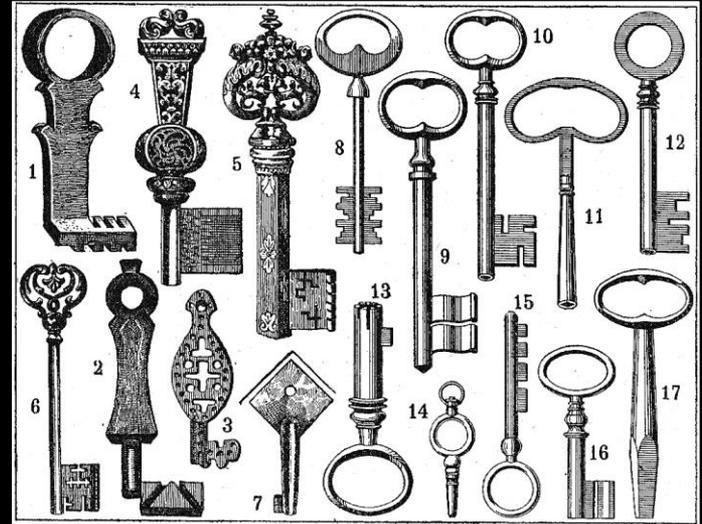


Keys to Employee Cybersecurity



Al Lewis, CISSP-ISSMP, CISM

FISSEA Annual Conference
March 25, 2015
NIST HQ, Gaithersburg, MD

“Tell me... and I forget.
Teach me... and I may remember.
Involve me... and I learn.”



**BEN
FRANKLIN**

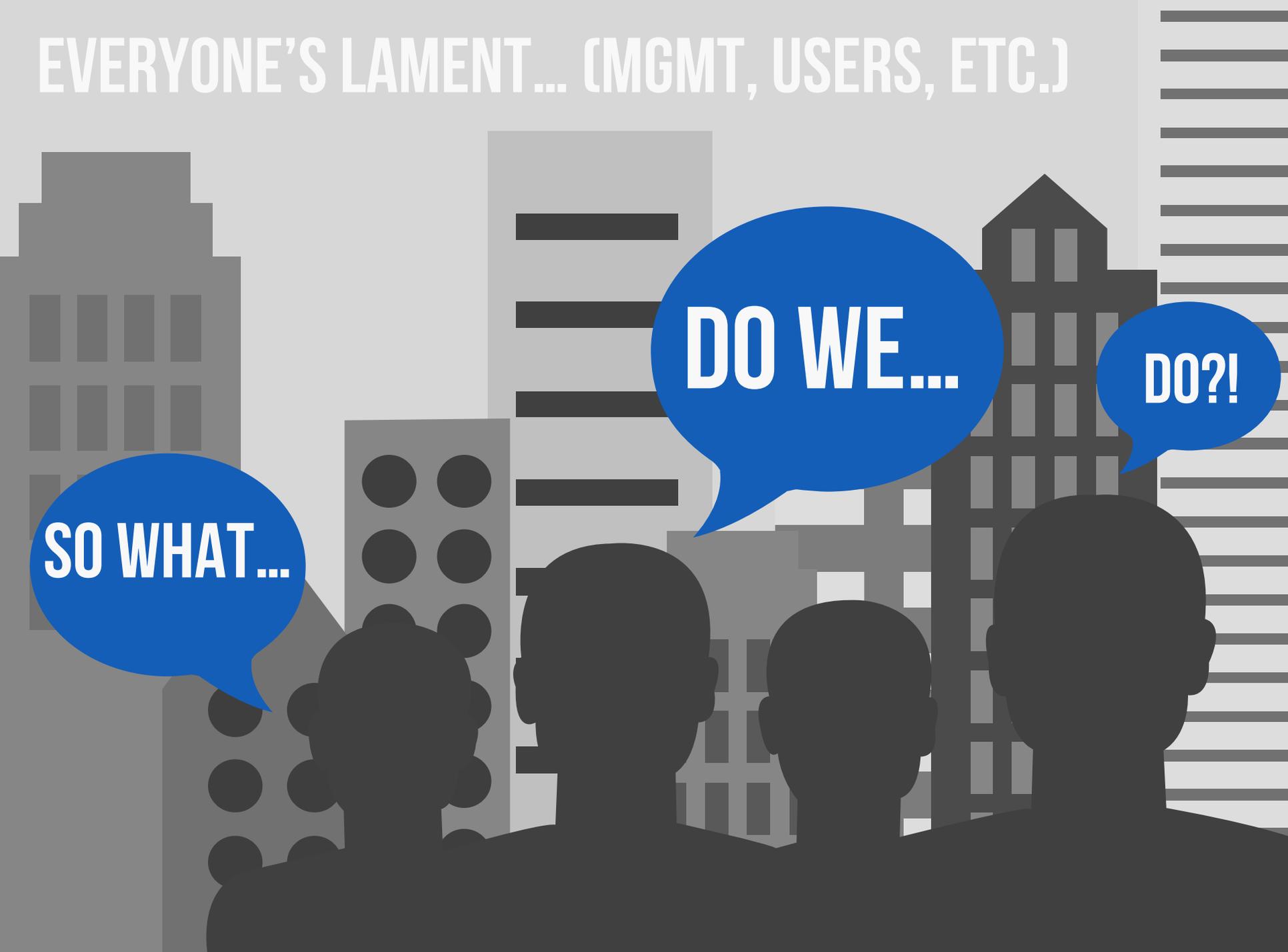
MY TALK IS ABOUT...

