CRACKS IN THE FOUNDATION

. . . .OR


NO, YOU'RE
DOING IT
WRONG!

WHO ARE THESE CLOWNS?

Combined, your presenters have almost 40 years of Enterprise Operations, Support, and Security experience most major industries: Legal, Medical, Financial, Insurance, Manufacturing, & Technology (both inside and outside).

Joe Daw
Cybersecurity Architect
IBM

President Emeritus,
(ISC)2 CLE Chapter

CRob
Cat Herder
Red Hat Inc.

President,
(ISC)2 CLE Chapter

http://www.isc2chapter-cleveland.us/

BUT WAIT!

We've had years of experience managing internal teams, dealing with vendors, working with internal partners.

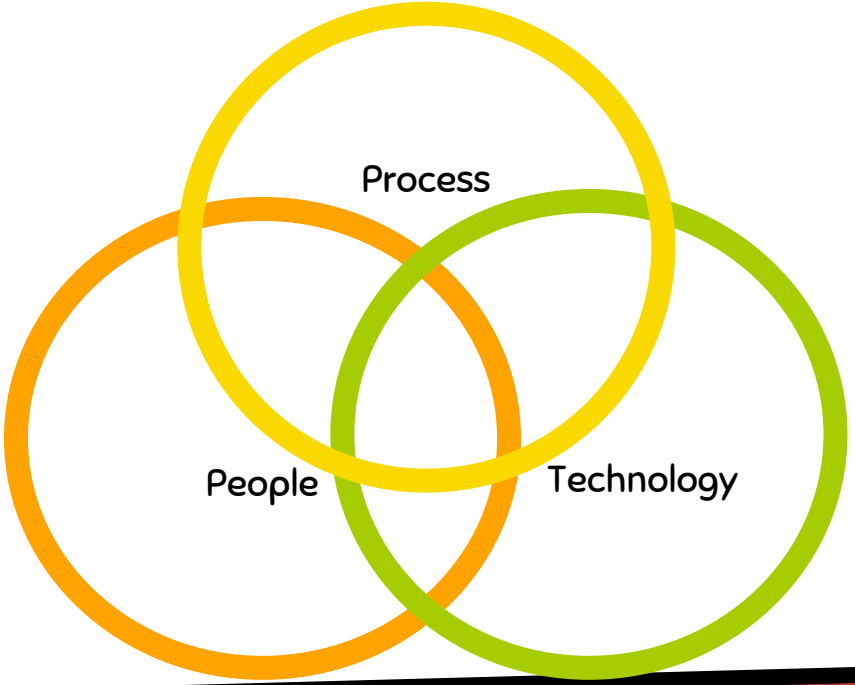
Currently we now work for major Technology Companies and we get to work with many Fortune <insert value between 1 & 1000> companies.

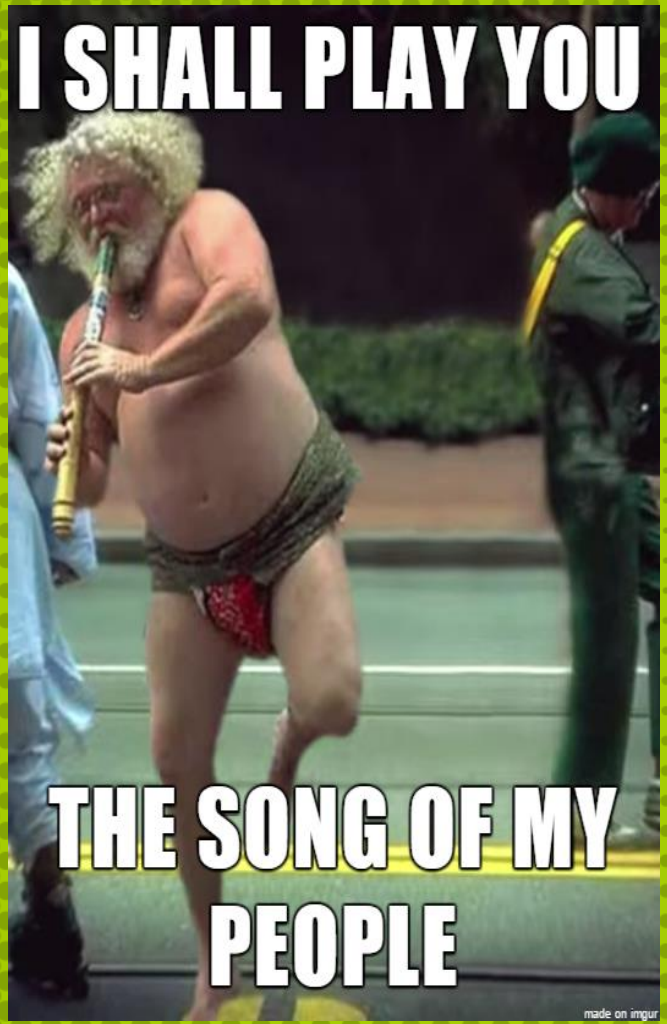
We're here to share some of the things we've observed and learned along the way.

