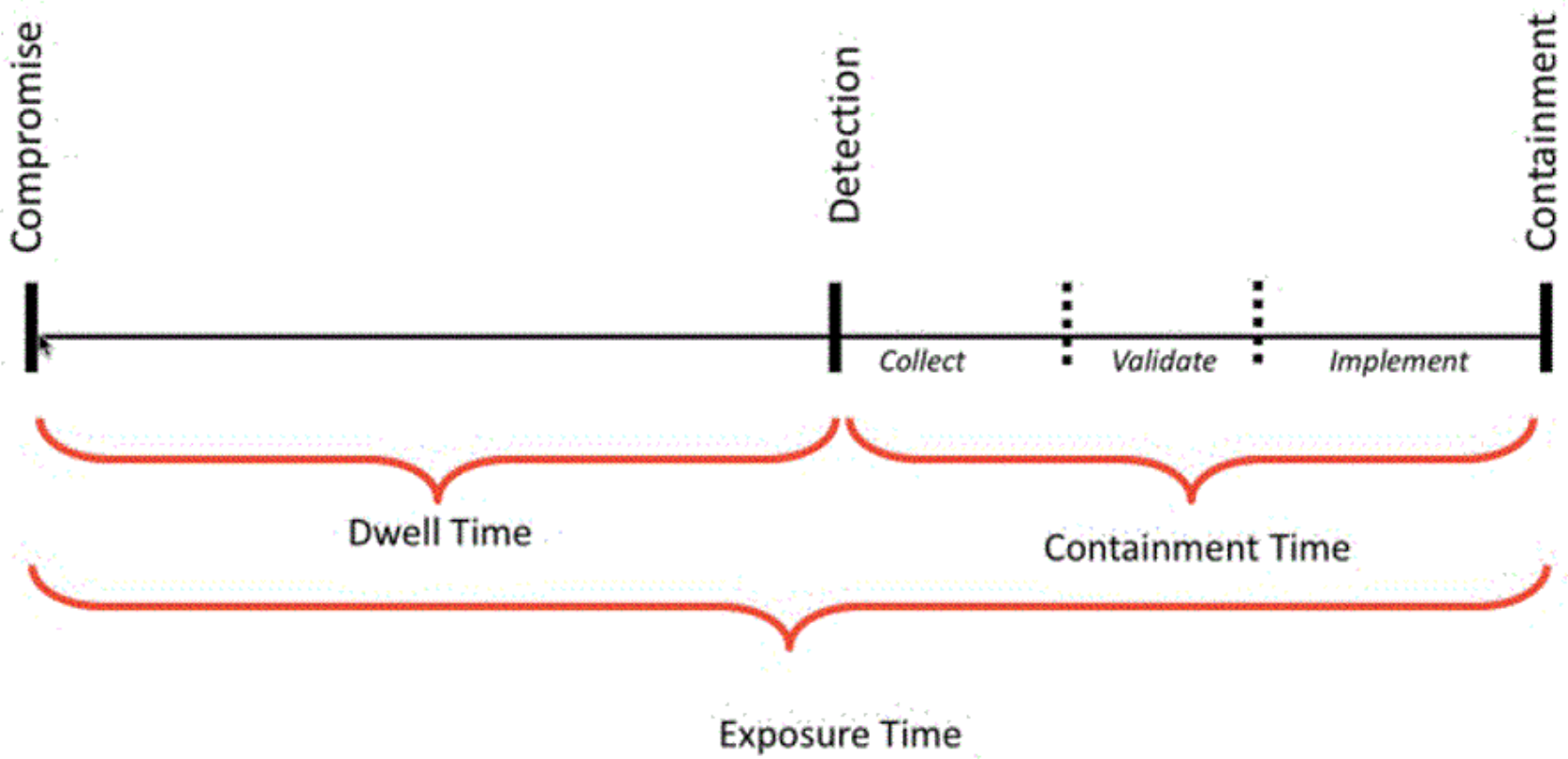
Breach: Threat actors completing their objective



Defining terms (cont'd)

- Dwell time
- Detection elements
  - Collect info
  - Validate
  - Implement
  - Containment time
  - ***Metrics***

Very important to create and use consistent terms.
Consider the complexities that are involved . . .



Management may not be technical,
but they know risk very, very well

RSAConference2019

Group discussion: Metrics and organization maturity level

Would the detection and response approaches work at your organization?

