Impact of Security Awareness Training Components on Security Effectiveness: Research Findings

Federal Information Systems Security Educators' Association (FISSEA)
2012 Annual Conference
National Institute of Standards and Technology
March 27, 2012

Karen Quagliata, Ph.D., PMP

This session

We will be discussing my 2010 doctoral research conducted while I was a student at the University of Fairfax.

- What prompted me to choose security awareness training as my doctoral research topic
- How I went about conducting my research
- The findings from my research
- How those findings can be applied in the real world

Introduction

- 15 years experience in the information technology field in diverse capacities.
- Currently work within the financial services industry as an information security analyst, specializing in risk management.
- Entered information security because of its importance to the global economy.
- Chose security awareness for my doctoral research because of the unpredictable nature of humans.
- Published writer
- Author The Security Awareness Link blog – http://thesecurityawarenesslink.myblogsite.com
- Contact me at: karen.quagliata@gmail.com

Overview

- Information security studies have supported the concept that user awareness training is an important link in the security chain.
- As such, public and private organizations implement these security awareness programs.
- However, often times security awareness programs are established without considering how to determine whether a return would be made on their investment, or even what will ensure the program's effectiveness.

Problem

- Part of the problem is that few formal research projects have attempted to examine which components of security awareness training have the most significant impact on security effectiveness.

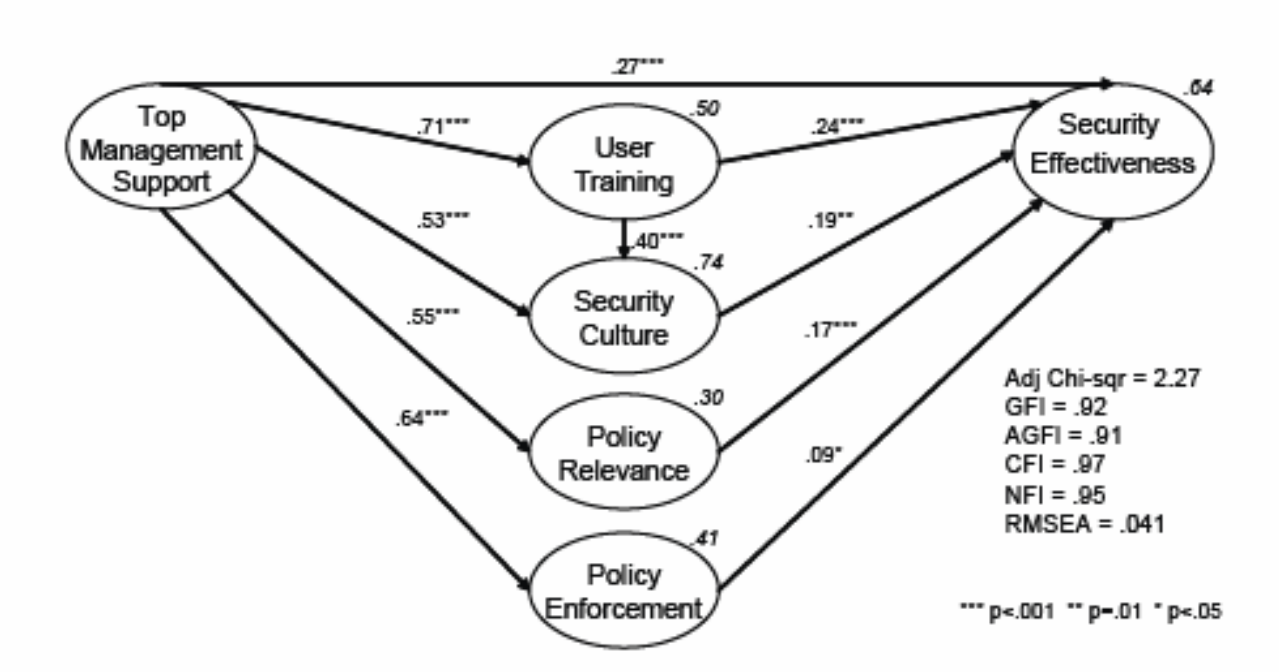
- It is not enough to merely instruct organizations to implement security awareness as part of their security strategies. They need more guidance on how best to do it.