- **Technology has changed, but people have not inherently changed (much)**
- **User behavior has adapted to meet technology... but not always in a good way**

MY TALK IS ABOUT...

- Security has not evolved rapidly enough to keep up with:
 - Increasing plethora of threats
 - Burgeoning compliance requirements
- Compliance and security – two different animals

EVERYONE'S LAMENT... (MGMT, USERS, ETC.)

The image features a stylized cityscape background with various grey buildings of different heights and shapes. In the foreground, there are four dark grey silhouettes of people's heads and shoulders, facing right. Three blue speech bubbles are positioned above the silhouettes, each containing white text. The first speech bubble is above the leftmost silhouette, the second is above the second silhouette, and the third is above the rightmost silhouette. The overall color palette is muted, consisting of greys, blues, and whites.

SO WHAT...

DO WE...

DO?!

MY TALK IS ABOUT...

Never lose sight of the importance of people in the security equation

- **Educated, informed, engaged users**
= Reduced probability of attack
= Reduced risk

MY TALK IS ABOUT...

- Fully utilizing technology to educate and involve users on cyber awareness
- Educating, informing, and training your users is a worthwhile effort – and worthy of increased funding
- Our job is to educate everyone on the importance of our field – not just content

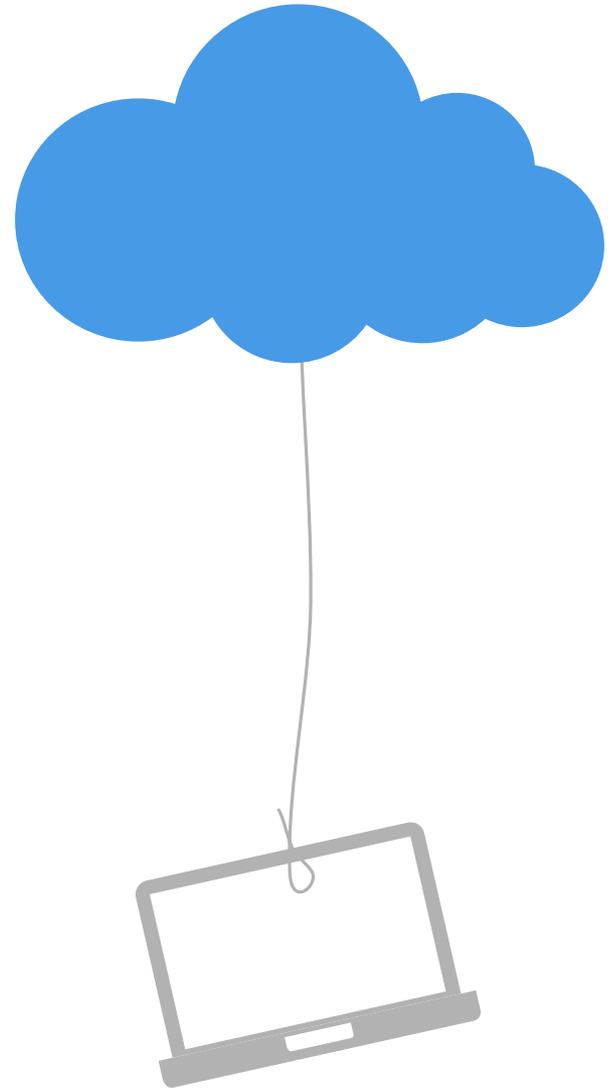
WHO AM I?



- 28 years in federal and commercial IT
- 15 years in cyber security operations, program management, policy and compliance
- Companies: HP, MITRE, many medium and small firms
- Former Clients: DoD, FBI, HHS, DOL, Supreme Court, EPA, CMS, etc.
- Member FISSEA board
- I like technology AND I like working to help people understand the role people play in designing it... developing it...using it...and abusing it

