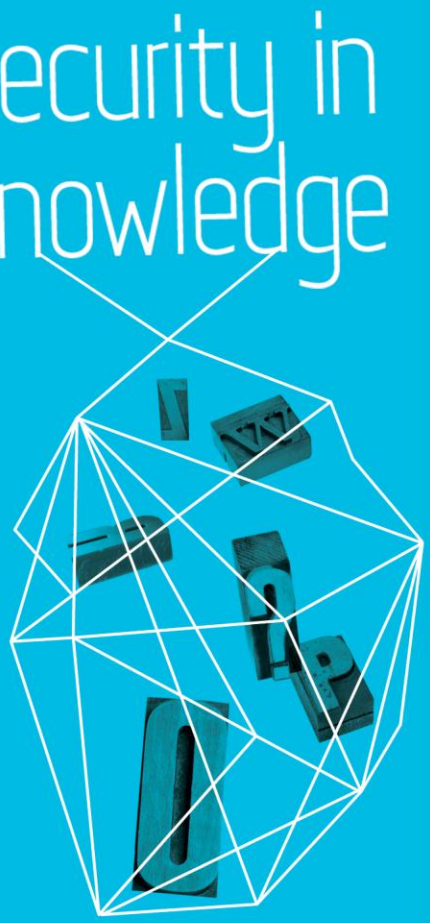
THE 7 HIGHLY EFFECTIVE HABITS OF SECURITY AWARENESS PROGRAMS



Ira Winkler
Secure Mentem

Samantha Manke
Secure Mentem

Session ID: HUM T-17

Session Classification: Intermediate

WHY SECURITY AWARENESS?

CAPTAIN KIRK

- Who wouldn't guess a password of "Captain" on an account with the user ID, "Kirk"?
- This happened at NSA

WHOSE FAULT IS IT?

- She sounds like an idiot
- She is an Ivy League graduate
- Why was she not previously told that she shouldn't have that as a password?
- Why was the password allowed in the first place?

THIS IS NOT UNIQUE

- Security professionals make assumptions in the base level of knowledge in end users
- Also extends to knowledge assumptions about other technical professionals
- As per Felix Unger, when you assume you make an ass/u/me

COMMON SENSE

- The problem is that security professionals assume that the users should exercise common sense
- There is no such thing as common sense without a base common knowledge
- Security programs fail, because they assume there is the common knowledge

IT'S NOT STUPID USERS

- It's incompetent security professionals
- While there are some stupid activities on the part of the users, I always ask what could the security staff have done better?
- Does your staff stop and ask how could the incident have been prevented
- Is there a discussion of both modifying user activity and preventing user activity

SECURITY AWARENESS IS IMPLEMENTING SECURITY CULTURE

- Not exactly, but close enough
- Security awareness is to get people to implement secure practices into their daily activities
- Must instill common knowledge of concerns and base actions
- Training is different from Awareness

WHY SECURITY CULTURE?

- The human factor
- Technology can only help so much
- Cost-effective solution
- Required by standards and regulations

THE STUDY: METHODOLOGY

OPPORTUNITY STATEMENT

- Work experience allowed me to build and improve many security awareness programs
- The local ISSA chapter's Security Awareness user group (a.k.a. "Support Group") meets bi-monthly and delegates were willing participants
- Security Awareness material is seen as non-proprietary

THE PROBLEM WITH SECURITY AWARENESS

- Varying degrees of quality in awareness programs
- The 3-year cycle
- Poor security cultures

APPROACH/METHODOLOGY

- Qualitative
  - Face-to-face interviews with Security Awareness Specialists
- Quantitative
    - 2 Surveys
      - 1 for Security employees
      - 1 for Non-Security employees
- Limitations

STUDY: ANALYSIS

ANALYSIS: GENERAL TRENDS

- Participating companies from the following sectors:
  - Health Sector
  - Manufacturing Sector
  - Food Sector
  - Financial Sector
  - Retail Sector
- Companies were often surprisingly honest about the success of their programs
- No participating company had any metrics to assess their effectiveness