Background

- The objective of my project was to extend Knapp's 2005 research.
- Knapp conducted research in which he addressed the question of what is the relationship of top management support on perceived security effectiveness, and what are the constructs that mediate that relationship.
- Knapp looked at the relationship between perceived security effectiveness and:
  - User training
  - Security culture
  - Policy relevance
  - Policy enforcement

Background

Knapp concluded that user training had a very strong relationship with security effectiveness.



Background

- I wanted to extract user training from Knapp's study and focus just on that component.
- I decided to examine three factors of security awareness training that appeared most frequently in my literature review:
  - Frequency of delivery
  - Method of delivery
  - Compliance monitoring
- I used a quantitative correlational/predictive research design to examine the patterns of association between the independent variables of training frequency, training method, and training compliance monitoring, and the dependent variable of perceived security effectiveness.

Purpose of research

- This research attempted to identify the key components of user training that will provide the greatest probability of security effectiveness.

- Caveat about correlational studies
  - They observe relationships between variables, but any correlation observed does not *prove* causation.
  - Correlation does not indicate which variable came first, and it does not rule out alternative explanations.

Research Methodology

- The research site used was ISACA. ISACA is an international professional organization comprised of all levels of IT professionals who are dedicated to the promotion of advanced IT governance, control and assurance practices.
  - IT professionals, rather than regular employees, were chosen for the research because they are more aware of IT security issues and are a more homogeneous group.
  - Presenting the survey to the random public would have likely resulted in more inconclusive findings because of the heterogeneous nature of such a large group.
  - Limiting the survey to one industry or organization would have limited the scope of the research.
- An online anonymous survey was used as the data collection tool.
- The survey used a five-point Likert scale to measure the participants' attitudes (Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree)

Research Questions

- The research was driven by three questions:
  - What is the relationship between **training frequency** and perceived security effectiveness as measured by the survey?
  - What is the relationship between **training delivery method** and perceived security effectiveness as measured by the survey?
  - What is the relationship between **training compliance monitoring** and perceived security effectiveness as measured by the survey?
- Why "perceived security effectiveness"?

  "based on the subjective judgment of security professionals"

Respondents

A total of 133 ISACA members, representing multiple industries, participated in the survey.

Function	Count	Percent
Audit professional	58	43%
Department manager/supervisor/director	22	17%
Information security professional	16	12%
MIS/IS/IT/technical management	15	11%
Other IT/technical/scientific/professional	7	5%
Other managerial	2	2%
Owner/partner	3	2%
Senior manager/Executive (e.g. CEO, CIO)	10	8%
Totals	133	100%

Country Demographics

The majority of respondents were from the US. India represented the second largest percentage.

Country	Count	Percent
United States	98	73%
India	23	17%
Costa Rica	7	5%
Australia	2	2%
Belgium	2	2%
China	1	1%
Totals	133	100%

Experience & Responsibilities

The majority of participants reported that information security is a secondary responsibility of their jobs.

Primary/Secondary	Count	Percent
Primary	53	40%
Secondary	80	60%
Totals	133	100%

Furthermore, the majority of participants had more than 15 years of professional experience.