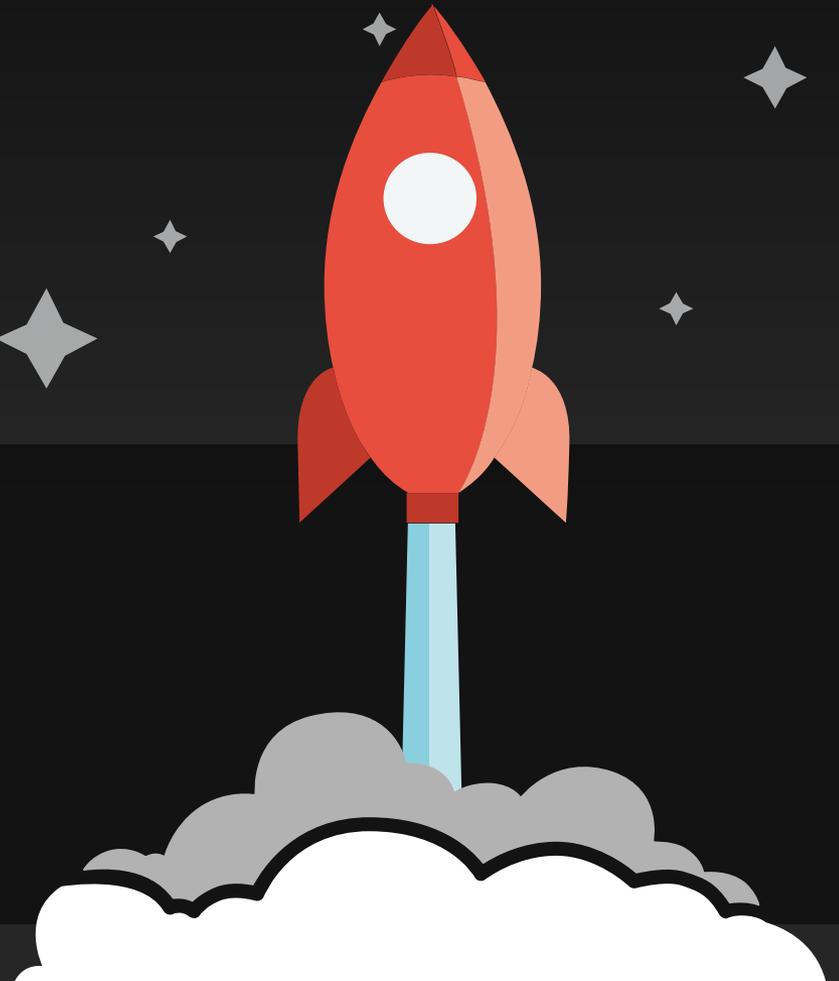
THREATS ARE INCREASING

- APT
- Crimeware
- Hackers
- Theft (physical and virtual)
- Domestic and international
- Higher probability of attack