ANALYSIS: GENERAL TRENDS

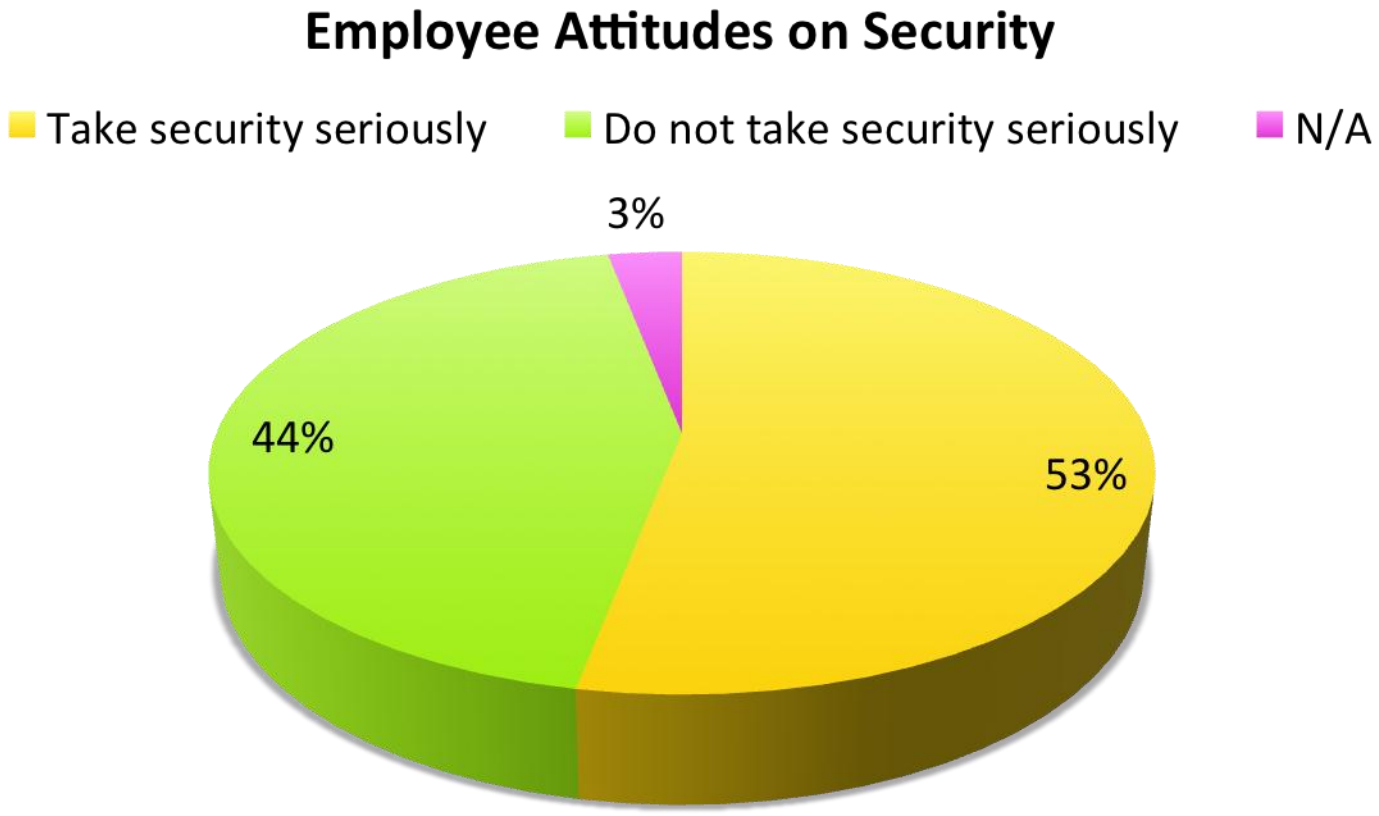
- Most companies struggle to gain support:
  - From upper management
  - From key departments
  - From their user population
- Compliance:
  - PCI helps with support and budget
  - HIPAA does not