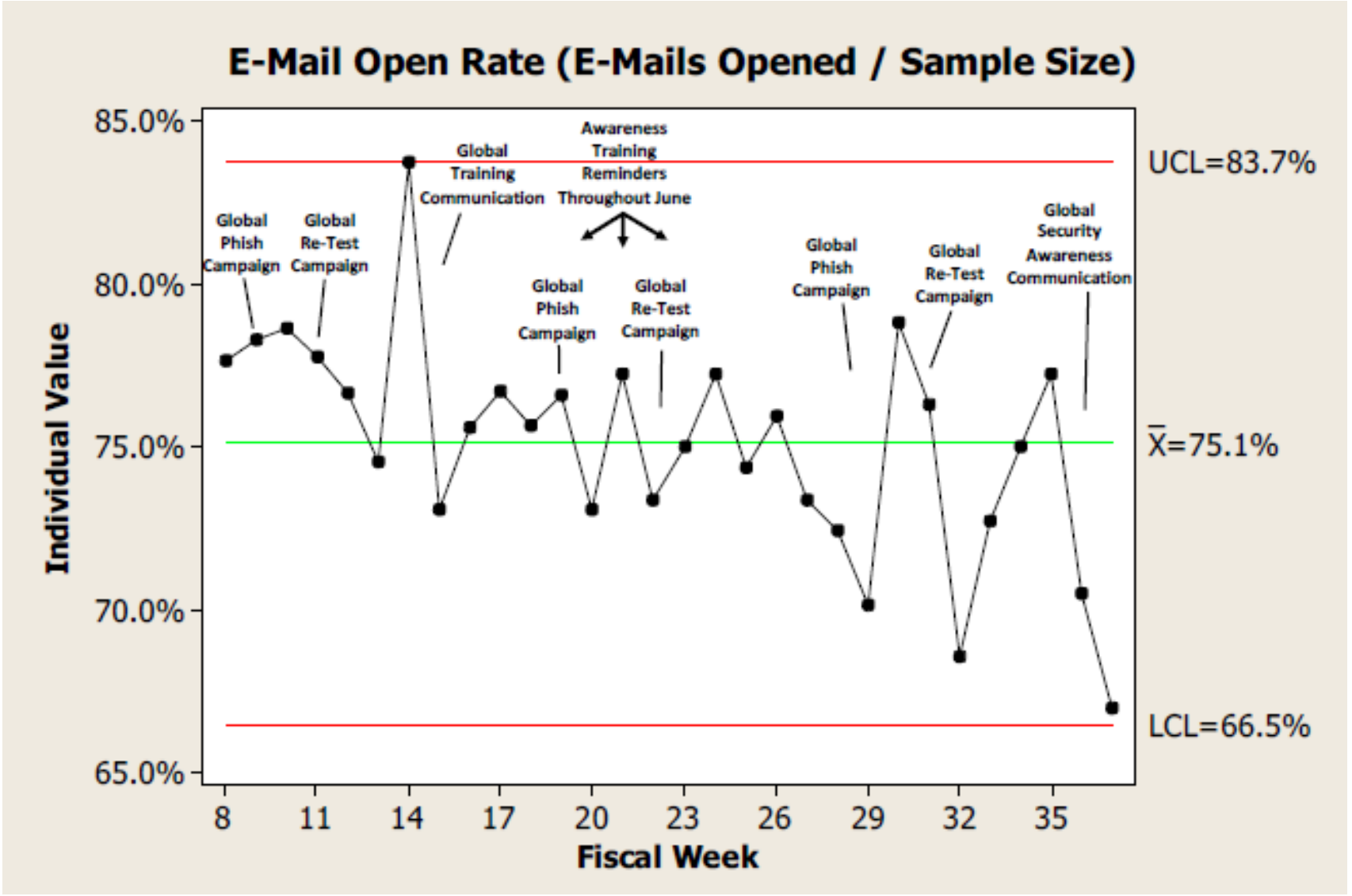
RSAConference2019

Creating useful metrics

Applied examples

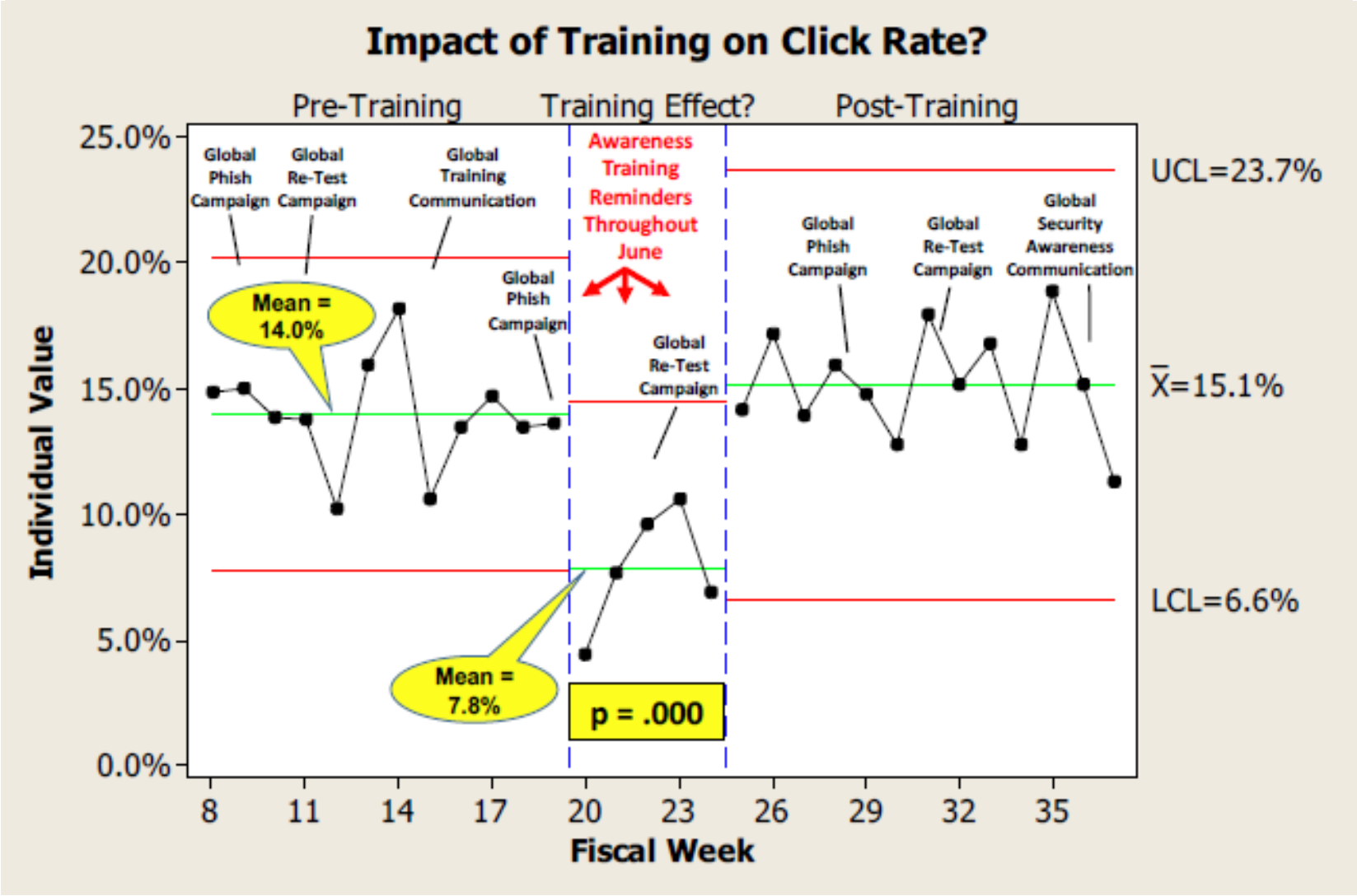
Creating metrics – email considerations

- Open rate
- Report rate
- Rates
  - Global
  - Region
  - Additional sectors



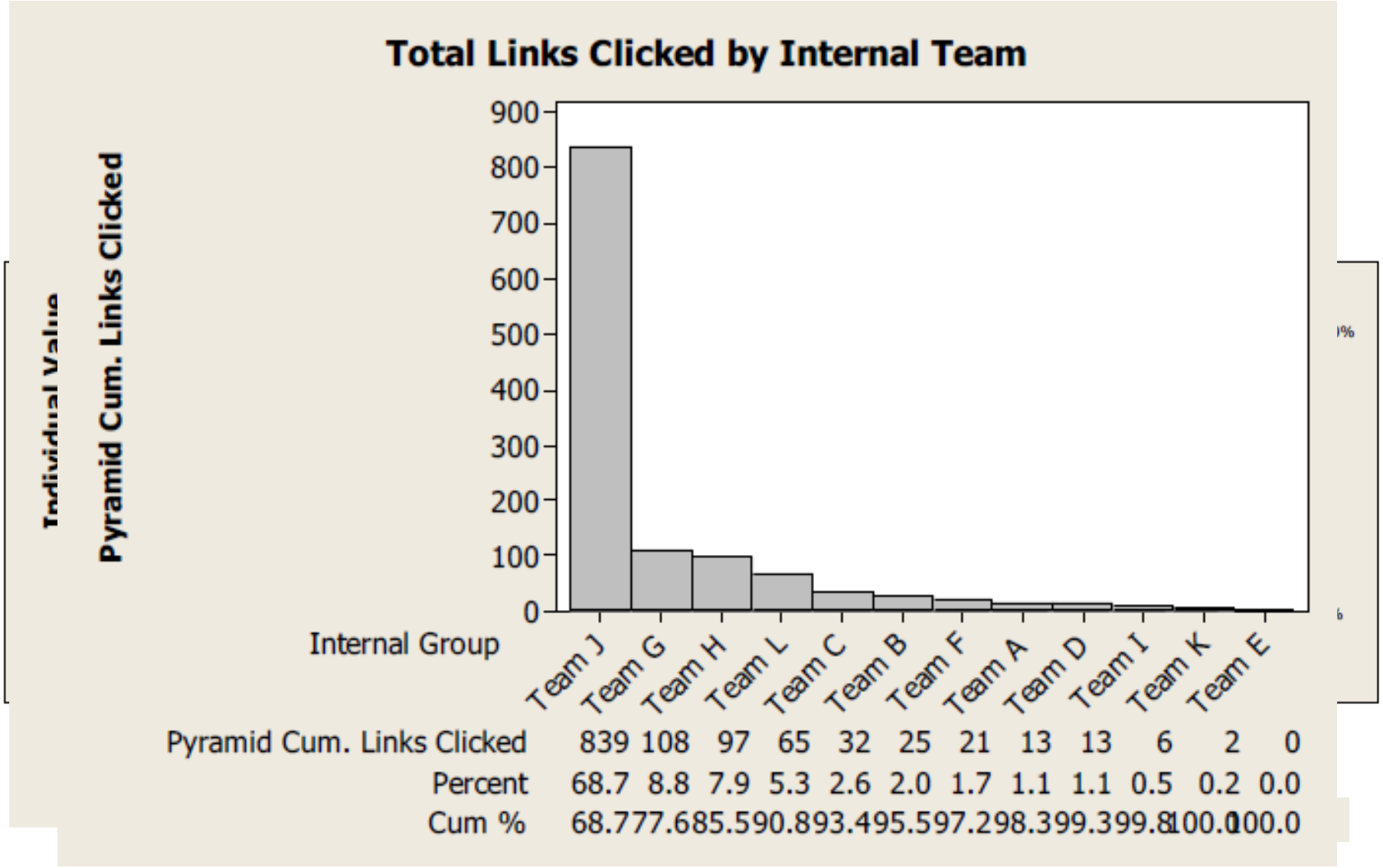
Creating metrics – email considerations (cont'd)

- Links clicked
- Click rate
  - Internal
  - Offshore
  - Contractor
- Success of awareness training



