


Don't Stop Believing on this



October 26, 2023



 <http://slides.dfirmatt.com>



Matt Scheurer

About Me

I work for a big well-known organization...



As an Assistant Vice President (AVP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

<https://threatreel.com>

Connect / Contact / Follow Matt:



<https://www.linkedin.com/in/mattscheurer>



@c3rkah (<https://twitter.com/c3rkah>)

Where I volunteer...

I am an Official



Advocate

<https://www.hackingisnotacrime.org>

I am also a



Women's Security Alliance
(WomSA) Technical Mentor

<https://www.womsa.org>

Disclaimer!

Yes, I have a day job.
However...

Opinions expressed are
based solely on my own
independent security
research and do not
express or reflect the views
or opinions of my employer.



Inspiration for this talk

I'm tired of
seeing the
cybercriminals
win! I think we
can do better
together.

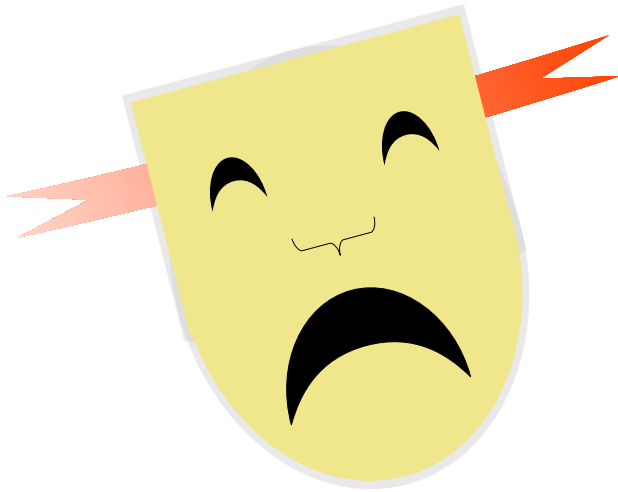


Threats Today

Hello
my name is

Skilled Adversary

Today's Threat Actors



Advanced Persistent Threats (APT's)

Nation States

Threat Actor (TA) groups

Organized Crime

Financially Motivated Actors

Cybercrime as a Service

Shopping List

Distributed Denial of Service (DDoS)

Initial Access Brokers

Phishing as a Service (PhaaS)

Ransomware as a Service

Just shy of an infomercial

**Breach
- N -
Leak**

Quantities Limited!!!

