Security Champions Workshop

SANS European Security Awareness Summit 2017

LAB 1: GETTING STARTED

You're here because you either have a Security Champions program already, you're starting one, or you're thinking about starting one. Security Champions programs help us tackle a variety of challenges, and are designed specifically around a company's unique mission, environment, and opportunities. Let's start by thinking about how a program like this could fit into your company.

Let's talk about your company!

1) Which industry does your company work within? (Please circle)

Accounting	Legal
Agriculture	Logistics & Supply Chain
Automotive	Manufacturing – Aerospace
Banking/Finance	Manufacturing – Defense
Business Services/Consulting	Manufacturing – Industrial
Chemicals	Manufacturing – Other
Computer Services/Consulting	Media & Entertainment
Consumer Electronics	Metals & Mining
Consumer Packaged Goods	Nonprofit
Education	Pharmaceutical/Biotechnology
Energy – Nuclear	Real Estate
Energy – Oil and Gas	Retail Trade
Engineering & Construction	Software
Food & Beverage	Technology
Government – Civilian – Federal	Telecommunications
Government – Civilian – Regional or Local	Transportation
Government – Military	Travel & Tourism
Government – Law Enforcement	Utilities – Power
Healthcare	Utilities – Water
Hospitality	Utilities – Other
Insurance – Health	Wholesale Trade
Insurance – Other	Other

2) How many total employees does your company have? _____

2a) Of these, how many are full-time employees? _____

2b) Of these, how many of these are contingent workers? _____

2c) Does the size of your company workforce vary seasonally? Y / N

If yes, approximately when does this occur in the year? From a security perspective, are there any additional risks or changes to consider during these periods?

_____

3) Where is your company headquartered? Where are the other physical locations of your offices?

_____

Let's talk about your security team!

4) Looking at the size of your company (FTEs + CWs), what is the approximate ratio of your company's size to the size of the security team? Please consider all aspects of security (e.g., engineering, physical) when answering this question.

4a) Total number of employees (Question 2) from above) _____

4b) Total employees on security team _____

4b) / 4a) = _____

5) What are the top five words you'd use to describe your company's culture?

_____

_____

6) What are your company's core values?

_____

_____

_____

_____

LAB 2: WHAT PROBLEM ARE WE TRYING TO SOLVE?

To help identify and prioritize areas of opportunity and focus, let's start with your current challenges.

1) What are your top five challenges? Examples can include, but are not limited to:

- Policies not being followed
- Cultural challenges (both geographically and within company culture)
- Password reuse
- Tailgating
- Developers/engineers not coding securely
- No patching
- Lack of priority for security by product development teams
- Compliance-driven security
- Attitude that one person doesn't make a difference (but we know they do!)
- Phishing

_____

_____

_____

_____

2) Of these five challenges, circle your top three… and let's call them *opportunities!*

- Share these with your neighbors for the next 3-5 minutes.
- Do you have any areas of overlap? If so, discuss. If not, share more about the current state of these three challenges and any approaches you've tried to solve them.

_____

_____

3) When it comes to security, what is the overall problem you're trying to solve?

4) Why is this problem worth solving?

LAB 3: LET'S EXPLORE SECURITY CHAMPIONS!

Defining your goals

1) What are your goals for the program?

_____

_____

_____

_____

2) What are your non-goals, if any? What is *outside* of this scope?

_____

_____

_____

_____

3) What's the best way to solve this problem?

3a) Training – What kinds of training do your employees need, but not currently have?

_____

_____

_____

_____

_____

3b) Community – What can you do to further engage employees?

LAB 4: LET'S START BUILDING!

Defining the Champion's role

A clear description of the roles and responsibilities of a Security Champion can help team members, volunteers, and managers understand the definition of the role. Note that this document can be flexible as you develop your program, and can be crafted in collaboration with your Champions.

1) What is the current security state on the teams where you'd like a Champion?

_____

_____

_____

_____

2) What are some ways the Champion can help (e.g., escalating security questions to appropriate channels, assisting with security reviews)?

_____

_____

_____

_____

3) What will the top three responsibilities of your Security Champions be?

_____

_____

_____

4) What are some other ways your Champions can help you?

_____

_____

_____

_____

5) What will you provide your Champions in return?

_____

_____

_____

_____

5b) How will you train your Champions?

_____

_____

_____

_____

5c) What resources will you provide to your Champions?

_____

_____

_____

_____

Leadership support

6) Who can help support your program?

_____

_____

6a) What are the ways in which they can lend you their support?

_____

_____

6b) How much time do you estimate you'll ask of your leadership?

_____

_____

Time & communication

7) Speaking of time, how much time do you estimate you'll ask of your Champions per week? Per month? Per quarter?

7a) Per week: _____

7b) Per month: _____

7c) Per quarter: _____

8) How will you communicate with your Champions? How frequently? How will you enable your Champions to talk to one another?

