Elevate Security

Your Program Is Awesome, Now Prove It

Masha Sedova, Co-Founder

Workshop agenda

- Intro to the problem
- Understanding our risks
- Data gathering conversations
- Understanding the data

30min

- Break out into groups
- Program planning time

40min

- Come back for read-out

20min

The Story

Each group of 4-5 people are all security team members of the same fictional company Sandalwood Forum.

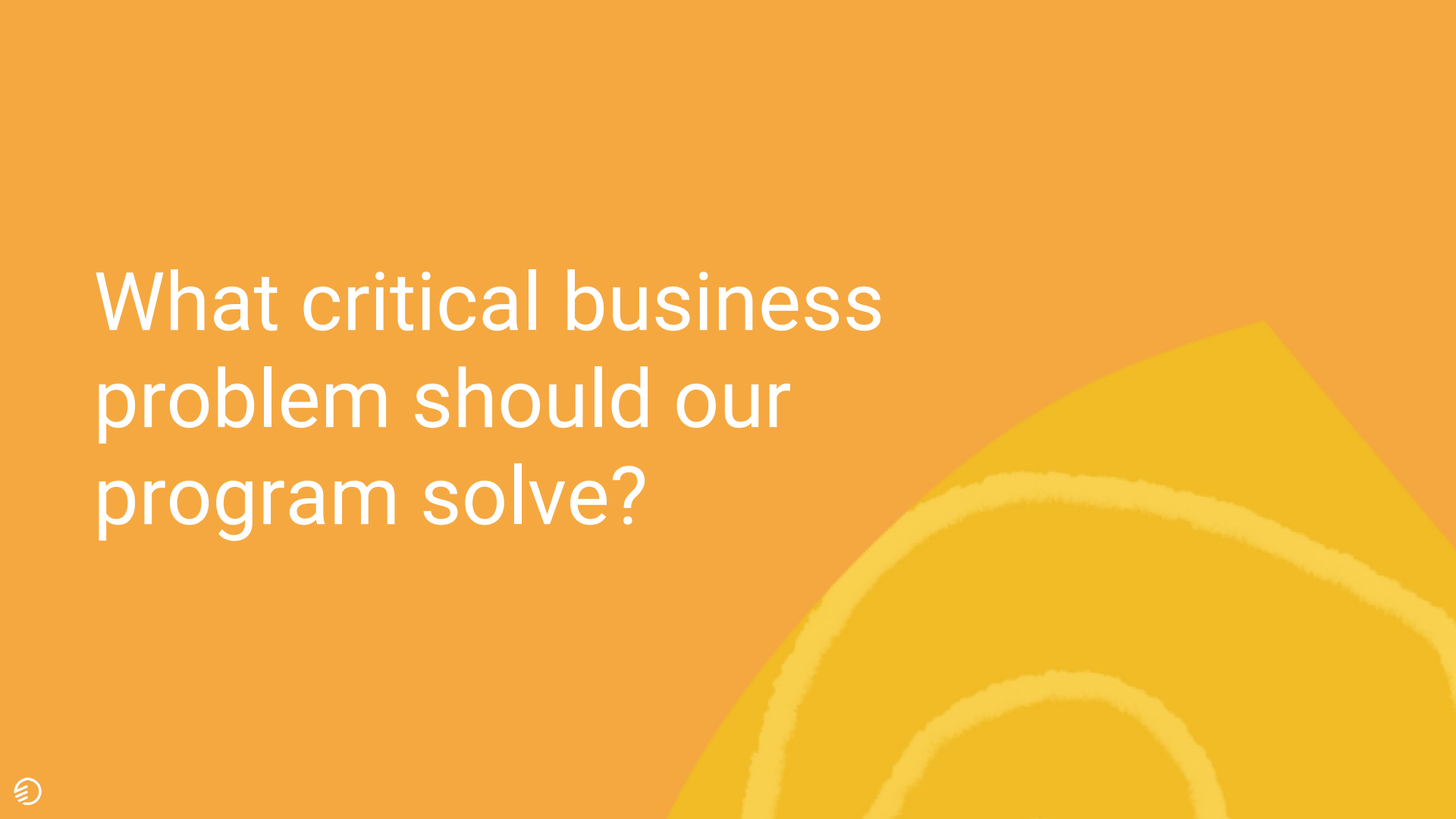
The Challenge

The company’s new leadership has prioritized managing **employee risk** as a top initiative in the next year. They’ve asked the team for a presentation on a key initiative of their choosing.