Creating metrics – teams

- Internal
- Offshore
- Contractor

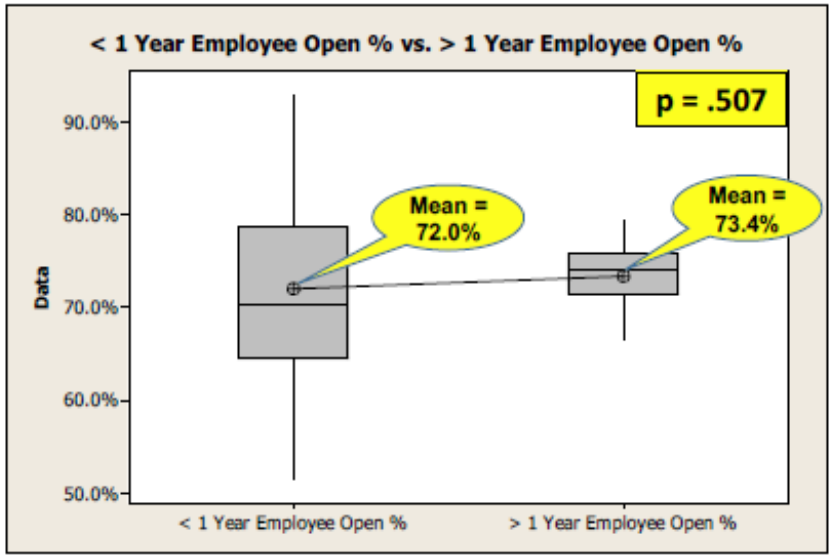


Creating metrics – developing stats

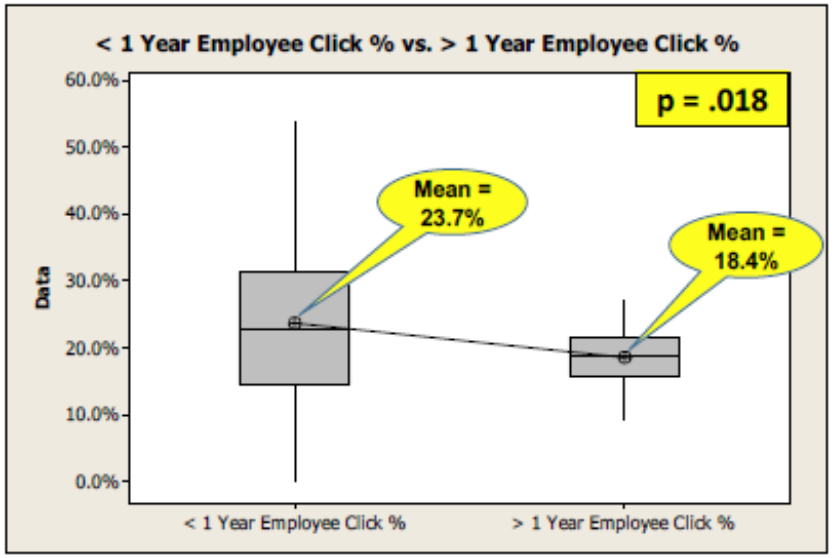
- Comparing tests
  - Baselines
  - Means
- How to obtain metrics
  - Meetings with stakeholders
  - Peers in similar situations

Searching for Statistically Comparable Phishing Tests
Comparison of Baseline Click Rates:
Baseline I (Fiscal Weeks 21-29)

Mean Phish Open Rates:
Employees on Staff < 1 year
vs.
Employees on Staff > 1 year

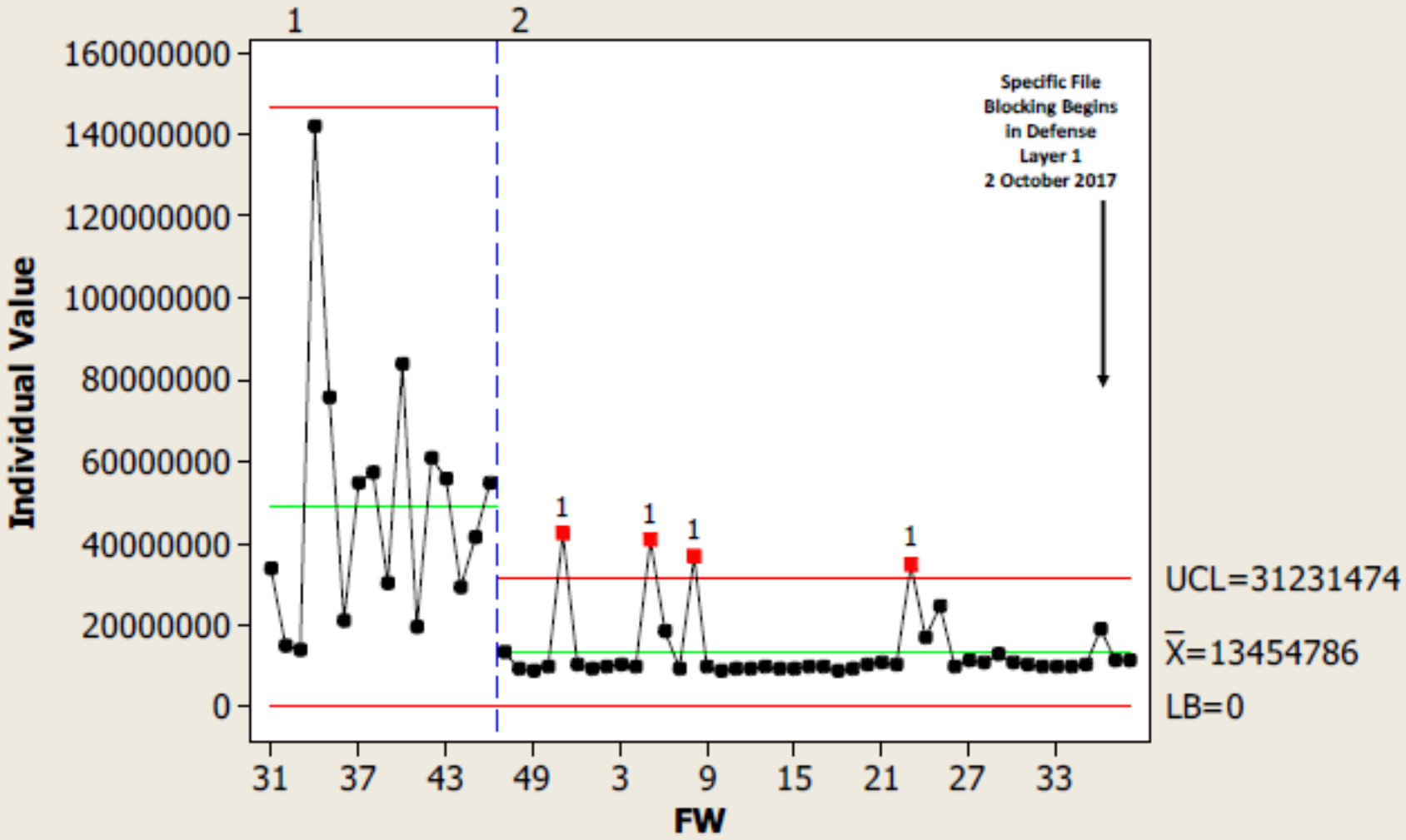


Mean Phish Click Rates:
Employees on Staff < 1 year
vs.
Employees on Staff > 1 year



Prevention failure metrics

- Considerations
  - Inbound
  - Delivered
  - Blocks
  - Blocks by reputation
  - Spam
  - Virus
  - Malicious URL
  - Junk
- By week



RSAConference2019

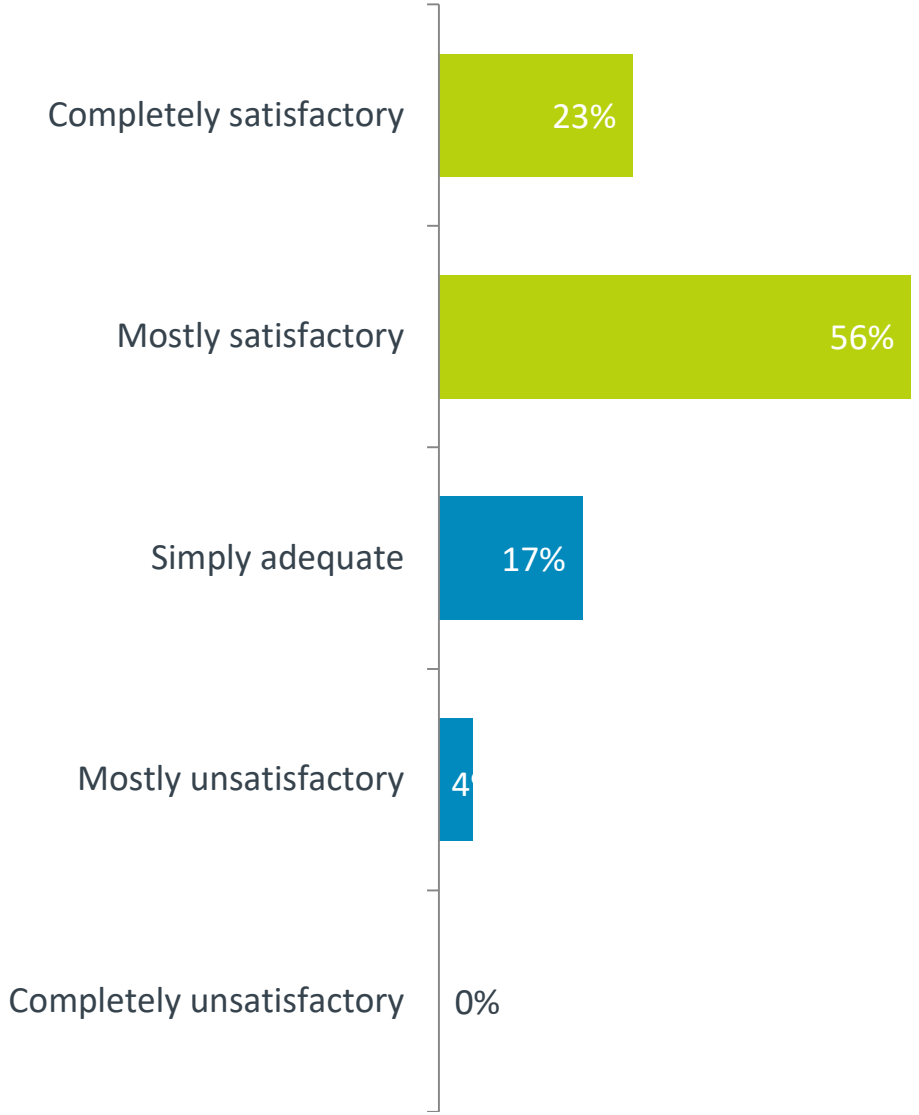
The proper foundation for creating metrics: What our research has shown