FUNDAMENTAL ISSUES

No matter what the industry, the size of the team, or the technologies involved – there are certain almost universal patterns that emerge with InfoSec & Operations teams that most Organizations exhibit…..maybe you do too.

WHAT WILL MAKE YOU BETTER IS NOT NEW NEWS





1.

YOUR PEOPLE

Let's start with a few slow ones right over the plate.....

33% OF YOUR PROBLEMS ARE BECAUSE OF YOUR PEOPLE & YOUR ORG STRUCTURE

Silos

Every Org has them; The boundaries between them are vast, and are hurting you

Do you REALLY have the right skills to pay the bills?

It's great you've got that Win2K-certified engineer and all....

InfoSec's Interpersonal "Skills"

"Dr. No", "The Department of No"... InfoSec hasn't had the best track record partnering

POTENTIAL

NOT EVERYONE GETS TO BE AN ASTRONAUT WHEN THEY GROW UP.


NEXT TIME YOU RE AFRAID
TO SHARE IDEAS
REMEMBER SOMEONE
ONCE SAID IN A MEETING
LETS MAKE A FILM WITH A
TORNADO FULL OF SHARKS

The Internet of Things does not need

"*More Silo*"

"Security Superfriends"

- Engage critical business and technical stakeholders
- Convert them into your champions to multiply your message
- Cooperatively help build a plan for security that accounts for and includes their viewpoints.


Sell
Yourself
and security
always!

BIG CONCEPT

You are your Brand

Every Customer interaction either improves or detracts from that brand

2.

YOUR AWFUL PROCESSES

Just because you've always done it this way doesn't mean it's right.

YOUR PROCESS MEANS NOTHING IF YOU AREN'T FOLLOWING IT

Compliance is not Security
Move beyond the checklist, focus on the intention.

Incident Response Plans
There's a reason Boy Scouts are so awesome...Always Be Prepared.

Inflexible Process
Attackers and your Business Competitors don't care about your cool dashboard

WHERE exactly is your data?
Do you know what's talking to your critical systems? Do you understand how those systems really work?

PROCESSING…. FOR THE SAKE OF PROCESS

Legacy means more than just a mainframe; it's processes (and people) too.

Think in terms of the DEV phrase "technical debt"

Running the Department Like a Business

- Engage critical business and technical stakeholders
- Convert them into your champions to multiply your message
- Cooperatively help build a plan for security that accounts for and includes their viewpoints.
- Reward positive interactions with the team (awards, contests, recognition)