In order to get program sign-off and budget, leadership has asked for a data-driven approach presentation answering:

- Why this initiative was chosen
- How we will measure its impact

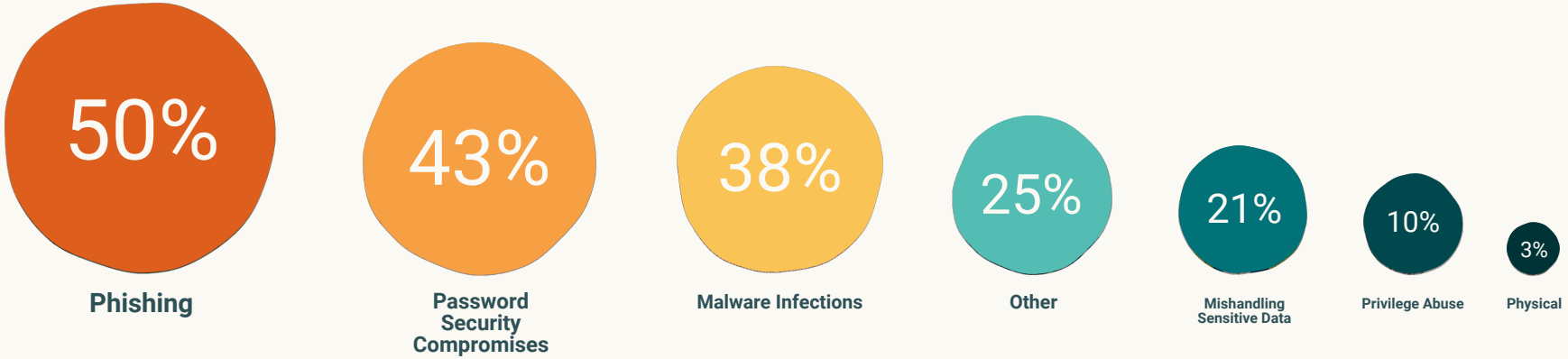
What critical business problem should our program solve?




Security
Operations
Center

State of Security at Lighthouse Company

Reasons for incidents over the last 3 years



Source: VDBIR 2020

An Incident is **more likely** to occur if an employee makes **more bad security decisions.**

An Incident is **less likely** to occur if an employee makes a **more good security decisions**.

...But what is a security decision?

Mapping Incidents To Their Underlying Behaviors

Decisions That Lead to
Phishing Incident

- Do I click on this link?
- Do I type in my credentials?
- Should I report this to my security team?

Decisions That Lead to
Password Compromises

- Do I click on this link?
- Do I type in my credentials?
- (Prior) Do I use a password manager for this site?
- (Prior) Do I turn on 2fa for this site?

Decisions That Lead to
Malware Infection

- Do I click on this link?
- Do I open this file?
- Do I run this even if its from an unknown source?
- (Prior) Should I snooze this security update request?

Data sets that can help us understand which decisions are happening in our company

Phishing Compromise

- Simulated Phishing data
- Real-world Phishing data
- Reporting data

Password Compromises

- Simulated Phishing data
- Real-world Phishing data
- Password Manager adoption
- MFA Adoption stats

Malware Infection

- Simulated Phishing data
- Real-world Phishing data
- Malware infection data
- Patching Status


