Using CTFs to enforce security awareness in your organization

Casey Trader - Mid-State Technical College

Disclaimer

The views and opinions expressed in this presentation are mine and do not reflect the views and opinions of Mid-State Technical College.

Reality check

This isn’t some magical “turn key” solution and should supplement what you are already doing

Definitions

- **Attack surface:** the sum of all the points through which an attacker could infiltrate your organization
- **Security awareness:** a program whose focus is educating users about computer and information security
- **Phishing:** attempts to fraudulently obtain sensitive information from users by appearing as a legitimate entity

What is the biggest vulnerability in an organization?

Users

Source: reality

Where are security budgets being spent?

Table 6. Operational Areas that Account for Security Spending

Operational Area	% Response
Protection and prevention	72.4%
Detection and response	62.8%
Compliance and audit (including legal)	58.6%
Risk reduction	49.7%
End user training and awareness	45.5%
Governance/Policies	43.4%
Staff training and certification	39.3%
Security program or project management	38.6%
Design/Development	34.5%
Discovery and forensics	31.7%
Other	2.1%

(Filkins, 2016)

Here is the problem

- IT/Security are being given tools to train end users
- Requests for staff to provide training are unfilled
- Requests for 3rd party awareness training go unfilled
- The result is "cheap" automated training/awareness tools

Table 8. Breakdown of Unfilled Requisitions

Incident Type	Tools	Staff	Services
Compliance and audit (including legal)	18.3%	23.1%	12.5%
Design/Development	12.5%	16.3%	4.8%
Detection and response	27.9%	26.0%	6.7%
Discovery and forensics	21.2%	14.4%	7.7%
End user training and awareness	16.3%	22.1%	16.3%
Governance/Policies	9.6%	18.3%	7.7%
Protection and prevention	25.0%	17.3%	7.7%
Risk reduction	19.2%	18.3%	6.7%
Security program or project management	12.5%	21.2%	10.6%
Staff training and certification	14.4%	20.2%	15.4%

First Second Third

(Filkins, 2016)

Question

How do you protect your largest attack surface on a limited budget?

Answer

Create a ***WORTHWHILE*** security awareness program

What is “worthwhile”?

It **IS** something that:

- engages users
- explains the benefit
- provides incentives

It **IS NOT** something that:

- uses only automated trainings
- penalizes users
- expects users will just “do it”

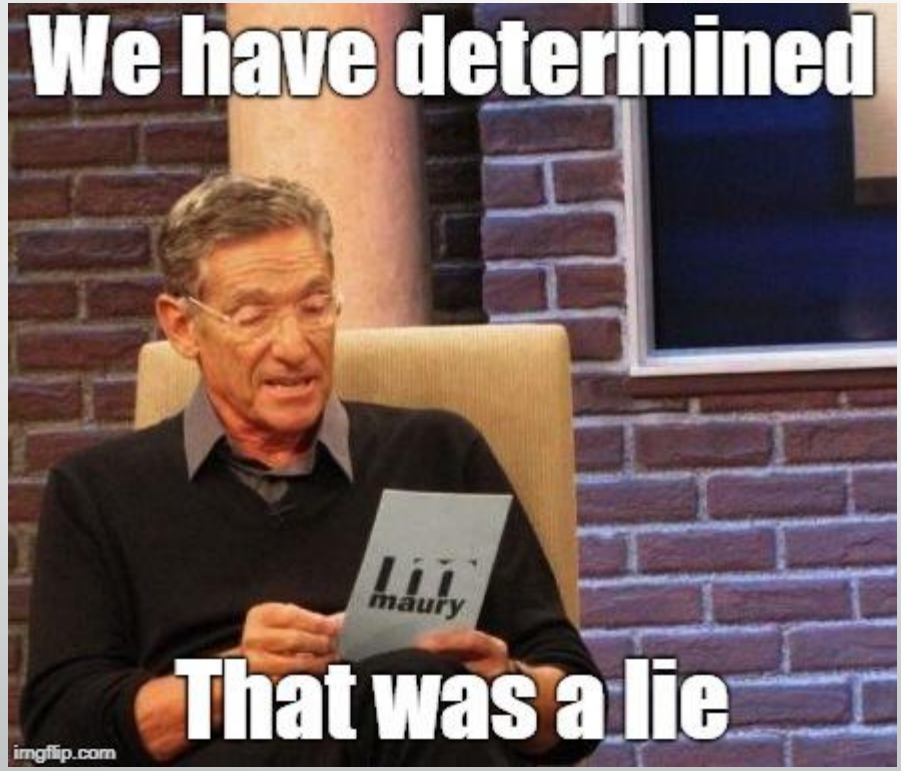
Why make it “worthwhile”?

1. It’s a better investment of time and money
2. Can spawn knowledge transfers between teams
3. Can help to uncover hidden talent within an organization

Are automated trainings “worthwhile”?

NO

My salesperson said their “CBT” is good!



How do I do this?

Use CTFs!

…hence the name of the presentation

What is a CTF?

- CTF stands for “Capture the Flag” and is a competitive event
- Participants seek out “flags” or “answers” to questions for points
- Clues get participants started
- The event lasts for a predetermined amount of time
- At the end of the event the top teams/participants are rewarded

Why a CTF?

- It encourages teamwork
- It requires participants to think critically
- It can "gamify" learning which is highly effective
- It uncovers hidden talent
- It is low cost

What does Casey do?

- Semester challenges in the classroom
- Capture the Campus event
- Extra credit opportunities
- Security club does them to help hone skills
- ***I use them to trick students into teaching themselves***

Ideas for using a CTF to help raise awareness

- http://www.superlegitwebsite.com/user/login.php?q=flag{super-sneaky}
- Have emails look legit but have flag in the text
- Gift card incentive
- Attempt to “tailgate”
- Personal security assessment

Tips for using a CTF to help security awareness

- Challenge both IT and non-IT employees
- Have IT and non-IT employees on the same teams
- CTF should not require hacking/coding tools
- Try not to penalize employees
- Run event(s) on a monthly or quarterly basis

Resources to get started

CTFd - https://github.com/CTFd/CTFd

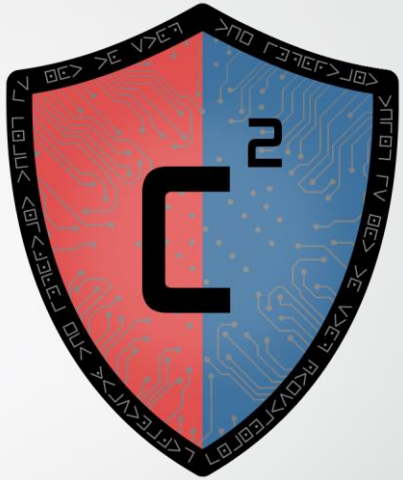
Facebook CTF - https://github.com/facebook/fbctf

CTFLearn - https://ctflearn.com/

E-mail -> casey.trader@mstc.edu
LinkedIn -> https://www.linkedin.com/in/caseytrader

Questions?

Mini CTF Demo



- Register at: https://ctf.caseytrader.com
- Timeframe: **NOW** until **4pm**
- **Prizes:**
  - 1st place -> $20 Starbucks gift card
  - 2nd place -> $10 Starbucks gift card
  - 3rd place -> $10 Starbucks gift card
- Total cost to run this event = $45 including prizes

Resources

- Filkins, Barbara. (February 2016). IT Security Spending Trends - SANS Survey (https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697)