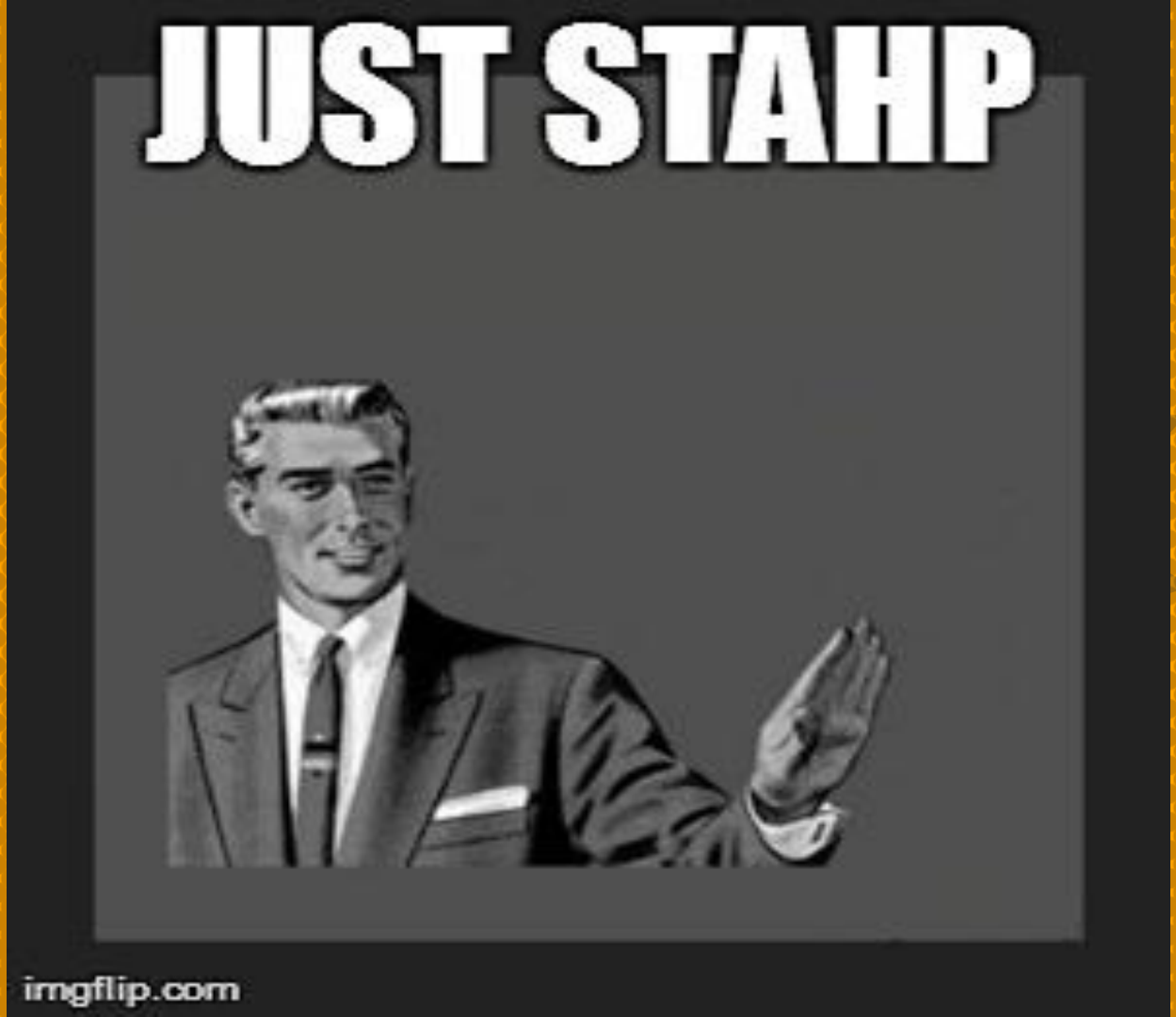
BIG CONCEPT

Sometimes you have to burn things to the ground before you can start to move forward again

3.

YOUR TECHNOLOGY

Why hasn't someone told you having 3 of the same thing isn't helping you if you can't even manage 1


JUST STAHP
imgflip.com

TECHNICALLY INCORRECT

Segmentation
How flat is your network? Y U NO SEGMENT?

Tools
Poorly/under-used tools, duplicate tools, tools focused on the wrong risks

Application/Server Documentation
Do you REALLY know how things work? IF you have this...how current is it?

Highway to Heck
Have a Security Roadmap? If you do, when did you update it last? If not....you better get up now and start researching one..