Experience Level	Count	Percent
Less than 8 years	41	31%
Between 8 and 15 years	37	28%
More than 15 years	55	41%
Totals	133	100%

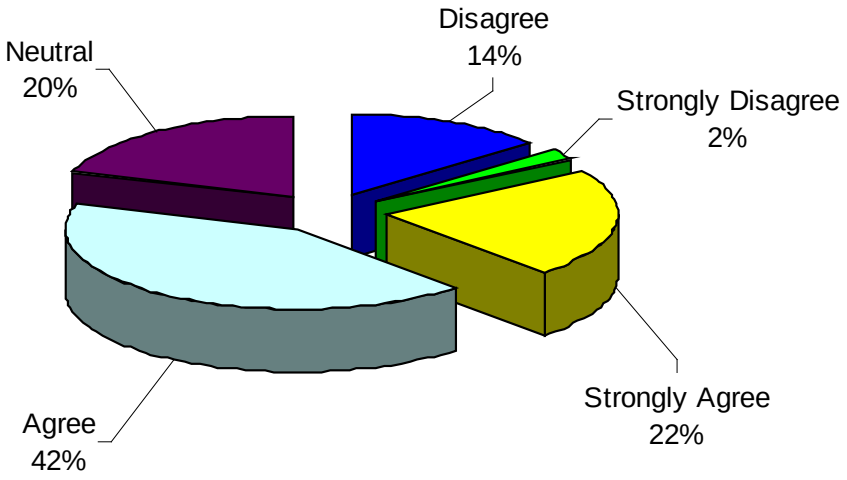
Findings

Six key findings came out of this research, which can be categorized as:

1. Overall security effectiveness
2. Training frequency
3. Training methodology
4. Training compliance monitoring
5. Training topics
6. Relationships

Overall security effectiveness

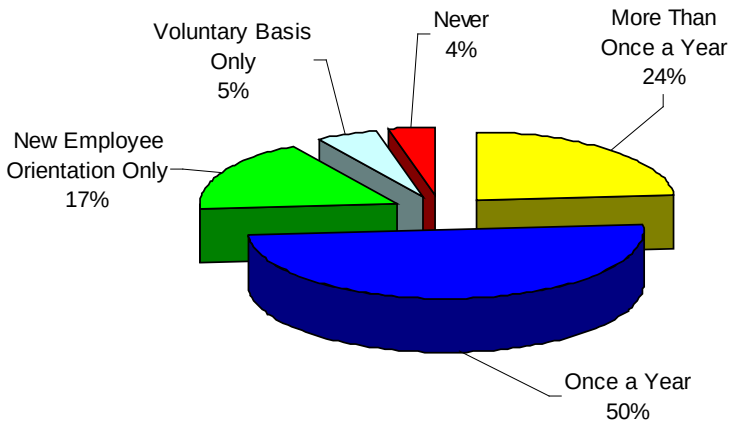
- Employees' perceptions toward security effectiveness is overall positive.
- Data shows that 36% of those surveyed believe that their organization is either not effectively securing its data, or were neutral on the subject.
- Bottom Line: There's room for improvement!



Training frequency

- The majority of respondents reported that their organization provides user security awareness training once a year.
- The “once a year” category had the highest rate of participants who strongly agreed that their organization secures its data and information effectively.
- Bottom Line: Research showed that the fewer times that employees are exposed to user security awareness training, the less likely they will be to view their organizations as effectively securing data.

N=133	My organization secures its data and information effectively		
Training Frequency	**Strongly Agree**	**Less than Strongly Agree**	**Totals**
Once a Year	15	51	66
More than once a year	11	21	32
New Employee Orientation Only	3	20	23
Voluntary Basis Only	0	7	7
Never	0	5	5
Totals	29	104	133