**Cybercriminal
Strength!**

<https://evil-cybercriminal.onion>

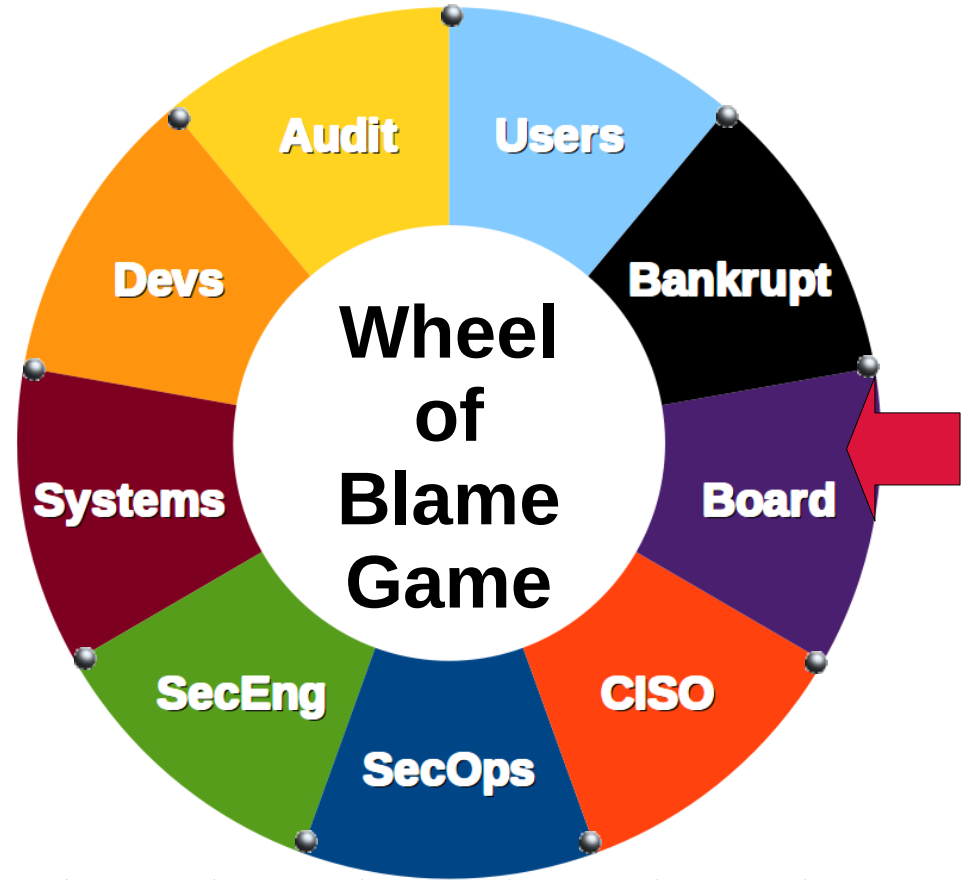
Cyber Criminals are doing well



Let's take a look at how we are doing as Tech Defenders today...

Too often, we're closer to here

“I mean, the breach couldn't have been my fault...”

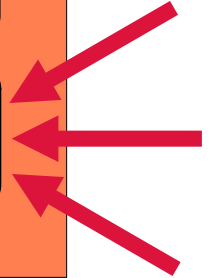
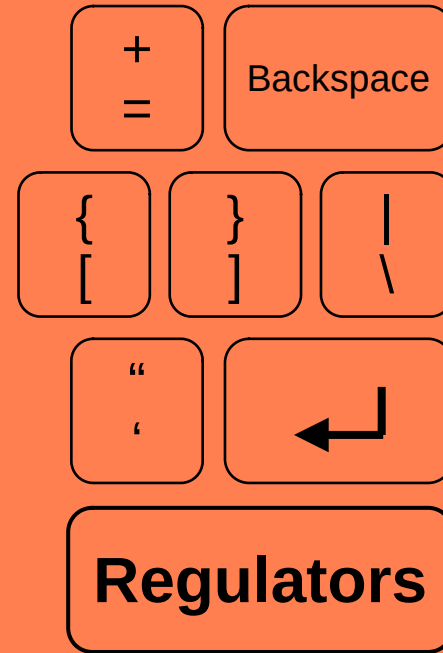


Or just blame our Regulators

Chance

**THIS CARD MAY BE KEPT
UNTIL NEEDED OR SOLD**

GET OUT OF BLAME FREE



The issue with the blame game

As my own mother would say...



"If you point a finger at someone, three fingers are pointing back at you!"

Global Thermonuclear Blame is...


A STRANGE GAME.
THE ONLY WINNING MOVE
IS NOT TO PLAY.

The CiNPA Security SIG

I used to run a Cincinnati-area monthly InfoSec meetup group:



Renowned Speaker Alumni



Amanda Berlin

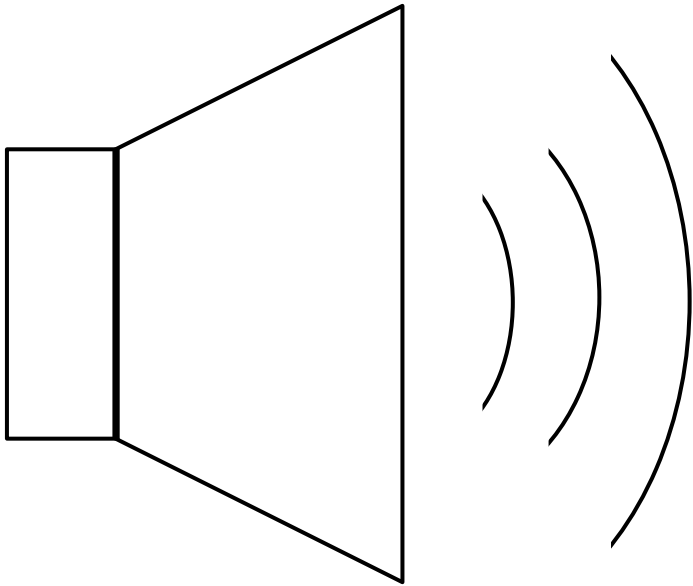
Phillip Wylie

Jorge Orchilles

Deral Heiland


Dave Kennedy

Other Quality Speakers



- Many former DerbyCon speakers
- Past BSides conference speakers
- Multiple SANS Instructors
- Amazing security researchers

Outcomes




Education and knowledge shares!
Professional Connections
Job Opportunities
Friendships
Timeless Funny Stories and Memories

Social Engineering Focus Group


Management at work
tasked me to organize
and run a brand new
internal enterprise
collaborative cross-team
Social Engineering
attack surface reduction
focus group program