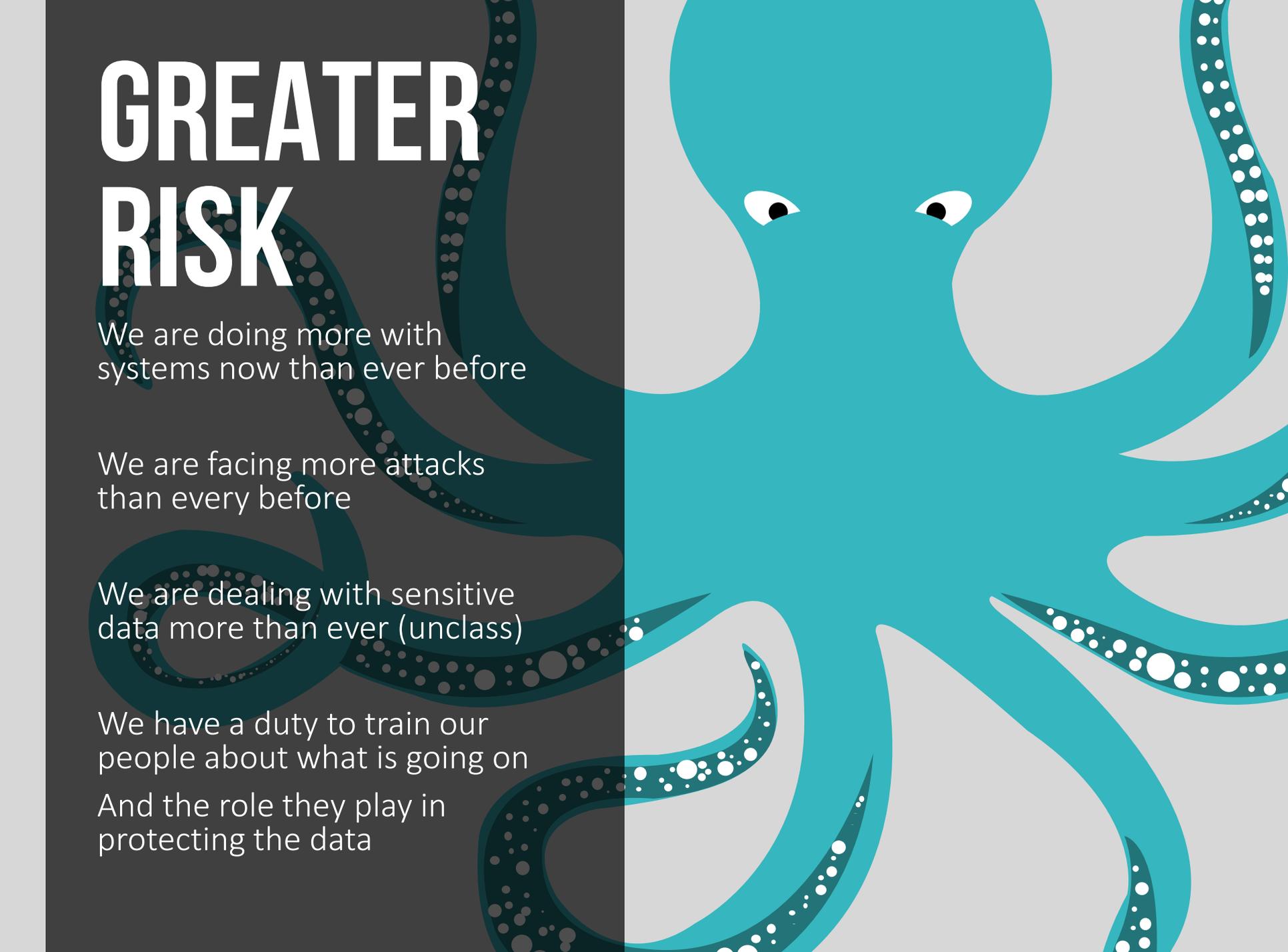


BIGGER IMPACTS

- Sensitive Data, UCTI, CUI, ePHI
- New regulations, new compliance picture



GREATER RISK



We are doing more with systems now than ever before

We are facing more attacks than every before

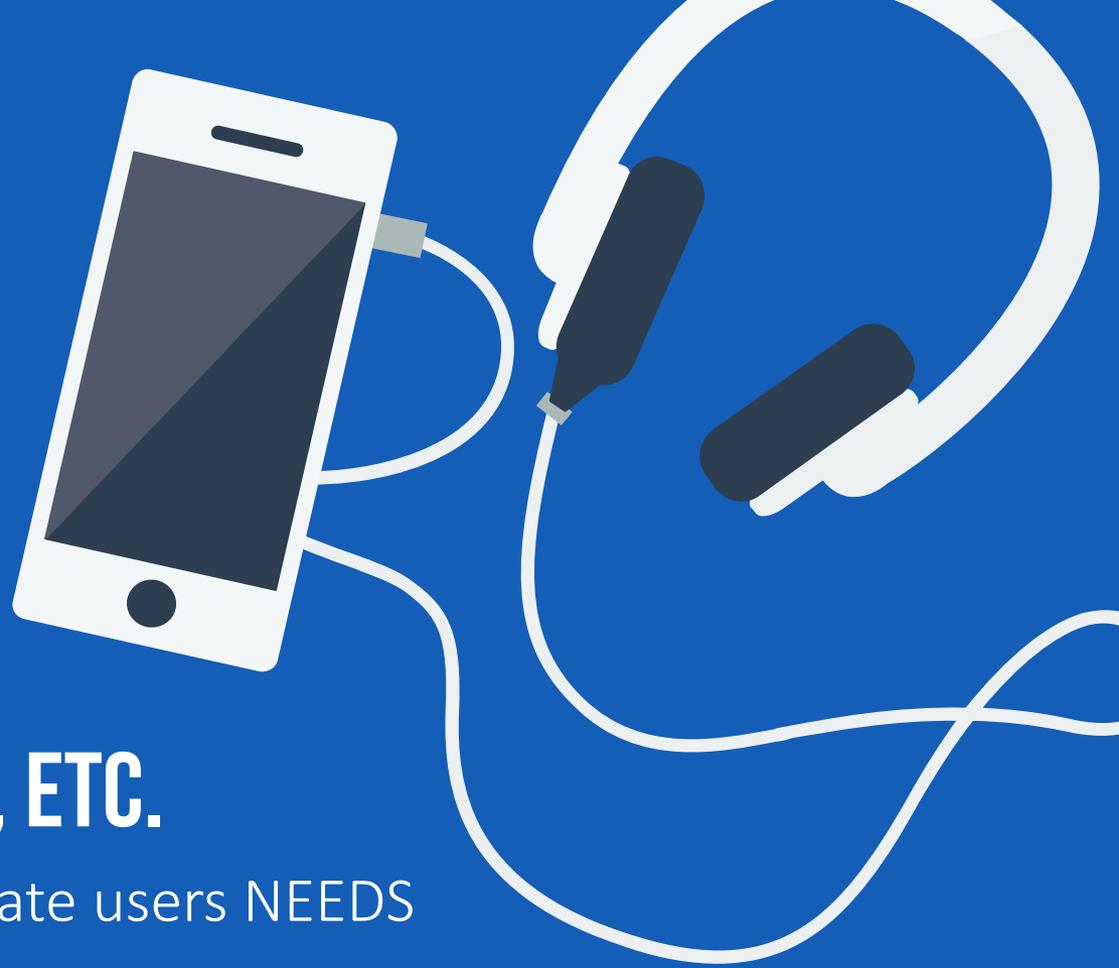
We are dealing with sensitive data more than ever (unclass)

We have a duty to train our people about what is going on
And the role they play in protecting the data

THE OLDEN DAYS

Technology has changed a lot over the last 28 years...
but people have not changed very much....
Still want to take the shortest route to get their job done....
But now they also expect to use work PCs as they do at home...





SOCIAL MEDIA, BYOD, ETC.

- How do we accommodate users NEEDS (WANTS) while accomplishing our Federal missions?
- We need to employ smarter technologies
- Also educate our users about the potential risks inherent in using new technologies