From CompTIA research: Over 600 companies surveyed in mid-late 2018

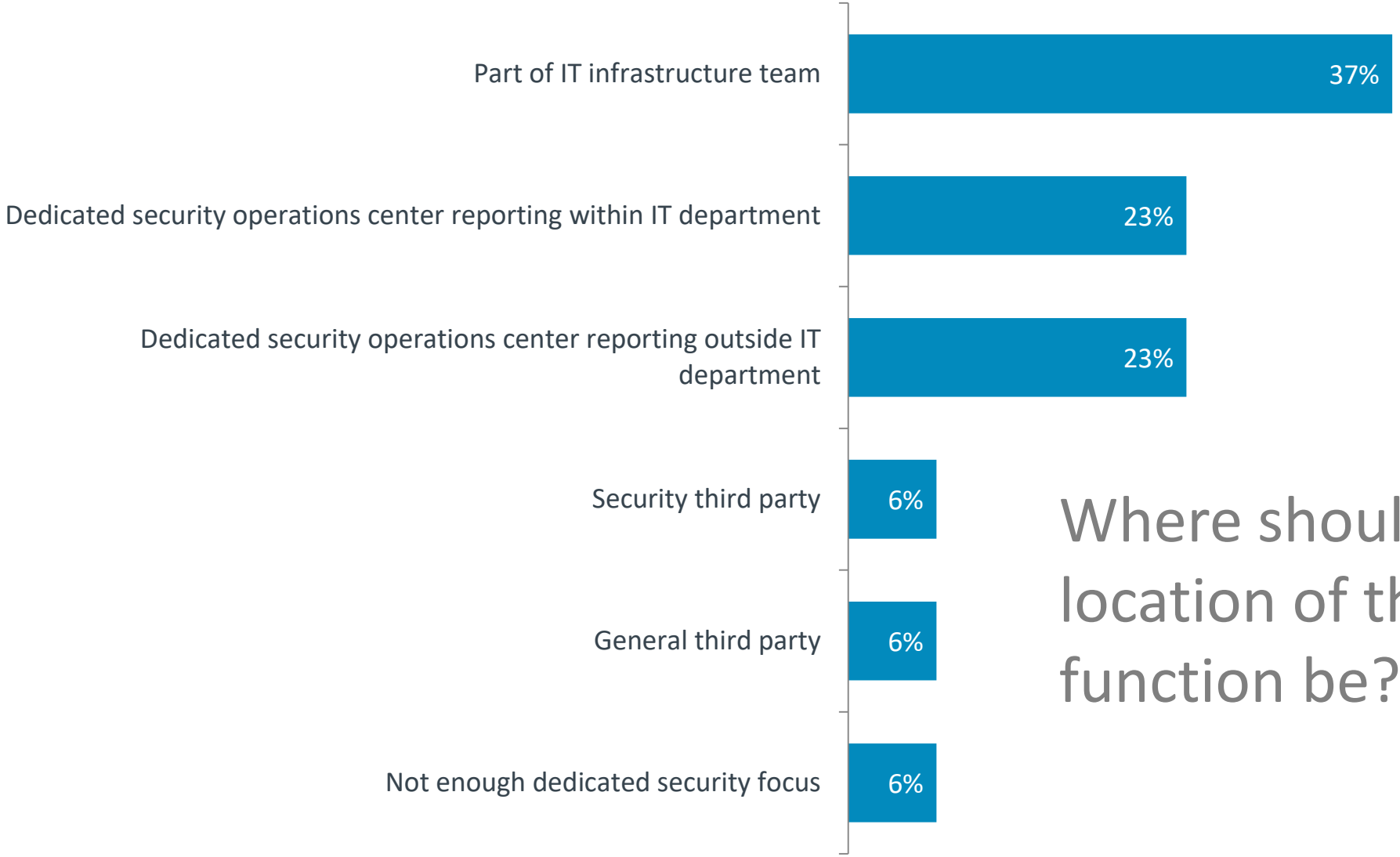
Characterization of current security

The success of any cybersecurity control is contingent on the *foundation* of the business

Is there a good foundation, according to these statistics?