Security
Engineering
IoT
64%
Sales Promotion

Pull data from tools you already have

Real World Phishing

Office 365 · proofpoint · cisco · G Suite

Phishing Simulations

KnowBe4 · COFENSE · Elevate Security

Reporting

KnowBe4 · COFENSE · G Suite · Office 365

Device Security/Patching Status

jamf · Microsoft Intune · mobileiron

Malware

Carbon Black. · CROWDSTRIKE · Office 365 · Symantec. · G Suite

HR/Directory Data

workday. · okta · Active Directory

MFA Adoption

onelogin · Office 365 · okta · G Suite

Password Manager

LastPass ••• · dashlane · 1Password

Pull data from tools you already have

Real World Phishing

Office 365 · proofpoint · cisco · G Suite

Phishing Simulations

KnowBe4 · COFENSE · Elevate Security

Reporting

KnowBe4 · COFENSE · G Suite · Office 365

Device Security/Patching Status

jamf · Microsoft Intune · mobileiron

Malware

Carbon Black. · CROWDSTRIKE · Office 365 · Symantec. · G Suite

HR/Directory Data

workday. · okta · Active Directory

MFA Adoption

onelogin · Office 365 · okta · G Suite

Password Manager

LastPass ••• · dashlane · 1Password

HR Data

Person Id	Manager Id	Last Name	First Name	Email	Start Date	Department	Work Location Geo	Title	Is Manager?	Is Active?
33652	24113	Keller	Laura	LauraKeller@sandalwood.org	3/8/14	Engineering	AMER	Engineering Executive	YES	YES
32291	90968	Rojas	Linda	LindaRojas@sandalwood.org	7/30/17	Marketing	APAC	Marketing Manager	YES	YES

Malware

Person Id	Email	Date	Event_Type	Device_ID	IP_Address
33652	LauraKeller@sandalwood.org	11/14/19	Downloaded	Laura's Macbook	34.120.88.252
90968	DeborahBrown@sandalwood.org	10/28/19	Installed	Deborah's Macbook	143.195.84.150
16268	MarciaBaker@sandalwood.org	5/27/19	Blocked	Marcia's Macbook	88.33.255.227

Password Manager

Person Id	Email	Has Installed?	Is Active?	Account created?	Date
24114	JamesJohnson@sandalwood.org	YES	YES	8/4/19	8/7/19

MFA

Person Id	Email	Installed?	Type	Date enabled
24114	JamesJohnson@sandalwood.org	YES	Token	9/30/17
18581	MonicaContreras@sandalwood.org	YES	SMS	4/1/19

Phishing

Phishing campaign id	person_nid	email	status	send_date	modified_date	details
219553	90968	DeborahBrown@sandalwood.org	Email Sent	4/1/19	4/1/19	Payload-1231944820941576062551469417387826431044
219553	90968	DeborahBrown@sandalwood.org	Email Opened	4/1/19	4/11/19	Payload-1231944820941576062551469417387826431044
219553	90968	DeborahBrown@sandalwood.org	Reported	4/1/19	4/12/19	Payload-1231944820941576062551469417387826431044
181119	28245	JessicaStewart@sandalwood.org	Email Sent	6/30/19	6/30/19	Payload-2444503224361362201120707566887100368744
181119	28245	JessicaStewart@sandalwood.org	Email Opened	6/30/19	7/5/19	Payload-2444503224361362201120707566887100368744
181119	28245	JessicaStewart@sandalwood.org	Clicked Link	6/30/19	7/6/19	Payload-2444503224361362201120707566887100368744

Reporting

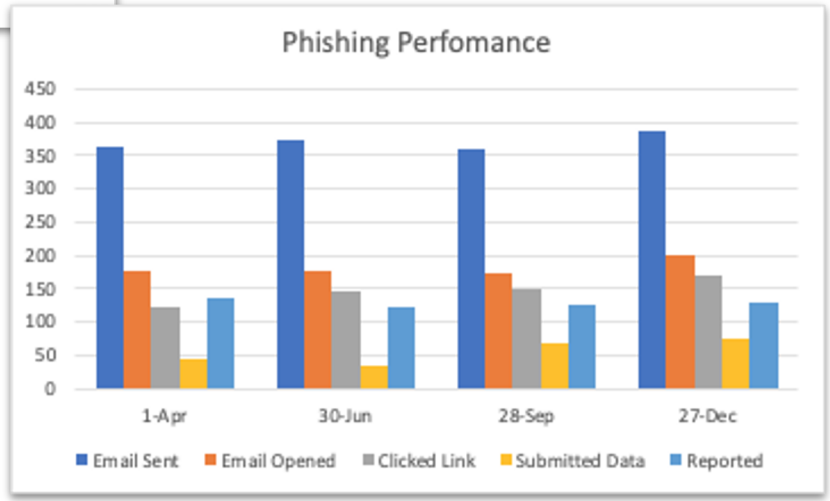
person_nid	sender_email	send_date	message_subject
90968	DeborahBrown@sandalwood.org	4/1/19	This is a suspicious email...