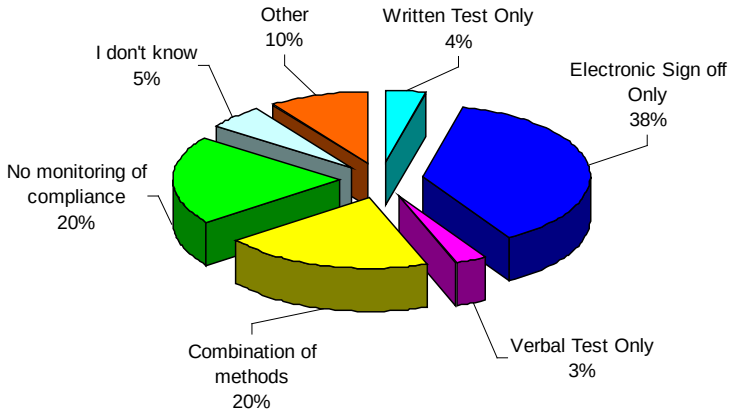
Training methodology

- Majority of organizations use some combination of methods to deliver training.
- "Combination of methods" category had the highest rate of participants who strongly agreed that their organizations secure their data and information effectively.
- Employees exposed to only one type of user security awareness training methodology were less likely to view their organizations as effectively securing their data.

N=133	My organization secures its data and information effectively		
Training Method	**Strongly Agree**	**Less than Strongly Agree**	**Totals**
Combination of Methods	24	69	93
Computer Based Training Only	2	6	8
All Methods	1	4	5
Policies & Procedures Only	1	11	12
Newsletter Only	1	1	2
Leader Led Training Only	0	8	8
Don't Know	0	2	2
Video Only	0	1	1
Posters Only	0	1	1
Brochure Only	0	1	1
Totals	29	104	133

Training compliance monitoring - Method

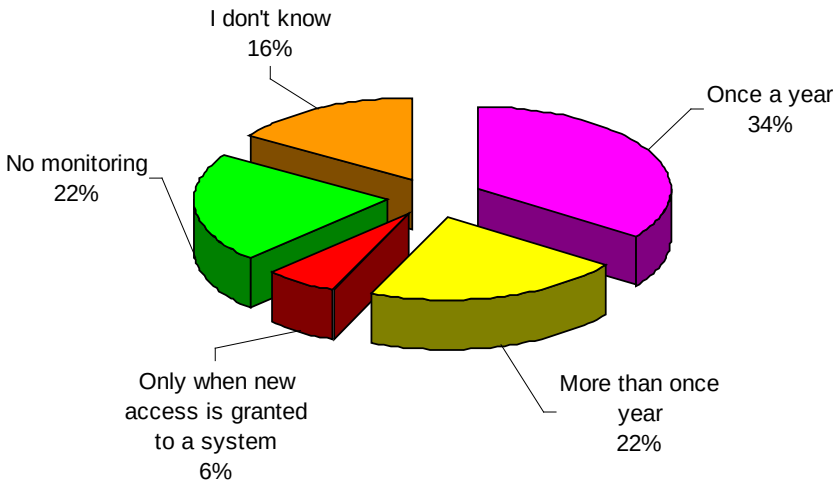
- Majority of respondents indicated that their organizations use electronic sign off only as the means for training compliance monitoring.
- 20% stated that their organizations use no training compliance monitoring methods.



N=133	My organization secures its data and information effectively		
Training Compliance Monitoring Method	**Strongly Agree**	**Less than Strongly Agree**	**Totals**
Electronic sign off	14	36	50
Combination of Methods	7	20	27
Verbal test	2	2	4
Written test	1	4	5
No monitoring	1	27	28
I don't know	0	7	7
Other	1	0	1
Written sign-off	0	6	6
SOX Testing	1	0	1
Policies, Audits, as part of other functional trainings	1	0	1
Automated Tools Monitor Security Sensitive Activity	0	1	1
Monitoring of user behavior	0	1	1
Web-based exam	1	0	1
Totals	29	104	133

Training compliance monitoring - Frequency

- The once-a-year is the largest group to strongly agree that their organizations effectively secure their data.
- More-than-once-a-year is the second largest group to strongly agree that their organizations effectively secure their data.



N=133	My organization secures its data and information effectively		
Training Compliance Monitoring Frequency	**Strongly Agree**	**Less than Strongly Agree**	**Totals**
Once a year	13	33	46
More than once year	9	20	29
I don't know	5	16	21
Only when new access is granted to a system	1	7	8
No monitoring	1	28	29
Totals	29	104	133

- 22% of respondents' organizations conduct no monitoring.