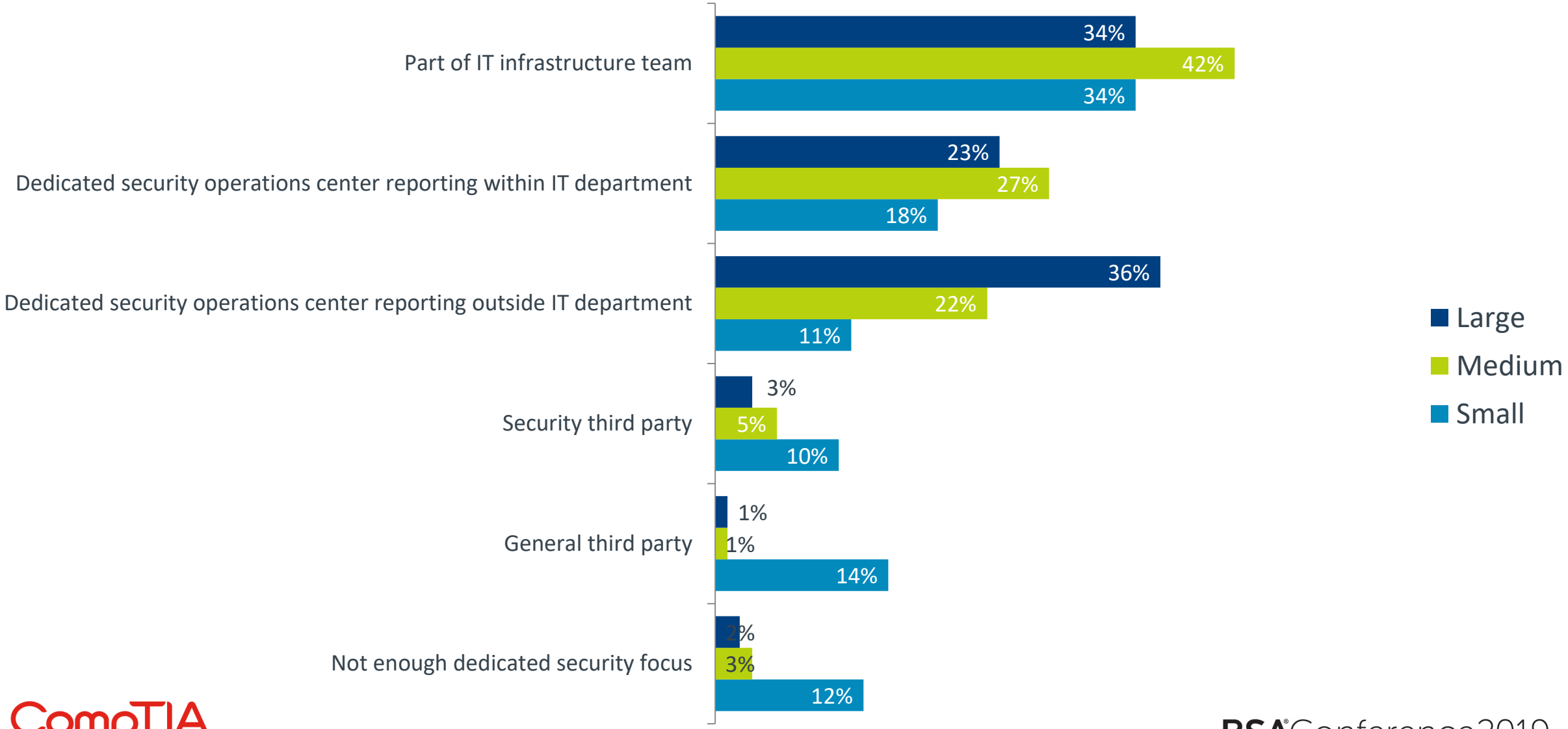


Primary location of security function

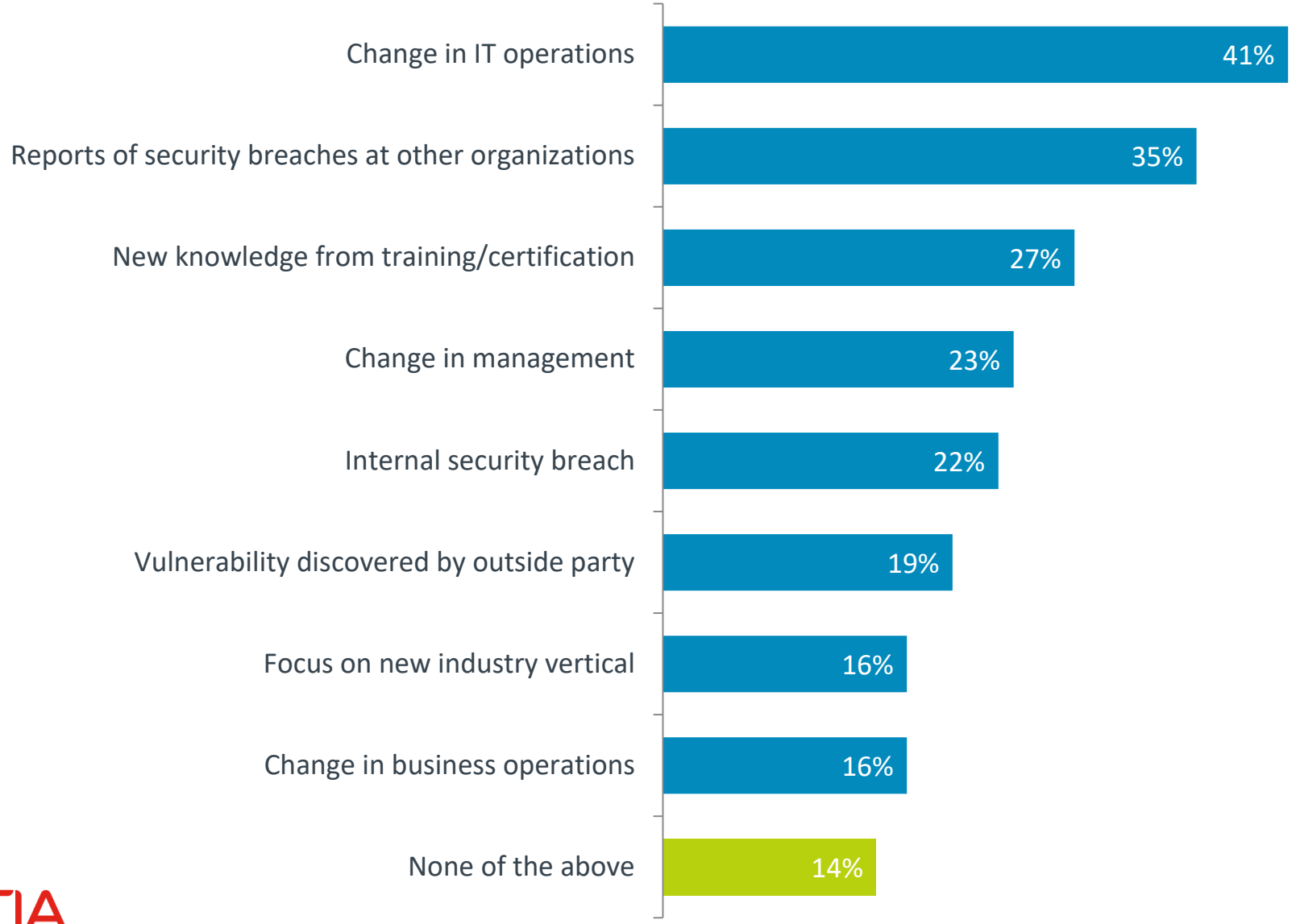


Where should the primary location of the security function be?

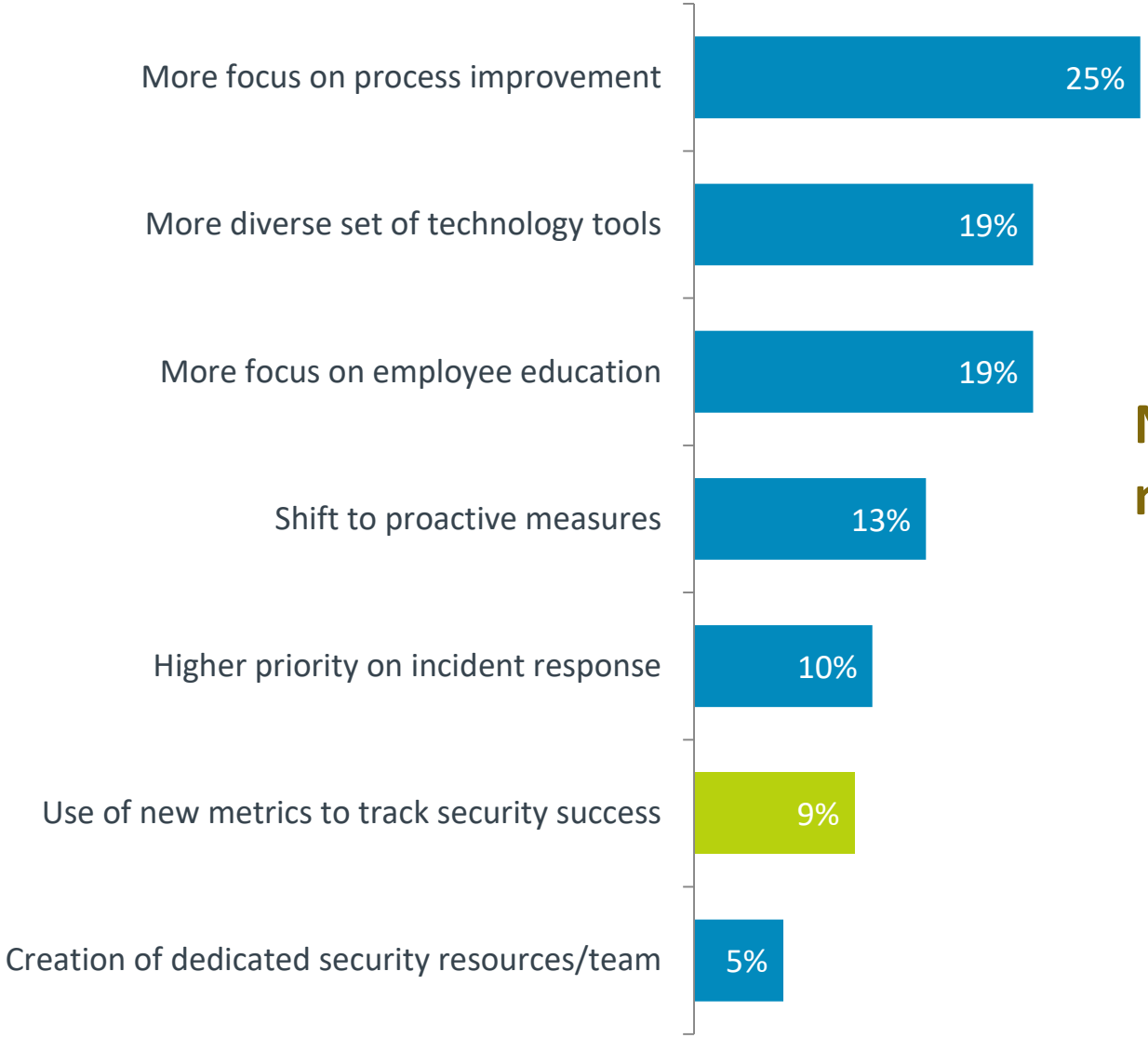
Primary location of security function – company size



Drivers for changing security approach

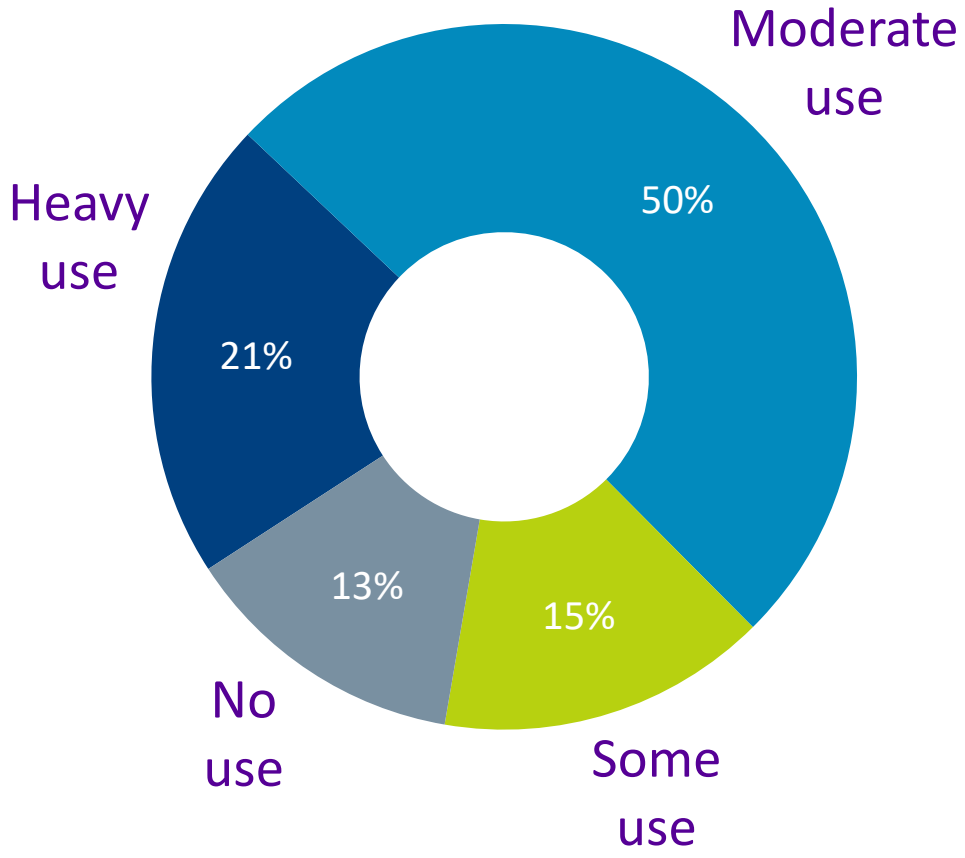


Primary reasons why their security approach has changed



Notice the low use of metrics

Setting and reviewing metrics



Areas of organization where security metrics are set and reviewed

	Set metrics	Review metrics
IT function	73%	57%
Some business units	43%	50%
Middle management	48%	54%
Senior executives	47%	52%
Board of directors	30%	38%