ANALYSIS: GENERAL TRENDS

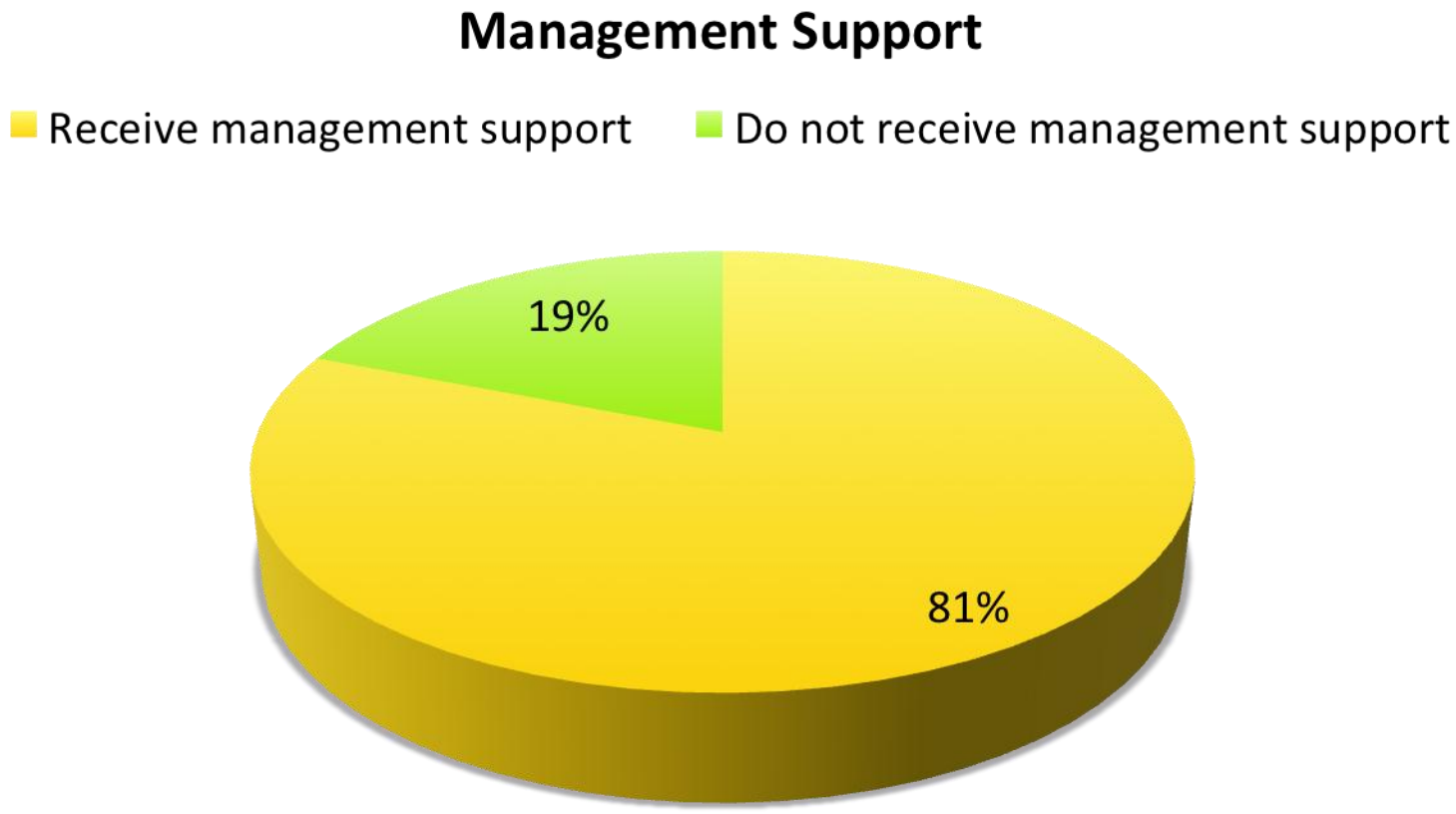
- Variety of approaches
  - Some Security Awareness Specialists had a security background while others had a marketing or communications background
  - Companies had 1-26 employees contributing to efforts