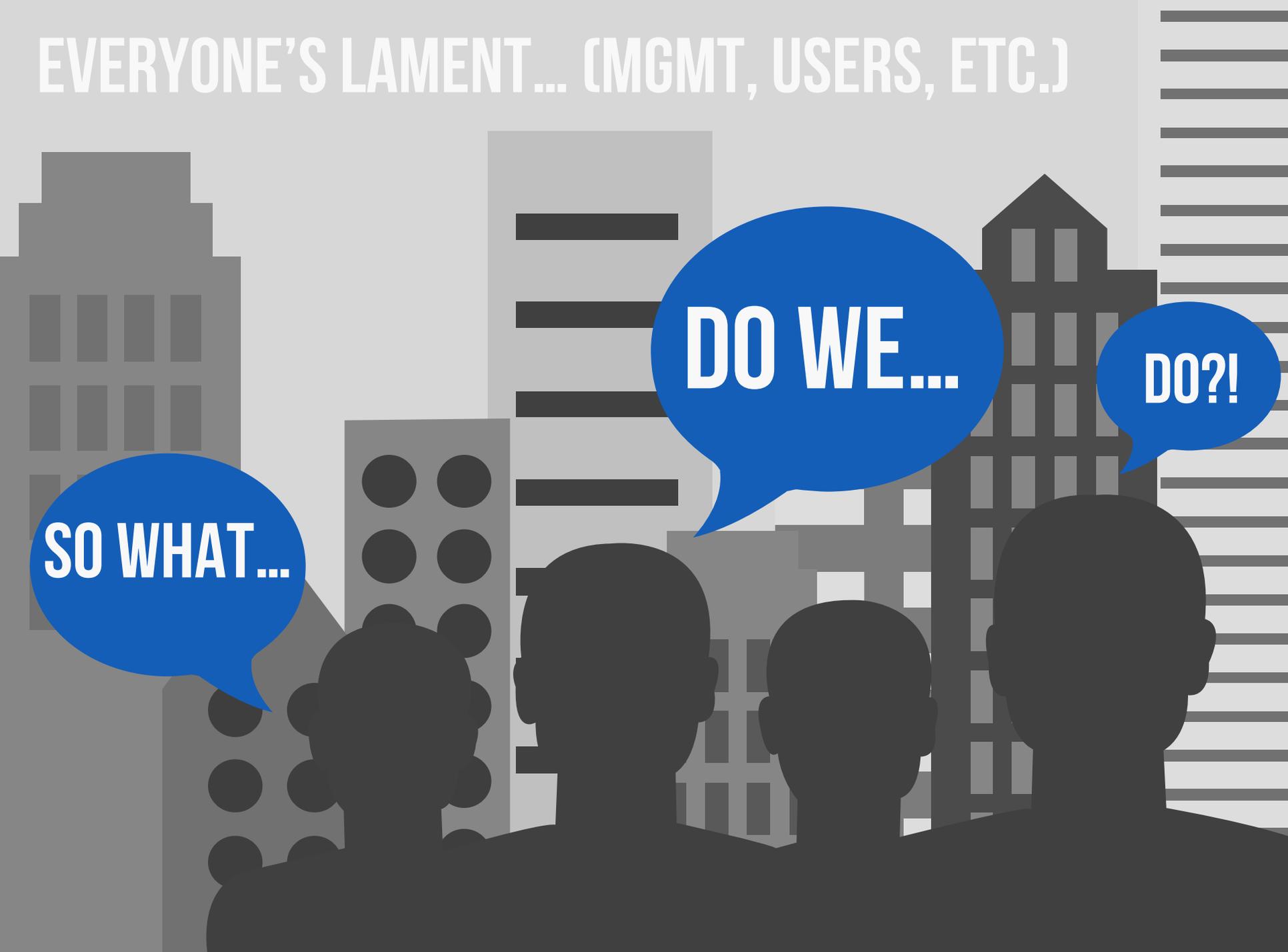
I CAN'T GET NO SATISFACTION

Who are we aiming to please:

- Mission requirements
- User wants
- Compliance mandates



EVERYONE'S LAMENT... (MGMT, USERS, ETC.)

The image features a stylized cityscape background with various grey buildings of different heights and window patterns. In the foreground, the dark silhouettes of four people are shown from the chest up, facing right. Three blue speech bubbles are positioned above them, containing white text. The first bubble is above the leftmost person, the second is above the middle person, and the third is above the rightmost person.

SO WHAT...

DO WE...

DO?!

COMMUNICATION IS KEY

- At all levels
- Is your security training education, and awareness a means to an end...what end?
- Better security? Or to lessen risk of non-compliance...or both?



COMMUNICATION IS KEY

- How often do you train?
- How often do you find people out of compliance – signal that more training is needed