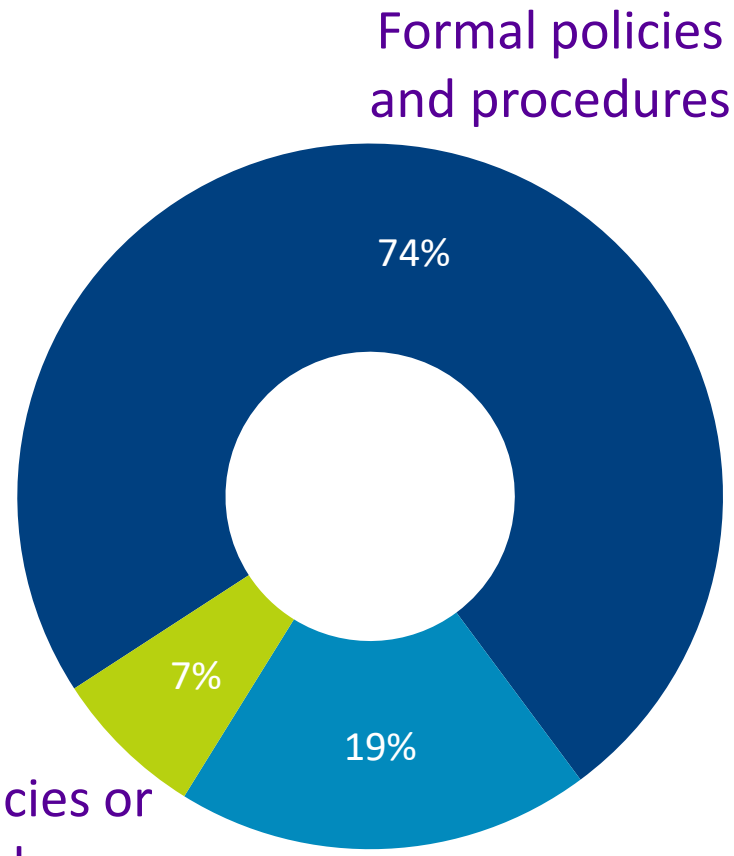
Lots of metrics have been set

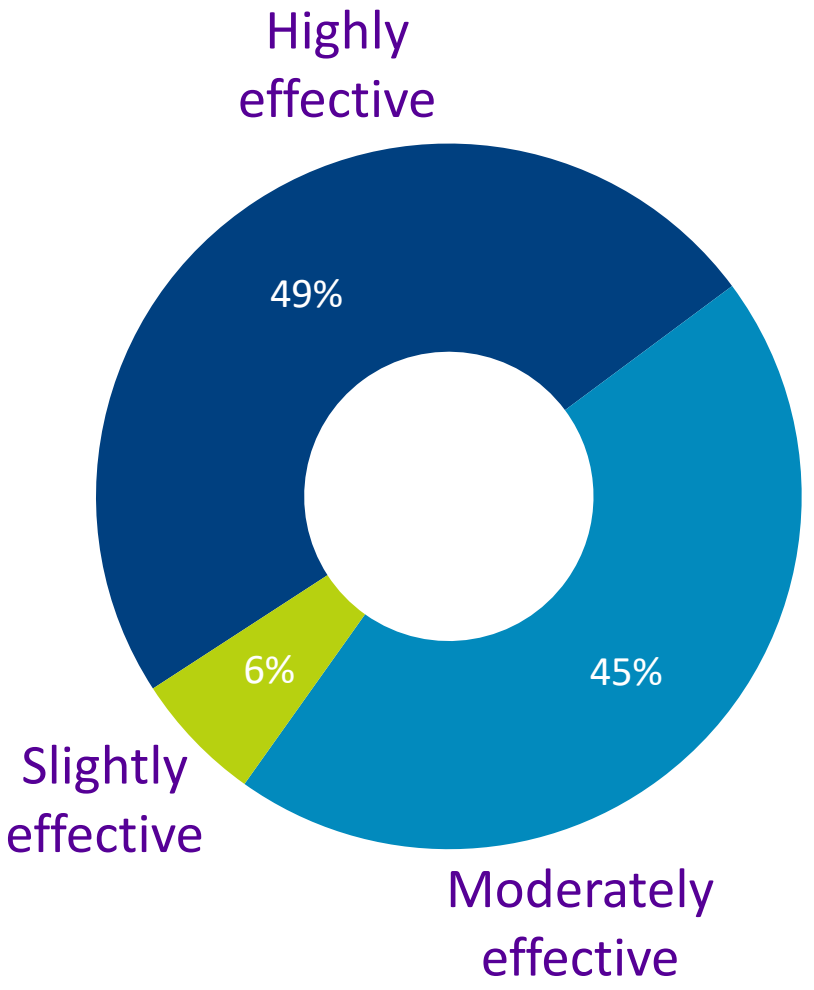
But few use these metrics effectively

Reasons why some companies don't use metrics

1. Not enough available resource for metric tracking
2. Insufficient skill for tracking/understanding metrics
3. Not sure which metrics to use
4. Security not a high enough priority
5. Uncertainty around tying security metrics to corporate health

The best laid plans of mice and men . . .





RSAConference2019

Group discussion: Baselining your organization

Where are you, based on the data we've given you?

RSAConference2019

Creating meaningful, impactful metrics

Questions to ask – and answer

Mapping controls to metrics

- Security controls galore
- But very little measurement of success
- The goal?
  - Create consistent, justifiable metrics
  - Ensure funding for personnel
  - Funding for tech, too
- This isn't a "checkbox" exercise

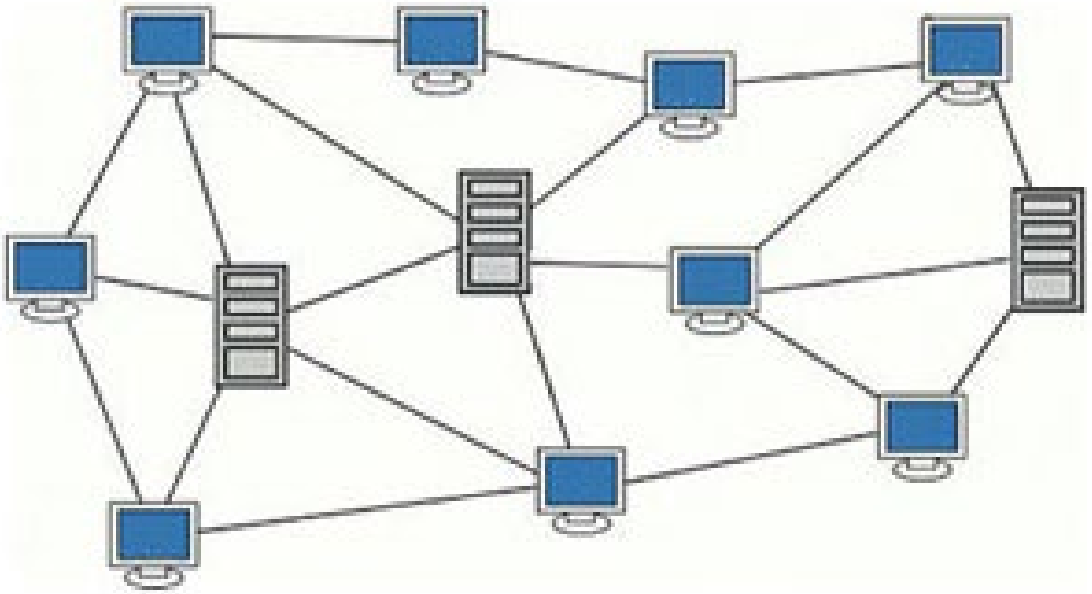
Critical Security Control	PCI-DSS	HIPAA	NERC-CIP	NIST 800-53	NIST Framework	FFIEC	COBIT	ISO 27002
CSC 1	✓	✓	✓	✓	✓	✓	✓	✓
CSC 2		✓		✓	✓		✓	✓
CSC 3	✓	✓					✓	✓
CSC 4	✓	✓				✓	✓	✓
CSC 5	✓	✓				✓	✓	
CSC 7	✓						✓	
CSC 10	✓			✓	✓		✓	
CSC 11	✓	✓	✓	✓	✓	✓	✓	
CSC 14	✓	✓	✓	✓	✓	✓	✓	