ANALYSIS: SECURITY RESPONDENTS

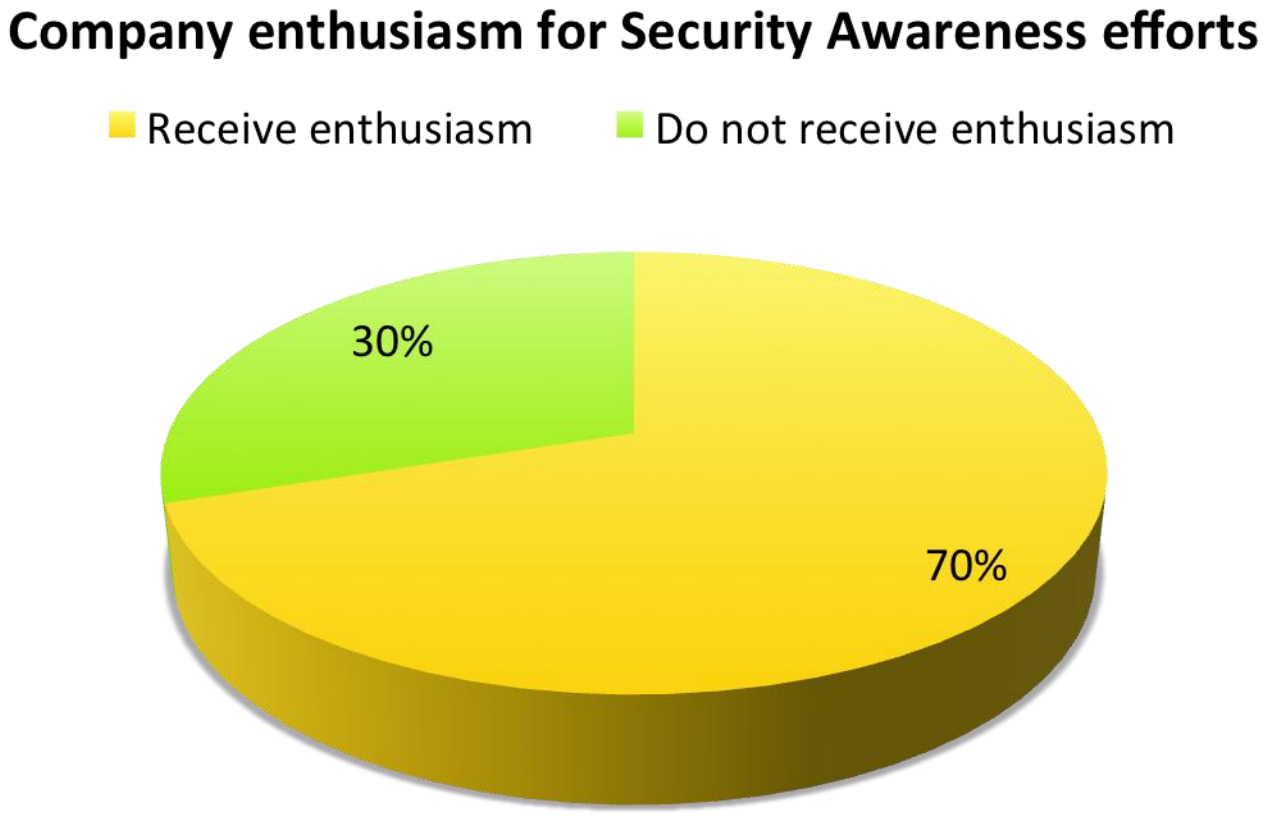
ANALYSIS: SECURITY RESPONDENTS



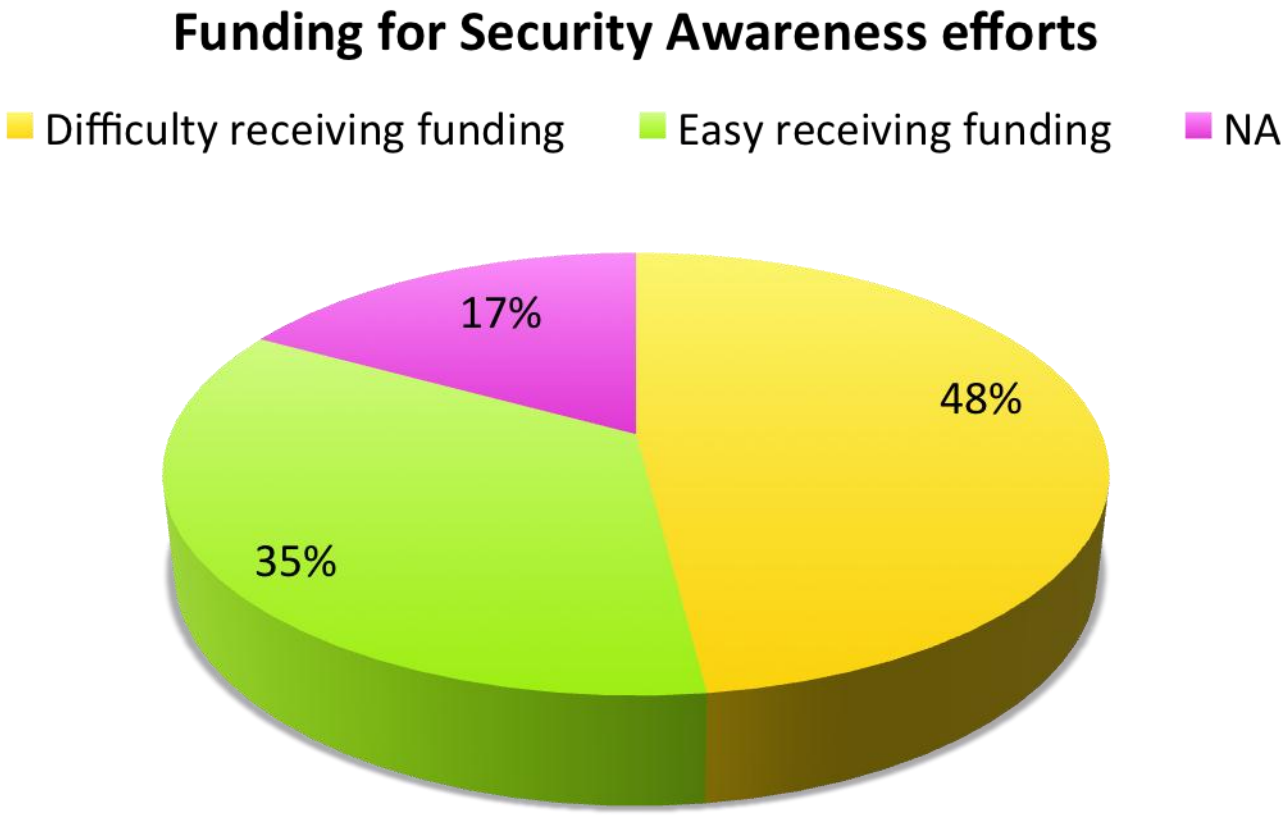
ANALYSIS: SECURITY RESPONDENTS



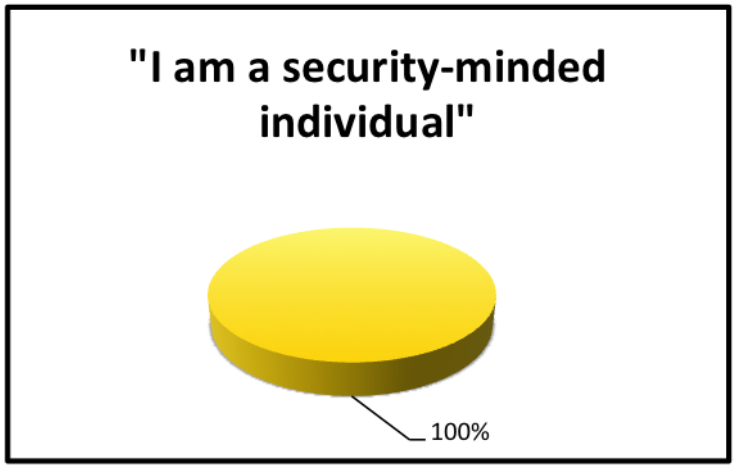
ANALYSIS: SECURITY RESPONDENTS



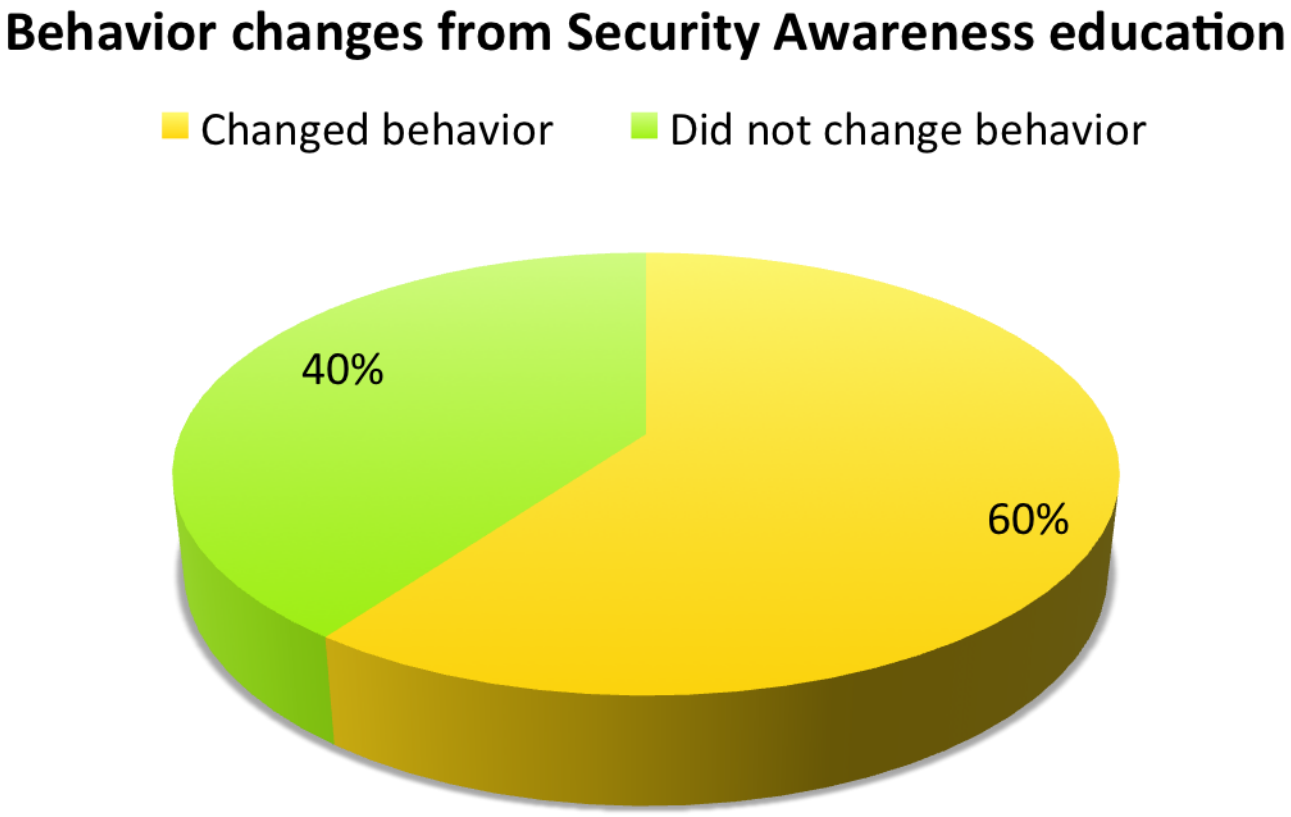
ANALYSIS: SECURITY RESPONDENTS



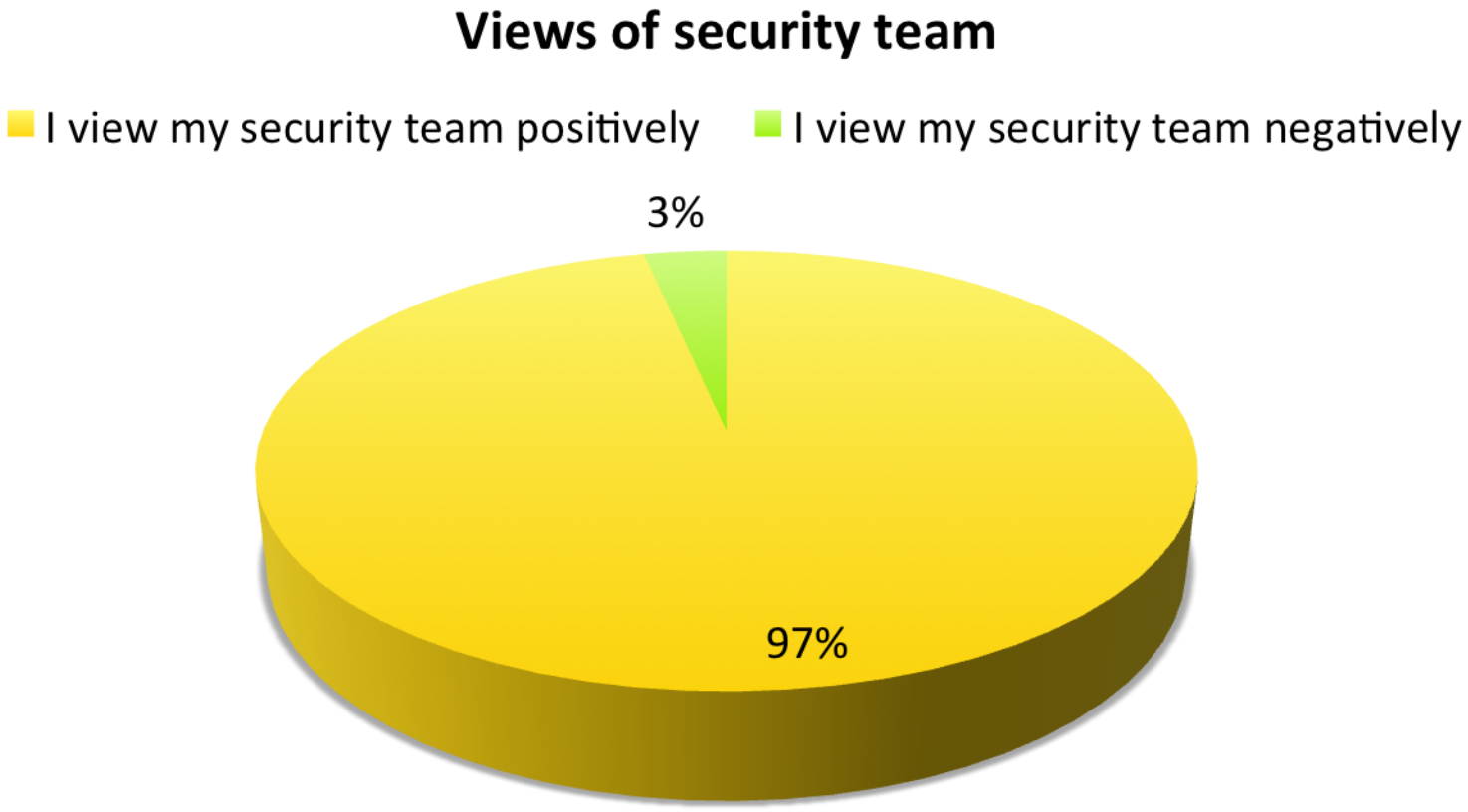
ANALYSIS: NON-SECURITY RESPONDENTS



ANALYSIS: NON-SECURITY RESPONDENTS



ANALYSIS: NON-SECURITY RESPONDENT



ANALYSIS: NON-SECURITY RESPONDENTS

RESULTS

- Security is difficult to administer at most companies
- PCI compliance helps with enforcement and awareness
- Creativity and/or participatory training are the key(s) to success
- Companies with more top-level support are more successful

THE HABITS