AVOID GETTING CAUGHT

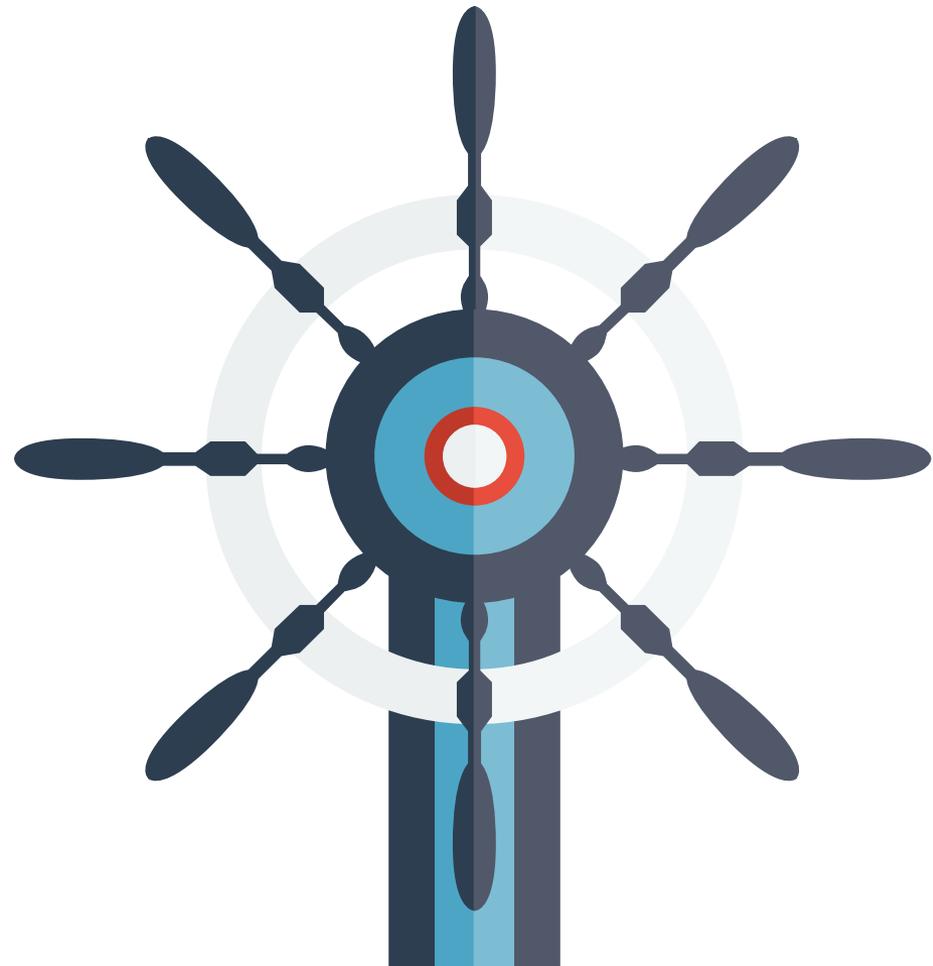
The background is a solid teal color. It features several small, stylized fish icons in a darker teal shade, scattered across the page. A large, stylized orange fish is positioned in the lower right quadrant, facing right. A white dashed line runs vertically along the right edge of the page, ending in a small white circle. A white curved line starts from the bottom of this circle and curves back towards the large orange fish, resembling a hook or a path.

With an inadequate strategy for user awareness

- Policy is not enough
- Compliance program is not enough
- Awareness needs to be constant because risks are constant

LEAD

- The Educator is often the first-level contact with all users
- This represents a lot of **POWER!**
- If you know your users – AND you know your threats and risks – then you can lead the BoX with initiatives
- What are the targeted training, education, and awareness initiatives that matter most?
Why?



GUIDE

A stylized illustration of a red lighthouse on a rocky island. The lighthouse has a red cylindrical body with a small square window, a white balcony with a railing, and a red domed top with a glass lantern room. The background features a light gray sky with white clouds and three black birds in flight. The foreground shows a blue sea and dark gray rocks.

...your leadership with targeted training initiatives tied specific threats that exist in your organization

...your users with Insider Threat, Cloud Security, Risk Assessment, and other user engagement activities to enhance cyber security awareness

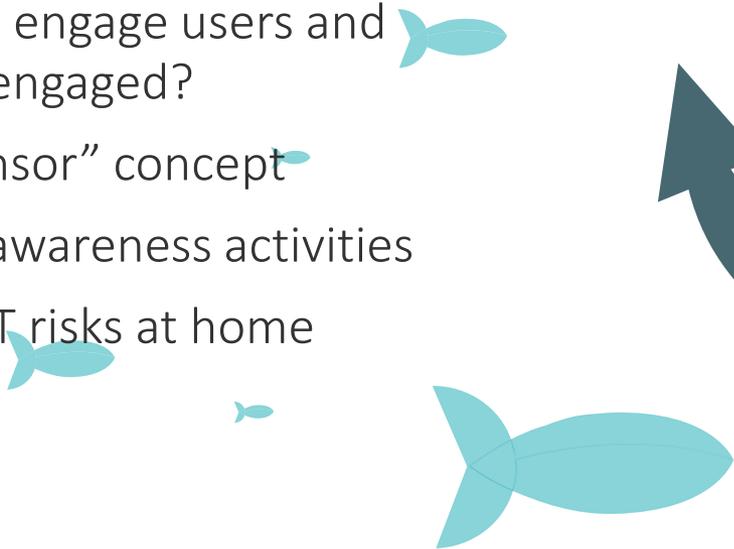


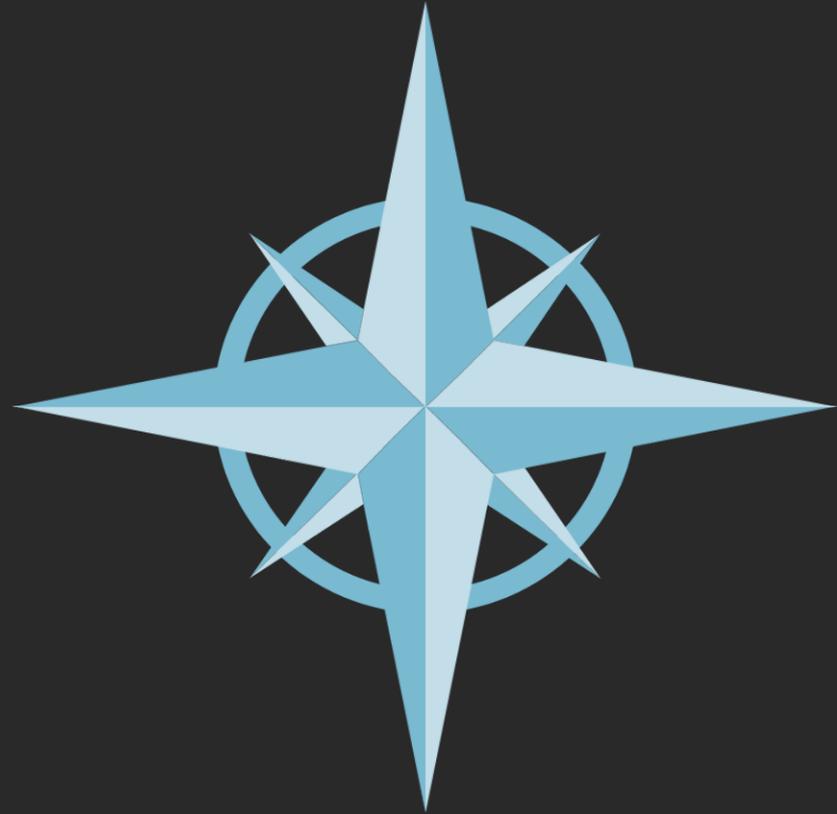
HELP VS. PUNISH?