Social Engineering Timeline

Pre-1940's + 

1950's + 

1970's + 

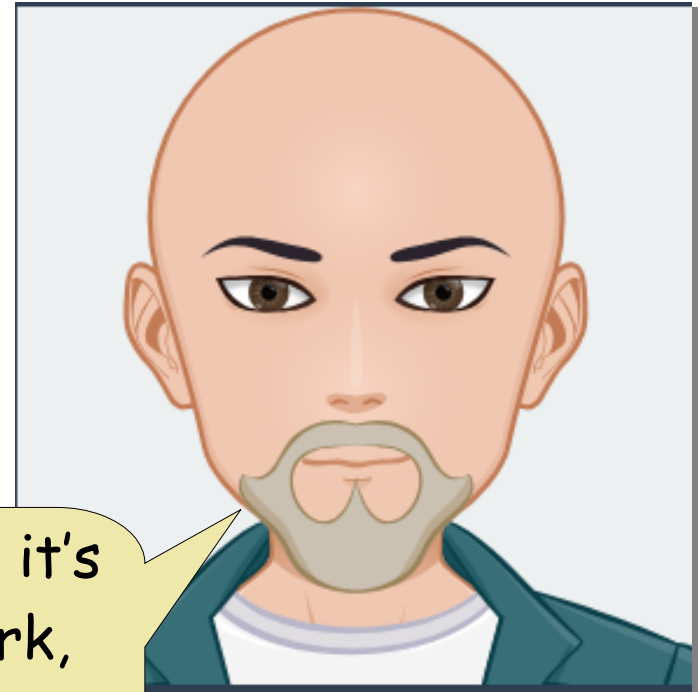
1990's + 

2000's + 

Enthusiasm in the beginning

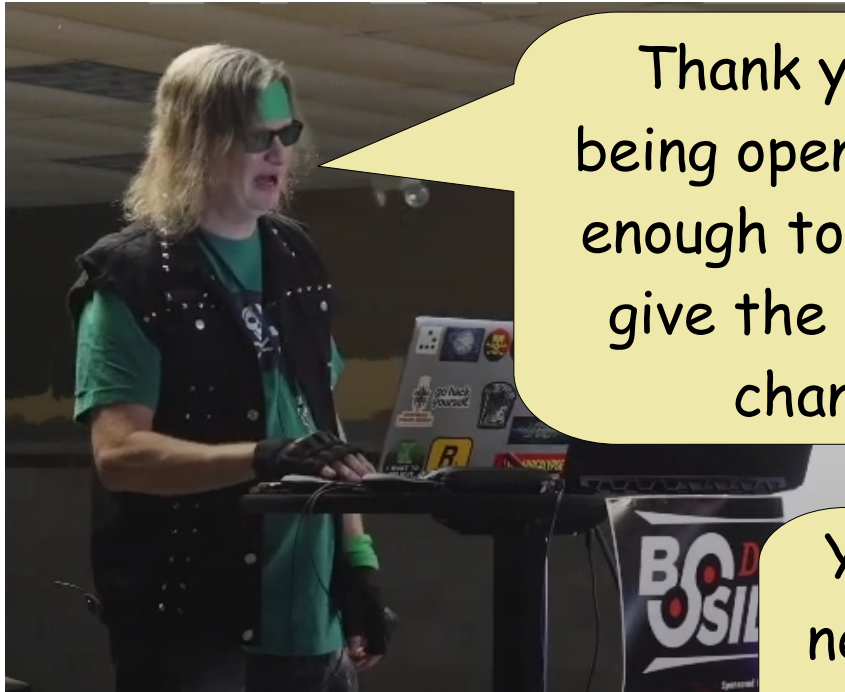


We're building something new to help combat Social Engineering threats!

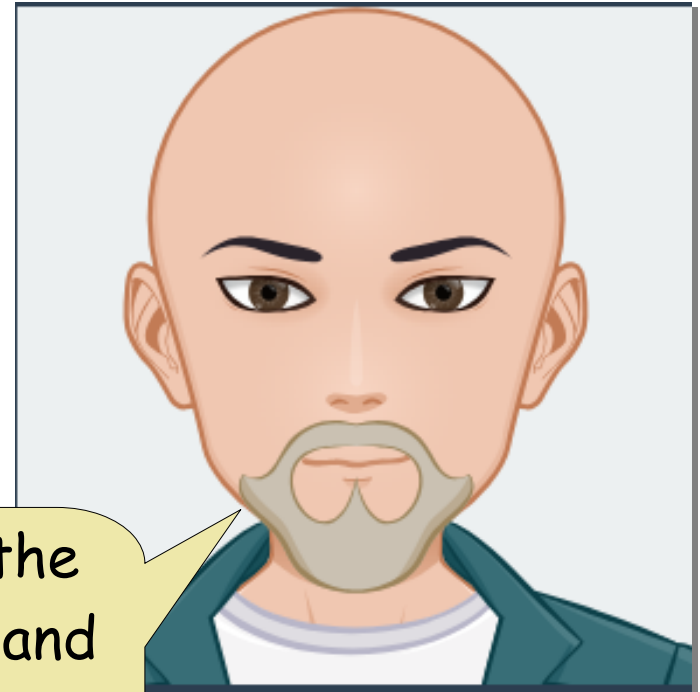


I don't think it's going to work, and I expect it to fail.

Two Years Later...



Thank you for
being open-minded
enough to at least
give the group a
chance



You moved the
needle here and
made things
suck less.

Side Note: Getting along

Rock
★
Search

emotional intelligence improvement

x



Outcomes & Wins

- Relationships were formed
- Knowledge & Expertise was shared
- Greater cross-team engagement
- Trends identified & discussed
- Successful workshops & conferences

Unexpected Outcomes

- A corporate communications person responsible for customer awareness is now working towards a cybersecurity career
- I actually flipped a pentester to becoming the technical resource in the Fraud Department

I was formally honored at work...



Parting Words

I'm a firm believer of "Defense in Depth".

Parting Words

I'm a firm believer of "Defense in Depth".

Beyond our standard practices, policies, controls,
and technology, I firmly believe...

Parting Words

I'm a firm believer of "Defense in Depth".

Beyond our standard practices, policies, controls, and technology, I firmly believe...

"People-in-Depth", working collaboratively together is our best path to genuinely drive continual improvements in our security programs.

Thank you for joining me on this



October 26, 2023



 <http://slides.dfirmatt.com>



Matt Scheurer