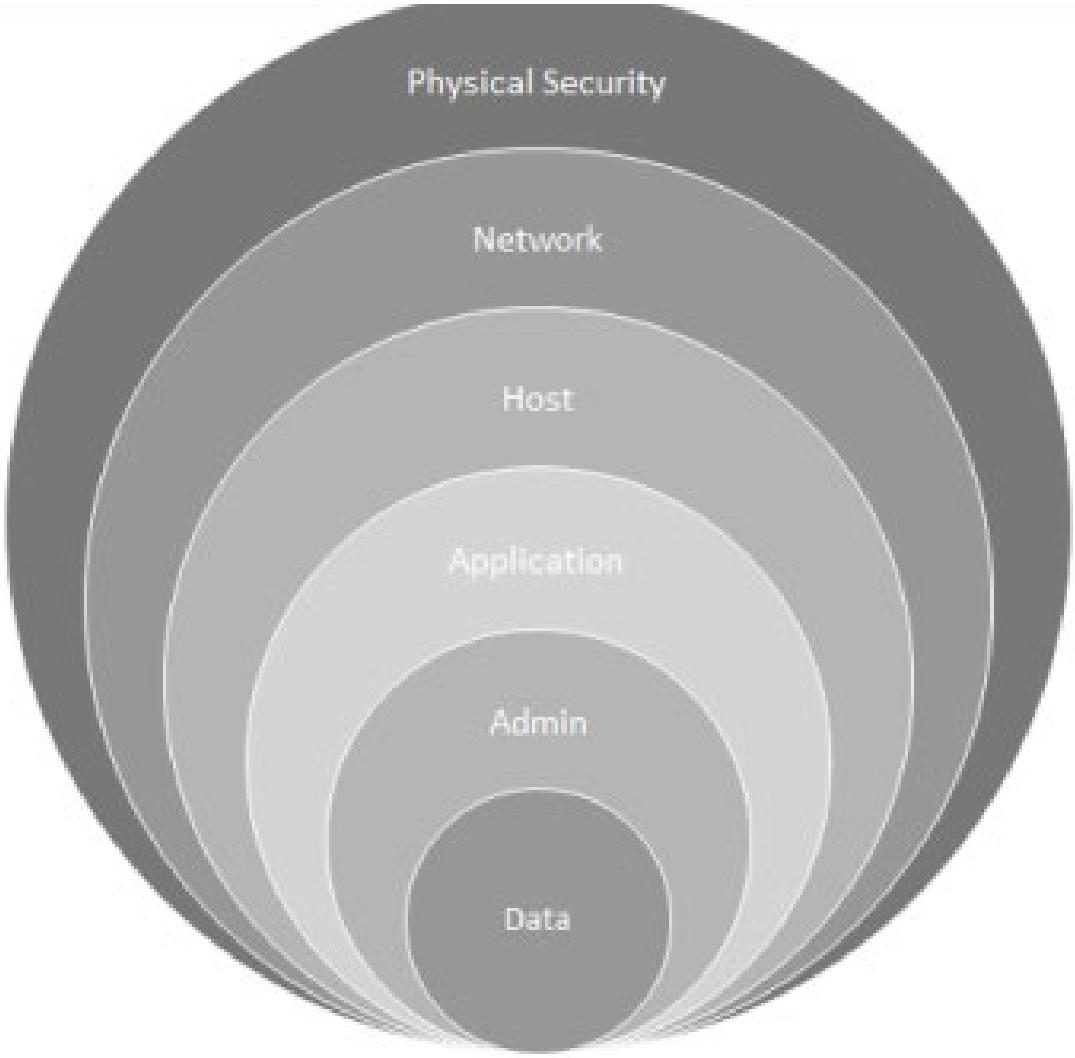
Some considerations

- X vs Y side of the equation
- Coverage
- Baselines
- Use cases
- Team member skill

Some considerations (cont'd)

- Overlap != Bad
  - Defense in Depth vs. Redundancy
  - Approach





Some considerations (cont'd)

- Cost vs. Breach
  - Direct Cost
    - Legal
    - Notification
    - Professional Services
  - Reputation/Brand
- Considerations
  - Cost
  - Savings
  - Recovery

(R-E) + T = ALE

R – ALE = ROSI

T == Cost of IDS

E == Dollar Savings of Using IDS to stop intrusions

R == Cost per year to recover

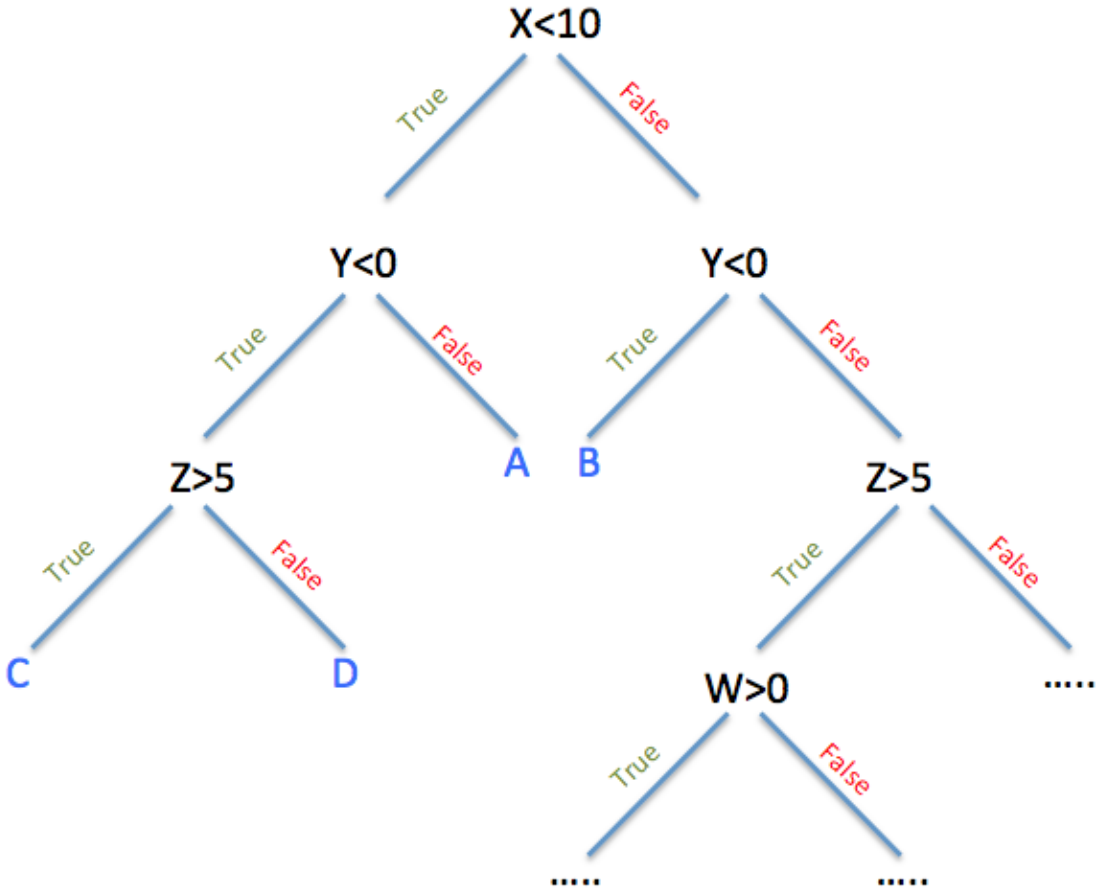
ROI – really?

ROI compares the amount of income derived from an investment with the cost of the investment. ROI is known as a profitability ratio, because it provides information about management's performance in using the available resources to generate income.

Those who advocate using ROI in the context of security equate savings with return. The key principle to understand is that wealth preservation (saving) is not the same as wealth creation (return). -- Bejtlich

Conclusions?

- Justify new spend?
  - 7% - 10% of overall IT
- Buy/No Buy/Replace/Remove
  - Does it provide a significant NEW/UNIQUE capability?
  - Does it significantly improve an existing capability?
  - What is the effectiveness measurement of the tool?



RSAConference2019

Group discussion 4

Mapping metrics to security controls: Tracking progress, identifying value for money / ROI

RSAConference2019

Driving behavior with metrics?