- Is your compliance program all about sanctions?
- Is there an emphasis on ensuring people better understand policy up front? When it is published? Do you monitor your waiver volume as an indicator of policy effectiveness?

AWARENESS AS AN ANCHOR

- How do you engage users and keep them engaged?
- “Human sensor” concept
- Interactive awareness activities
- Talk about IT risks at home





FOCUS

Security educators need to understand risks that face their organization –

- Probability of compromise
- Impact
- Mitigations

ONE WAY?

There is no single solution to employee education because

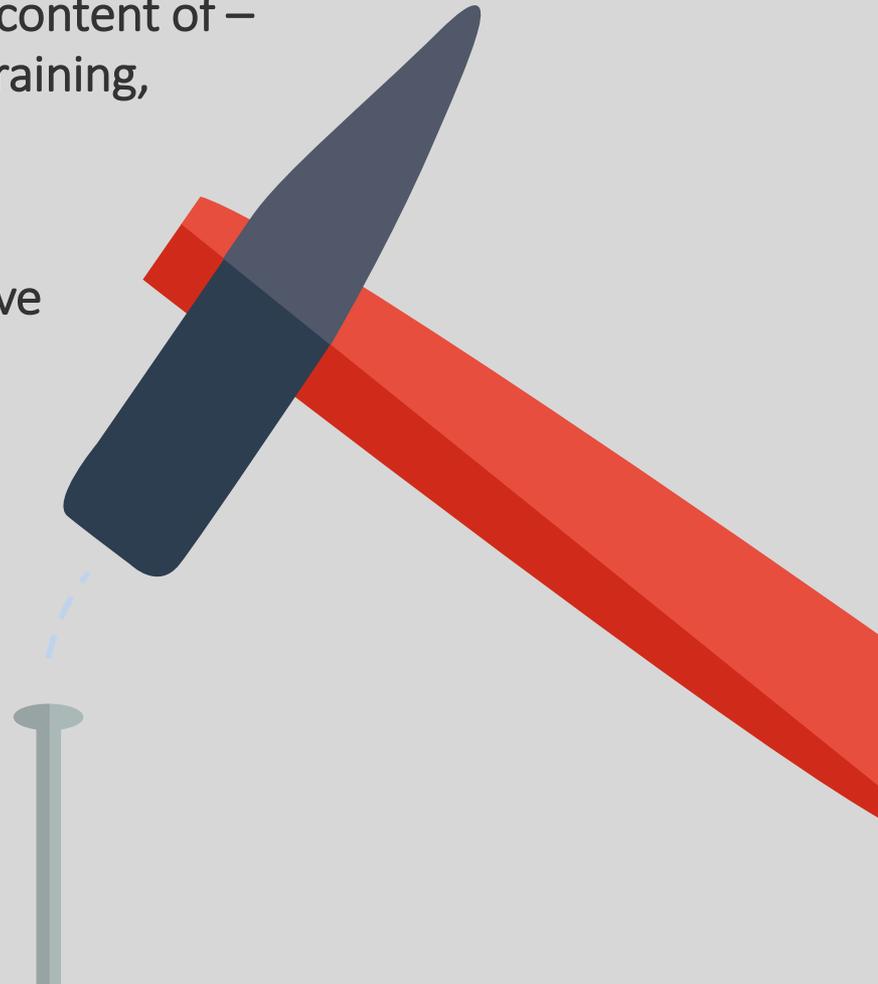
Every organization is different

- Every employee is different
- Risk appetite
- Budgets



HAMMER TIME

- When is the last time you revisited the content of – and revised – your security education, training, and awareness programs?
- Does delivery technology delivery involve interaction... or just pushing buttons?
- Compliance oriented (therefore may be boring) or security oriented (more exciting) or a combination?