Tools for analysis

Department Analysis

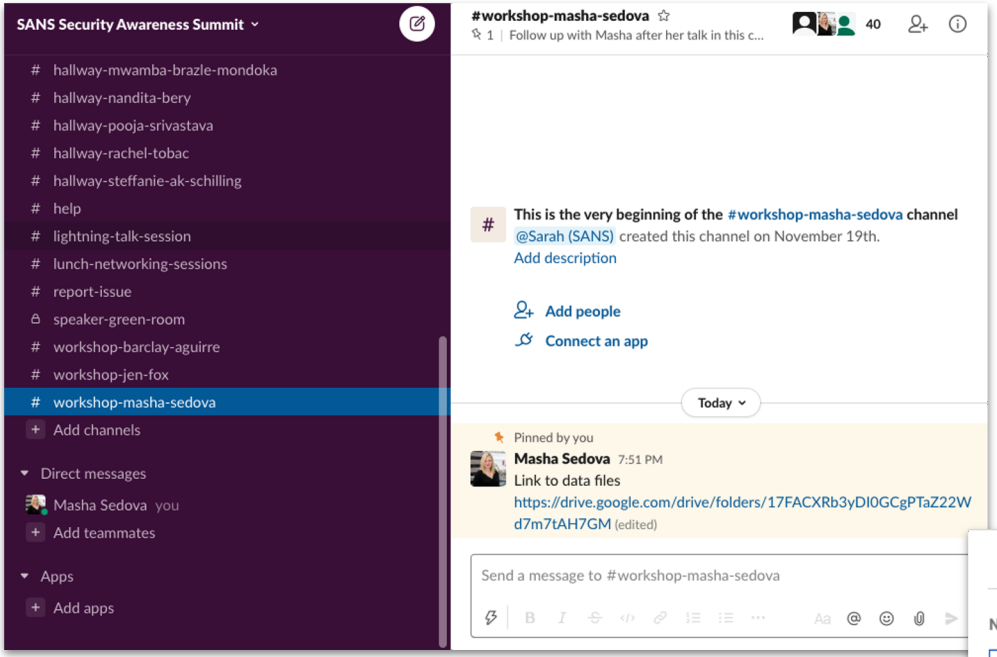
work_location_geo	(All)
is_manager	(All)

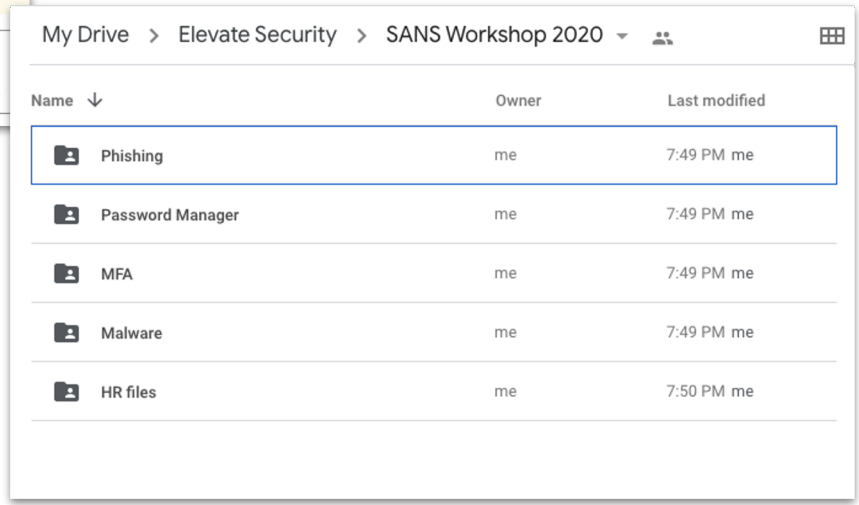
Incident Count	Phishing Action					
Department	Email Sent	Email Opened	Clicked Link	Submitted Data	Reported	Grand Total
Engineering	344	62	20	4	220	650
Finance	396	86	26	9	238	755
HR	360	87	23	11	212	693
Marketing	387	83	26	8	245	



The Setup

1. Break out into groups of 4-5 people
2. Introduce yourselves to each other!
3. As a group, pick one key risk to focus on: Phishing, Password compromises, or Malware Infection
4. Obtain the necessary data sets +HR file for your area of risk focus (link in slack)
5. Run analysis on your data sets to understand trends in employee behavior in your org
6. Use your trend analysis to recommend a program