HABIT 1-CREATE A STRONG FOUNDATION

- This is the main source of failure
- Make a 3-month plan
- Topics may change
- Assess Approach
  - Softball
  - Hard push
  - Avoid fear-mongering

CHOOSING COMPONENTS

- Which mediums of communication will be most effective at your company?
- Which mediums are already saturated?
- What are employees most receptive to?

RECOMMENDED COMPONENTS

- Website
- Posters
- Newsletters/Blog
- Monthly tips
- Lunch and Learns
- Roadshows
- Speakers
- Security Week

KEEP THE PROGRAM FRESH

- Easy to fall behind
- Pay attention to the news
- Create new material for every month

HABIT 2-ORGANIZATIONAL BUY-IN

- Appeal to the highest level you are able to engage
- Market some materials to the C-level
- Stress benefits of Security Awareness

HABIT 3-PARTICIPATIVE LEARNING

- Learning modules
- Interactive components
  - Make user feel involved
- Additional tools--Phishing

HABIT 4-MORE CREATIVE ENDEAVORS

- Guerilla marketing campaign
- Security Cube
- Policy distribution
- Demonstrations and movie showings

HABIT 5-GATHER METRICS

- No participating company gathered metrics
- Compare rate of reported incidents pre and post
  - Collecting metrics ahead of time so you can potentially measure success after the fact

ASSESSING SUCCESS

- Assess which components have been successful
- Administer a survey
  - Try to keep it anonymous
  - Offer a drawing that employees can enter for a prize
- Understand limitations

HABIT 6-PARTNER WITH KEY DEPARTMENTS

- Reinforces company message vs. security message
- Consider departments such as:
  - Legal
  - Compliance
  - Human Resources
  - Marketing
  - Privacy
  - Physical Security

HABIT 7-BE THE DEPARTMENT OF HOW

- Department of “How” vs. Department of “No”
- Teach instead of dictate
- Establish positive security culture

CONCLUSIONS

APPLY

- Focus on building support before spending too much time on other aspects
- Do a thorough assessment of culture before starting or revamping program
- Consider partnership with other key departments
- Focus security awareness on common knowledge so users can exercise common sense

FOR MORE INFORMATION

Ira@securementem.com
+1-410-544-3435
www.facebook.com/ira.winkler
@irawinkler
www.linkedin.com/in/irawinkler

Samantha@securementem.com
+1-651-325-5902
@samanthamanke
http://www.linkedin.com/pub/samantha-manke/21/34/779