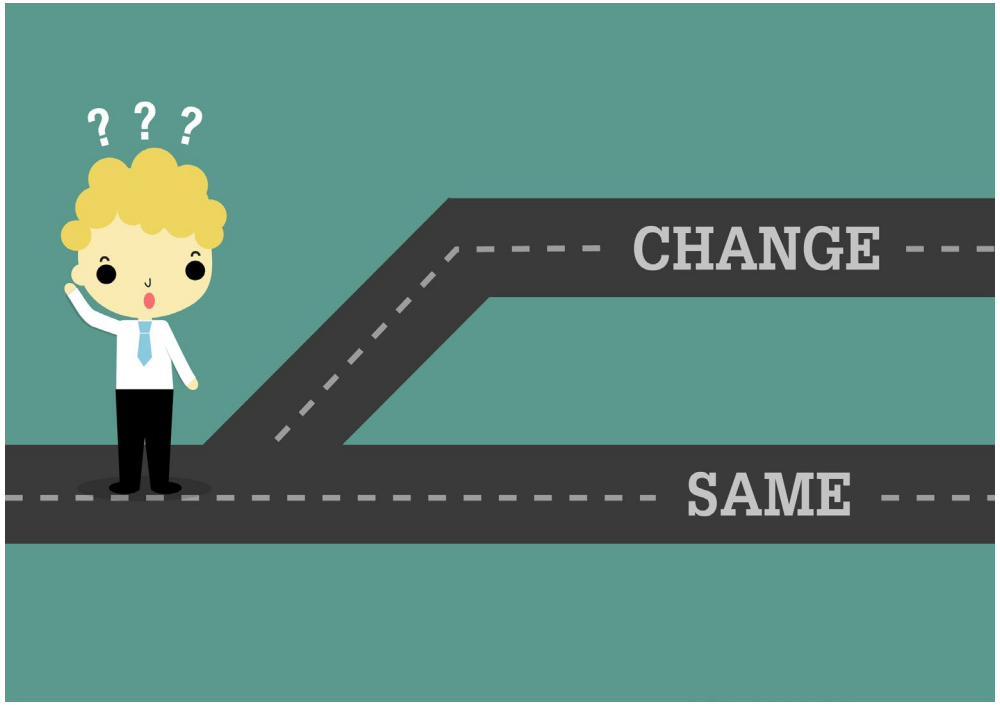
Let’s pivot to another outcome: Can we leverage security metrics to drive fundamental behavior changes?

Does security really need to be so hard?

- Social engineering – we can (re)educate for that
- Most application security flaws are just good coding practice issues
- Most system security flaws are just poor IT hygiene issues
- Many of the challenges in security stem from weak IT fundamentals
  - Patching
  - Consistent Configuration and Maintenance
  - Basic concepts like least privilege

What if we can cut through the confusion?

- Clarity on what we want business teams to prioritize
- Use a scoring model readily understood
- Patching?
- Findings?
- Security awareness?
- SAST, DAST, and Pentests?



RSAConference2019

Group discussion 5

What behavior would you want to drive with metrics?

RSAConference2019

Practical Application

Current situations and moving forward

Your current situation

1. What metrics do you have in place right now?
2. How do you develop those metrics?
3. Is management aware of these metrics? *Do they understand them?*
4. Have you shown progress to goal?
5. Discovery questions
   a) How do you prove value for money?
   b) What does the funding discussion look like with management?
   c) What teams do you currently have in place?

How to move forward

1. What would that discussion look like?
2. It's not a perfect world:
   - How do you cope with less-than-ideal situations?
   - Who can help you build consensus?
   - What tactics and strategies can help?

Real-world implementation challenges

- Data availability
- Resistance to measurement
- Measuring activity done by other teams
- People collected data vs. machine collected data

RSAConference2019

Group discussion 6

Discuss thoughts on how to move forward based on your current challenges

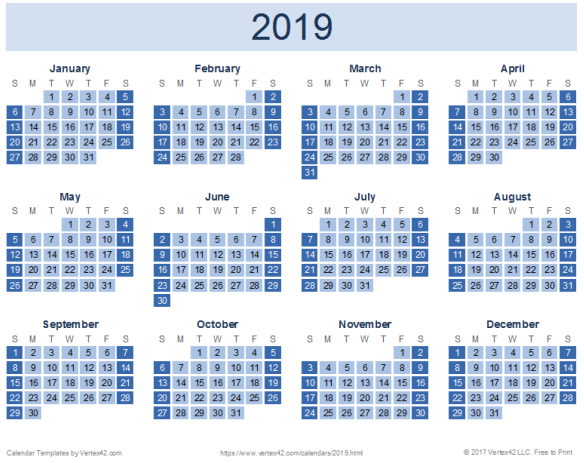
RSAConference2019

Group discussion 7

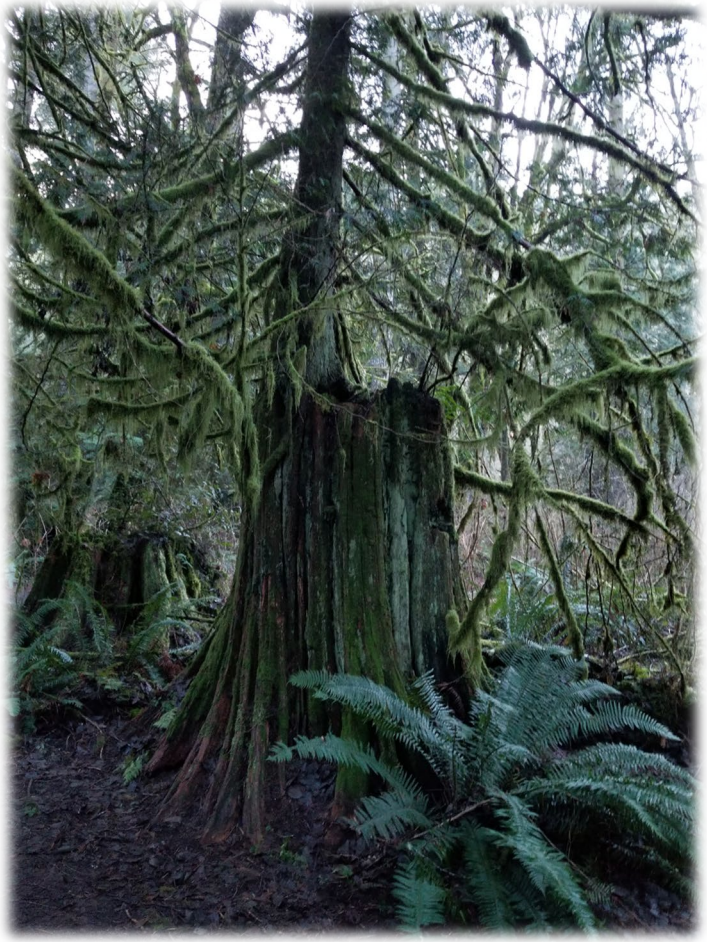
Using teams to customize and verify metrics

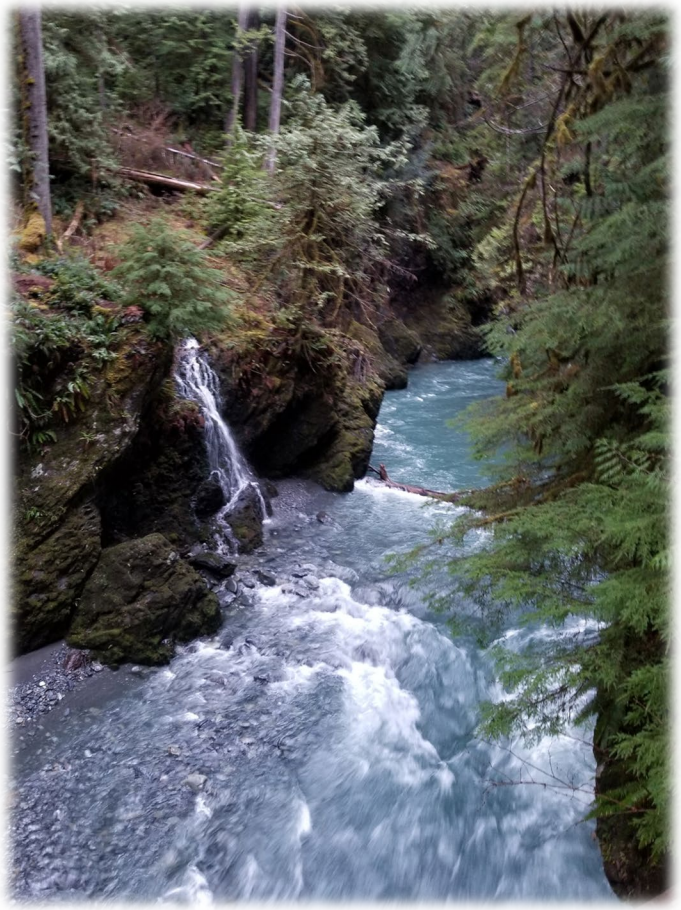
Apply what you have learned today

- Next week you should:
  - Identify stakeholders, as well as technical and business environments
- In the first three months following this presentation you should:
  - Identify most-critical resources (e.g., “crown jewels”)
  - Determine metrics for using key security controls
  - Have approved metrics
- Within six months you should:
  - Review metrics in a meaningful way
  - Adjust metrics according to findings of red team / blue team



Questions?





RSAConference2019

Thank you!

Tim Crothers

badsecurity@gmail.com

@soinull

linkedin.com/in/tim-crothers-5458738/

James Stanger

jstanger@comptia.org

@jamesstanger

https://www.linkedin.com/in/jamesstanger/