Training topics

- Most popular security awareness training topic pertains to e-mail, passwords, and Internet usage.
- Respondents whose organizations covered all of the topics included in the survey are the largest group to strongly agree that their organizations effectively secure their data.
- Bottom Line: Respondents whose organizations covered only one topic in their training were the least likely to strongly agree that their organizations effectively secure their data.

Security Awareness Training Topics	Count
Email	86
Passwords	83
Internet use	80
Locking work stations	74
Privacy	72
Data handling/classification	68
Social engineering	66
All of the topics listed	53
Network Security	47
Data Encryption	35
No user awareness security training is conducted	8
I don't know	2

Relationships

- Which components of security awareness training had the strongest correlation with perceived security effectiveness?
  - Training method – strong correlation
  - Training compliance monitoring – strong correlation
  - Training frequency – inconclusive
- What about training frequency?
- What about security culture?
  - Knapp's research and my research showed a strong relationship with security effectiveness.
  - security permeates all aspects of work in the organization
  - messages from all sources should be consistent

Respondents' comments

- "Training sessions are performed annually and attendance and understanding are monitored. However no action is taken that I know if someone does not participate in the training. It's just reported to management."
- "The biggest hurdle I see to InfoSec at an organization is fostering the daily awareness of security among the daily job tasks."
- "My organization is lax in security and information training but that will change within the next few months due to new Federal government regulations we must now adhere to."
- "Interesting survey, (but) I must say as a summary, companies are aware but costs often in budget are not there proactively."
- "We are a trading and manufacturing company located in the GCC (Gulf Cooperation Council). Generally the GCC countries are still in the year 2000, considering the maturity of information security conceptual understanding and practice followed."

Implications

Provide Training at Least Once a Year

- Not enough to provide training at new employee orientation only.
- Training on a voluntary basis has poor correlation to perceived security effectiveness.
- The field of education teaches us that humans learn better when they are exposed to a message repeatedly.
- Make sure the training program is sustainable and repeatable.
- Make sure leadership understands that security awareness programs are long-term efforts and require persistence.

Implications

Employ Multiple Training Methods

- The use of multiple methods of training produced the highest correlation to perceived security effectiveness.
- The majority of respondents state that their organizations use a combination of methods – good news!
- Research has shown that people recall more of what they hear *and* see together, versus what they only see or only hear.
- Reading policies and procedures is not an adequate training method!
- Mix it up – use blogs, email messages, newsletters, posters, computer-based training, leader-led training, and video.

Implications

Ensure Compliance

- Training compliance monitoring had a strong relationship with perceived security effectiveness.
- Monitoring should be an ongoing occurrence – not just once a year.
- Multiple benefits:
  - helps determine how well trainees are mastering the material
  - helps to evaluate the effectiveness of the training program
  - generates data that can be used in an organization's security metrics
- Methods include: Pre- and post-tests, surveys, and feedback
- Must be repercussions for noncompliance.
- Include security awareness training as part of employee performance appraisals.

Implications

Teach Relevant Topics

- Are passwords and email *really* the most relevant topics today?
- Review training topics on a regular basis –
  - use industry references (Verizon Data Breach Report, NIST, SANS, Ponemon Institute, etc).
  - scan industry publications for trends
  - identify training opportunities by reviewing your organization's IDS/IPS logs, change requests, variances from standards, security incidents - everything from unauthorized individuals entering your premises to computers infected with malware.
- Information security is a moving target!

Conclusion

This doctoral research was conducted to:

- Add to the information security body of knowledge.
- Equip information security practitioners with data that can be used to promote security awareness training within their organizations.
- Provide a guide post to help information security practitioners usher in a new era in cyber security awareness, training, and education by focusing on what matters most.

Questions