_____

_____

9) How will you communicate the Champions program to your company?

Feedback & recognition

10) How will you recognize your Champions? What will they be recognized for?

11) How will you get feedback from your Champions? How frequently?

12) Will you solicit feedback from your company? If so, how and how frequently?

LAB 5: BUILDING YOUR PROGRAM PLAN

1) What will you start tomorrow?

_____

_____

_____

_____

2) What will you include in your program plan?

_____

_____

_____

_____

3) What will your program look like in three months?

_____

_____

_____

3a) In six months?

_____

_____

_____

3b) In a year?

4) Who can support you in this room?

4a) Amongst your peers and colleagues?

4b) Amongst your company's leadership?

REFERENCE DOCUMENTS

Naming exercise

What you'll need: 30-40 minutes, Post-Its, pens, and people!

5 minutes – What do we want people to think when they hear "security"?

3 minutes – What words and associations would we like to avoid?

10 minutes – Share ideas on whiteboard

10 minutes – Group ideas based on common themes

10 minutes – Narrow down and decide

Metrics to measure engagement

Compliance metrics

- % of trained Security Champions
- % of teams with a trained Security Champion by FY end

Impact metrics

- Attendance at trainings
- Attendance at community events and activities
- Understanding of security issues
- Results from assessments/quizzes-- baseline and post-training are best
- # of times Champions reach out to security partners for help/advice
- # of times security partners reach out to Champions
- # of times Champions reach out with feedback
- # of times Champions seek out deeper engagement (e.g., conferences, presenting talks)
- Tenure of Champions
- Anecdotal stories (don't forget the power of storytelling!)
- Reported satisfaction with program via surveys/focus groups/feedback forms

Sample roles & responsibilities

Champions/Ambassadors

- Be an ambassador for security
- Encourage secure practices among their team
- Publicly list participation in Security Champions program (e.g., long-range planning, personal development goals, internal channels)
- Attend mandatory Security Champions training
- Meet with security team owner regularly (e.g., monthly, twice per project, once per release cycle)
- Identify and fix or escalate security vulnerabilities and/or bugs
- Escalate security concerns to appropriate points-of-contact
- Communicate with Champions

Program Manager

- Create processes to help structure program operations
- Recruit and enroll new Champions into program
- Track attendance at training and community events
- Monitor metrics and update program as appropriate
- Encourage Champions to spend a clear and defined amount of time on the program
- Communicate with Champions

Community Manager

- Create a Security Champions community
- Engage Champions on internal networks
- Encourage Champions to collaborate with other Champions
- Recognize Champions' achievements, including notifying managers
- Develop and host motivational events/activities, including hackathons, scavenger hunts, lunches
- Distribute exclusive swag to show appreciation and motivate continued engagement
- Communicate with Champions

Technical Trainer/Partner

- Identify curricula and appropriate training for Champions
- Train Champions, with customized training if applicable
- Build and maintain relationships with Champions to continue engagement on security matters
- Answer questions on security, facilitating partnerships with scrum teams
- Collaborate on engagement and appreciation events
- Recruit and enlist Security Champions into the program

Sample line items for your budget

Training

- Curricula
  - Internal/custom-created by your company?
  - Vendor? Up to $500,000 depending on the scope and amount
  - May also require purchasing an LMS platform to run the curriculum
- Catering
  - Do you need to cater? Consider time of day and number of attendees
- Additional skill-building opportunities
  - External conferences
  - External security trainings

Community

- Relationship-building
- Recognition for their efforts (e.g. trophy or prize)
  - Can be free by sending an email or publicly recognizing a Champion during a meeting
- Collaboration/partnerships – these are free!
- Motivation/incentive
- Events/activities
  - Outside partner events (e.g., hackathons)
  - Internal events (e.g., escape rooms, scavenger hunts)
- Branding
  - Logo/graphic design
  - Printing materials
- Catering
  - Appreciation lunch/happy hour
  - Treats as motivation/appreciation
- Swag
  - Stickers
  - Water bottles
  - Mugs
  - Pins
  - T-shirts
  - Hoodies or jackets
  - Bags or backpacks
  - Socks
  - Thematic or branded swag
  - Webcam covers

Checklist to get started

- ☐ Breakdown of company culture
- ☐ Leadership buy-in via an executive sponsor
- ☐ Program plan
    - ☐ Overview and problem statement
    - ☐ List of roles and responsibilities
    - ☐ Time (staff and champion)
    - ☐ Space
    - ☐ Proposed budget
    - ☐ Plan for pilot program and gathering feedback
    - ☐ Plan for evaluation and gathering metrics

THANK YOU!

Thanks for joining us at the SANS European Security Awareness Summit 2017!

Cassie Clark, Salesforce – cassie.clark@salesforce.com

Jessica Chang, Dropbox – findjess@dropbox.com