Designing the Path Forward: Security Awareness for the Indifferent Workforce
Agenda

Security Awareness Overview 5
Designing the Path Forward 8
Wrap Up 20
Hi! I’m Rose.

- Governance, Risk, & Compliance (GRC) Manager at Seiso, LLC
- 14 years in IT, 9 years in Security
- B.S. in Advanced Networking & M.S. in Cybersecurity and Information Assurance
- Industry experience: DoD, Healthcare, Education, Retail
My Talks...

Past recordings:

- Moscow Mules and NOP Slides Podcast... All things GRC
- Lessons Learned: Crash Course in ISMS Implementation
- The Overlooked Security Risk: 3rd Party Risk Management
- Designing the Path Forward: Security Awareness for the Indifferent Workforce

Upcoming:

- 10/2 Security Awareness Maturity Assessments (In-person, GA)
- 10/14 CMMC: Crawl, Walk, Run (Webinar)
- 10/26 CMMC: Control Breakdown (Webinar)
Security Awareness Overview
Security Awareness... What is it?

What?
Method to provide training to workforce for cybersecurity

Topics focus on safe habits:
- Computer
- Network
- Physical Security

Change the culture:
- Encourage positive interactions
- Facilitate conversations
2020 State of Phish – ProofPoint

A third-party survey of 3,500 working adults across seven countries (Australia, France, Germany, Japan, Spain, the United Kingdom, and the United States).

A third-party survey of 600 IT security professionals across the same seven countries.

More than 60M simulated phishing attacks sent by our customers over a 12-month period.

About 15M emails reported by our customers’ end users.

Impacts of Successful Phishing Attacks
- Loss of data: 60%
- Credential/account compromise: 32%
- Ransomware rotation: 27%
- Other malware infection: 29%
- Financial loss/wire transfer fraud: 16%

Frequency of Formal Training Sessions
- Never: 2%
- Quarterly: 5%
- Monthly: 12%
- Twice per year: 40%
- Yearly: 41%

Time Allocated to Formal Training Sessions Each Year
- 0-30 minutes: 24%
- 1-2 hours: 42%
- 2-3 hours: 17%
- Over 3 hours: 4%

Topics Covered in Security Awareness Training
- Phishing: 71%
- Wi-Fi security: 58%
- Mobile device security: 40%
- Password best practices: 44%
- Ransomware: 44%
- Malware: 43%
- Smishing: 43%
- Vishing: 41%
- Multi-factor authentication: 30%
- Business email compromise: 34%
- Best practices for remote working: 30%
- Compliance-related topics (GDPR, PCI, and so on): 28%
- Email reporting: 24%
- Insider threats: 20%
- Physical security measures ("look before you log," clean desk, etc.): 20%
Designing the Path Forward
Program Components

Overall Development
- Compliance / Regulatory\(^2\)
- C-level support
- Governance
- Partner with departments

Training Development
- Training and activities development
- Social engineering exercises (phishing)

Metrics Dashboard
Program Blockers

What is preventing overall success?³

• Time, not budget
• Technical program leads lack soft skills
• Strategic alignment (aka management buy-in)
Common Problems

Training Problems

- Given infrequently
- Not engaging enough
- Training not relatable

Behavioral Problems

- Not reporting suspicious behavior
- Repeat offenders
Types of Training

- Web-based (course, test, games, etc.)
- In-person (classes, conversations, etc.)
- Correspondence (newsletters, emails)
- Behavioral, role, and group-based (developers, administrators, etc.)
Frequency of Training

Compliance & Regulation
PCI, HIPAA, ISO, etc.

Event Driven
New Hire & Annual

Every 90 days
Rotate material to prevent overuse
Security Awareness Month

• October
• Promote all things security
• Make it fun!
  • Raffles
  • Games
  • Lunch & Learn Sessions
  • Posters
  • Videos

It's cybersecurity awareness month

Here's what you do: open your email, take a handful of best practices and throw them in there. Whatever people read - that's the correct dosage.
Social Engineering

Phishing Exercises

- Test the workforce via phishing exercise
- Determine if workforce understands phishing
- Retest the workforce on regular cadence
YEAH IF WE COULD JUST

STOP CLICKING ON PHISHING EMAILS, THAT'D BE GREAT.
IR Training

Incident Response

• Appropriate response if event / incident occurs
• Conduct tabletop exercise
• Provide plans, runbooks for use during event / incident
“If you can’t measure it, you can’t improve it.” – Peter Drucker

- Leverage SANS Security Awareness Maturity Model
- Metrics to understand the health of Security Awareness:
  - Track risky employee behavior
  - Frequency incidents are reported
  - Reported phishing email percentage
  - Assessment of employee knowledge
  - Employee completion of training
  - Overall maturity of program

SANS Institute Security Awareness Roadmap® scale
5 – Metrics Driven
4 – Long Term Sustainment
3 – Promoting Change & Awareness
2 – Compliance Focused
1 – No Awareness Program

Target State
Current State
2021 Annual Security Awareness Training

**Mock Metrics Dashboard**

*Metrics for workforce of 461 employees

** Indicates reduction in users clicking link

Phishing Exercise

<table>
<thead>
<tr>
<th>Month</th>
<th>User Clicked Link</th>
<th>User Reported to Security</th>
<th>User Did Nothing</th>
</tr>
</thead>
<tbody>
<tr>
<td>July</td>
<td>61</td>
<td>145</td>
<td>255</td>
</tr>
<tr>
<td>August</td>
<td>24</td>
<td>200</td>
<td>237</td>
</tr>
</tbody>
</table>

Sept. - Workstation Security

<table>
<thead>
<tr>
<th>Security State</th>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked</td>
<td>430</td>
</tr>
<tr>
<td>Unlocked / Unattended</td>
<td>31</td>
</tr>
</tbody>
</table>

*Completed* | *Not Complete*
Wrap Up
Wrap Up

Checklist

- Determine compliance requirements
- Receive C-level support
- Build partnerships with departments
- Develop program governance
- Develop training materials
- Conduct security awareness activities
- Build/report security awareness metrics
Contact Me

@rosesonger

linkedin.com/in/rosesonger

Rose.Songer@SeisoLLC.com
CONTACT US

412-206-6591
INFO@SEISOLLC.COM
SEISO-LLC
@SEISOLLC
References