SANS Security Awareness Summit
hallway-mwamba-brazle-mondoka
hallway-nandita-bery
hallway-pooja-srivastava
hallway-rachel-tobac
hallway-steffanie-ak-schilling
help
lightning-talk-session
lunch-networking-sessions
report-issue
speaker-green-room
workshop-barclay-aguirre
workshop-jen-fox
workshop-masha-sedova
Add channels
Direct messages
Masha Sedova you
Add teammates
Apps
Add apps
#workshop-masha-sedova
1 | Follow up with Masha after her talk in this c...
40
This is the very beginning of the #workshop-masha-sedova channel
@Sarah (SANS) created this channel on November 19th.
Add description
Add people
Connect an app
Today
Pinned by you
Masha Sedova 7:51 PM
Link to data files
https://drive.google.com/drive/folders/17FACXRb3yDI0GCgPTaZ22Wd7m7tAH7GM (edited)
Send a message to #workshop-masha-sedova


My Drive > Elevate Security > SANS Workshop 2020
Name
Owner
Last modified
Phishing me 7:49 PM me
Password Manager me 7:49 PM me
MFA me 7:49 PM me
Malware me 7:49 PM me
HR files me 7:50 PM me

The Deep Dive

Once you have the data set, use it to figure out how to focus your program.
Here are some questions you may want to answer.

- What is my organization's worst behavior today? Which has been getting worse over time?
- Which geography is my weakest? Which is my strongest?
- Who are my top performers? Who have consistently been my top performers?
- Who are my stragglers?
- How many risky managers do we have?

Use this data to provide program recommendations. Here are just a few examples:

- Which region to run more security awareness activities next october.
- Who needs more targeted training and on what topic
- Who would make good participants in the champion program
- Which execs need greater support

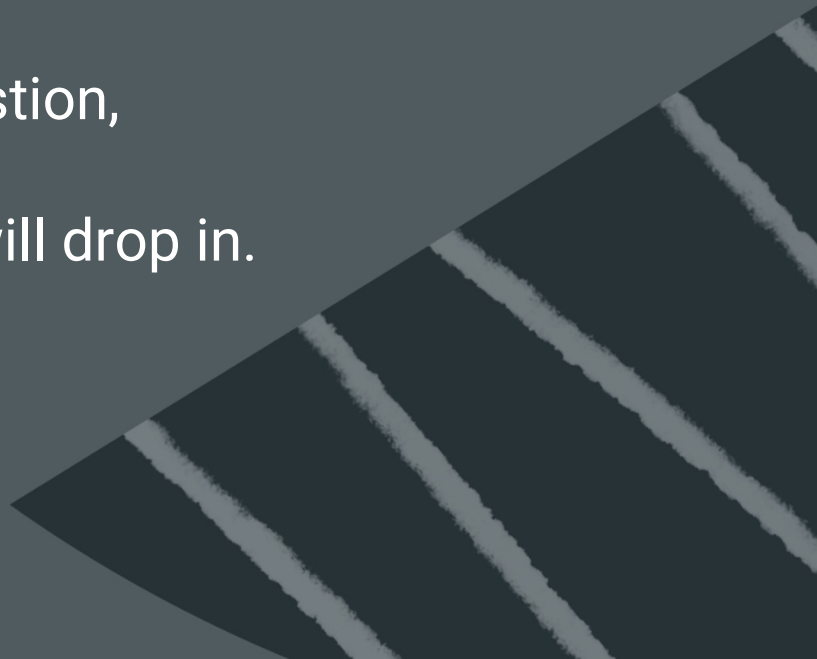
Preparing the presentation

At the conclusion of your analysis, prepare a presentation to the C-suite of Sandalwood answering the following:

- What risk (phishing, malware, passwords) you are focusing on
- What behaviors/security decisions you are tracking
- What insights you found in the data
- How you are going to shape your program using the answers from the data
- Who you needed to partner with going forward to track your progress on this program
- What are your next steps to prove ROI on their program and get more funding/support?

Stuck? Questions?

@mention me on slack with your question,
or
your zoom breakout room # and we will drop in.



Elevate Security

Q&A

Feedback survey:

sansurl.com/secaware-eval-day1

Ask your questions in Slack:

#workshop-masha-sedova