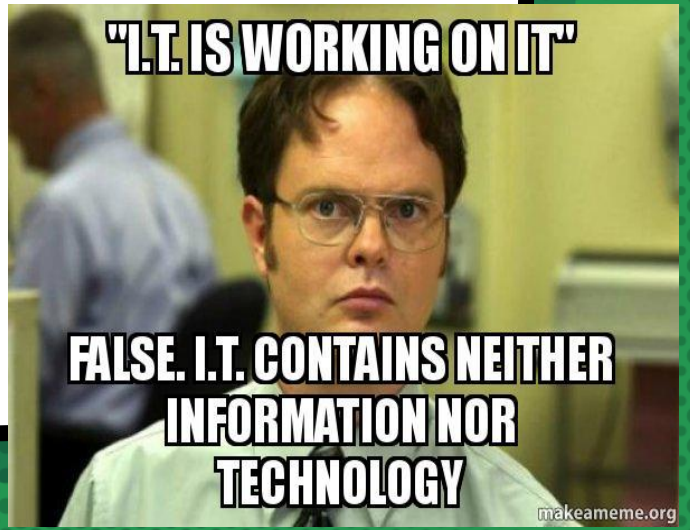
Automate the repeatable tasks, focus your talent on real problems

While that shiny new "next-gen" thing is cool and will solve all of your problems...

Do you even know where your data is, who is touching it, and where it's going?

Logs

Logs are a solved problem. Why are you still wrestling with them? Why aren't you doing them right?



KNOW THYSELF

- KNOW where the Business' MOST IMPORTANT data lives.
- KNOW how the MOST IMPORTANT Business systems work, communica
  accessed.
- Critically look at IT processes to remove inefficiencies and control gaps

INSANITY WOLF SAYS...

Focus on an area, mature yourself, move on to the next

BIG CONCEPT

Do a gap analysis to understand where your current technology excels and fails you. Then make RISK-based choices to change, augment, or replace selectively. Understand your Business' plans so you can help them achieve their goals.

LET'S REVIEW SOME CONCEPTS

Talent

Do your people have the right technical and interpersonal skills? How can you either help them get those or find new ones that can get the Business where it needs to be?

Processes

Chances are REALLY good that your current processes suck. Look at rebuilding them and integrating "DevOps" wherever possible to allow fastest response and agility

Eliminate Tribal Knowledge

Document critical systems, plan & test for failures, KNOW where your data is and how it is used.

Org Structure

Is your team aligned correctly with Business and Operations? Can you name your company;s top 3 Business objectives and describe how you're supporting achieving them?

Compliance is NOT Security

Just having the box checked will NOT stop an attacker. Look at the real intention of the guidance and strive to protect what it is overseeing.

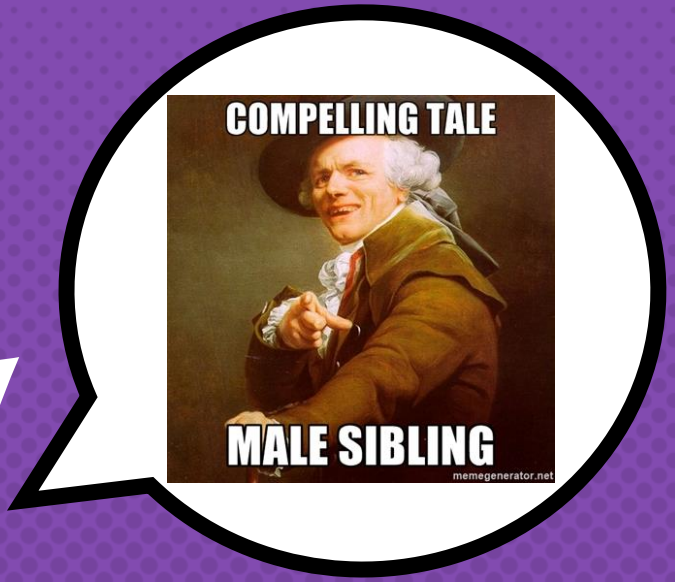
Roadmap

Take the time to understand the Business' plans and develop an agile, multi-year plan. Build a consensus of key stakeholders to develop and "sell" the plan. Be prepared to adjust parts of that plan annually.

CRob and Joe are vendors

All vendors should be awesome like Joe and CRob!

THANKS!



Any questions?

Joe@daw.org or whatever

CRob@RedHat.com
@RedHatCRob