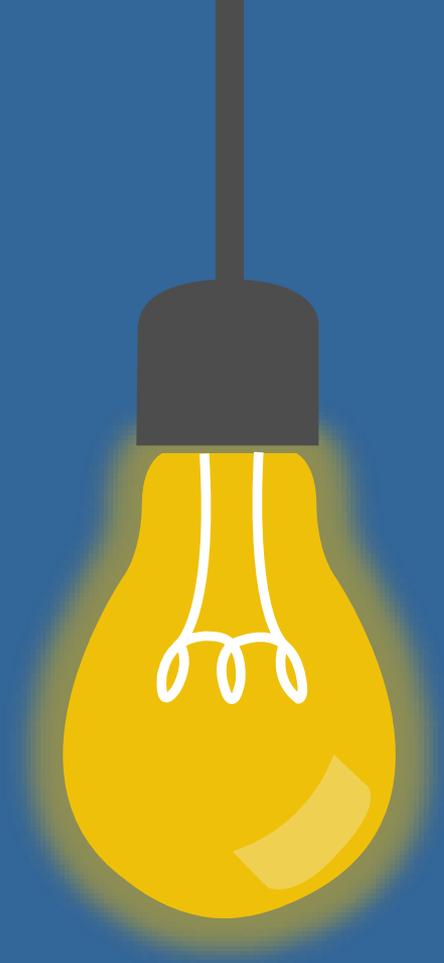
MEASURE

- How do you measure success with your security education, training, and awareness programs?
- Are your initiatives tied into a GRC tool?
- Do you encourage and log employee feedback?
- Do you review incidents and tie the data back to informing your users?



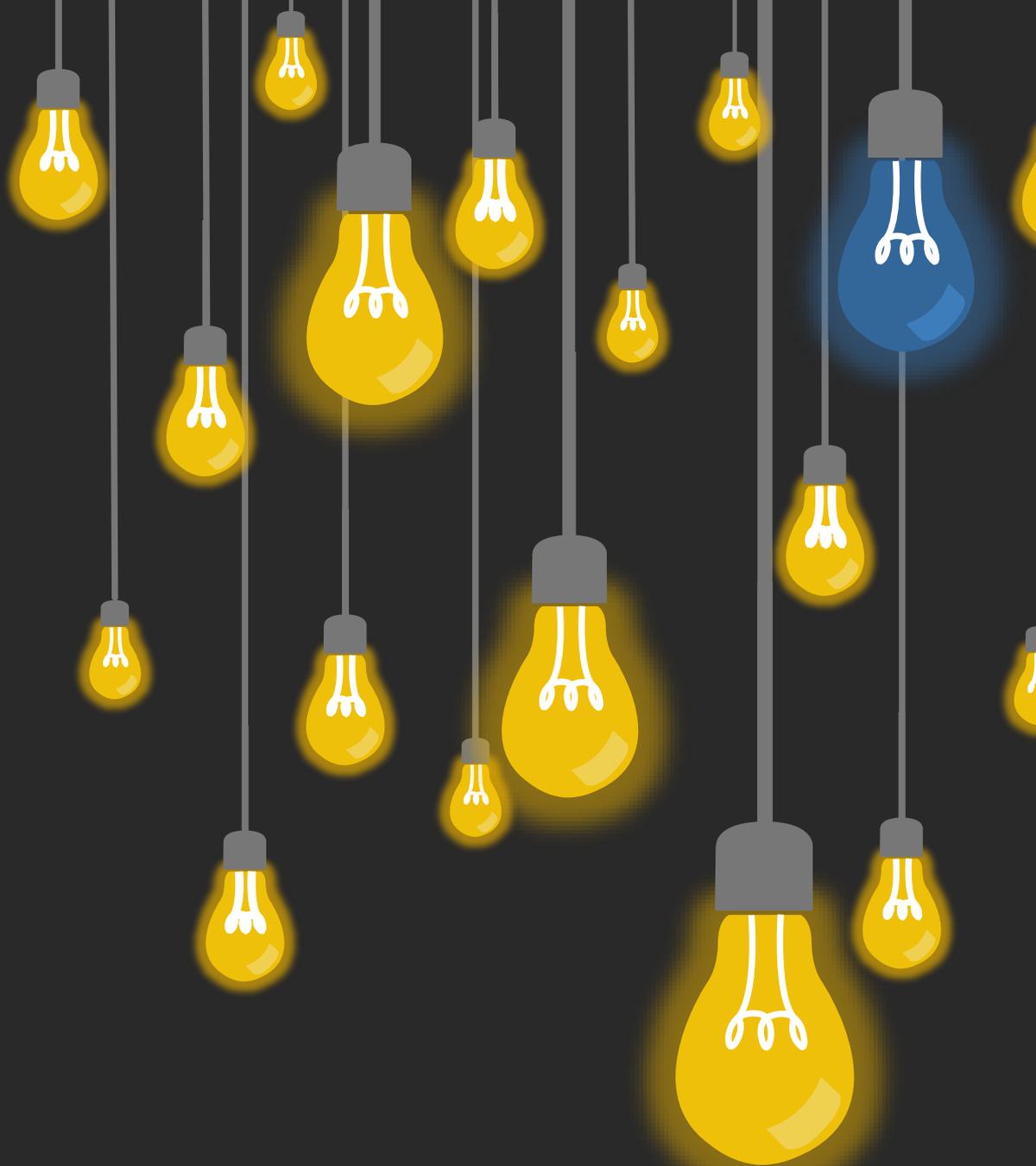
POWER OF MIND

- The reason why FISSEA exists is to support you – the Federal IT security educator
- This conference offers an opportunity to get new ideas and introduce them into your organizations



MORE IDEAS

By sharing your ideas with others – and learning from others – you can leverage the power of your network to solve your problems



EVERYONE

WINS

...when the entire organization is aware
and committed to safeguarding data and
systems

How do you obtain that
commitment?



ECONOMIZE

- Everyone needs to do more with less
- Which activities will provide the biggest bang for the buck?



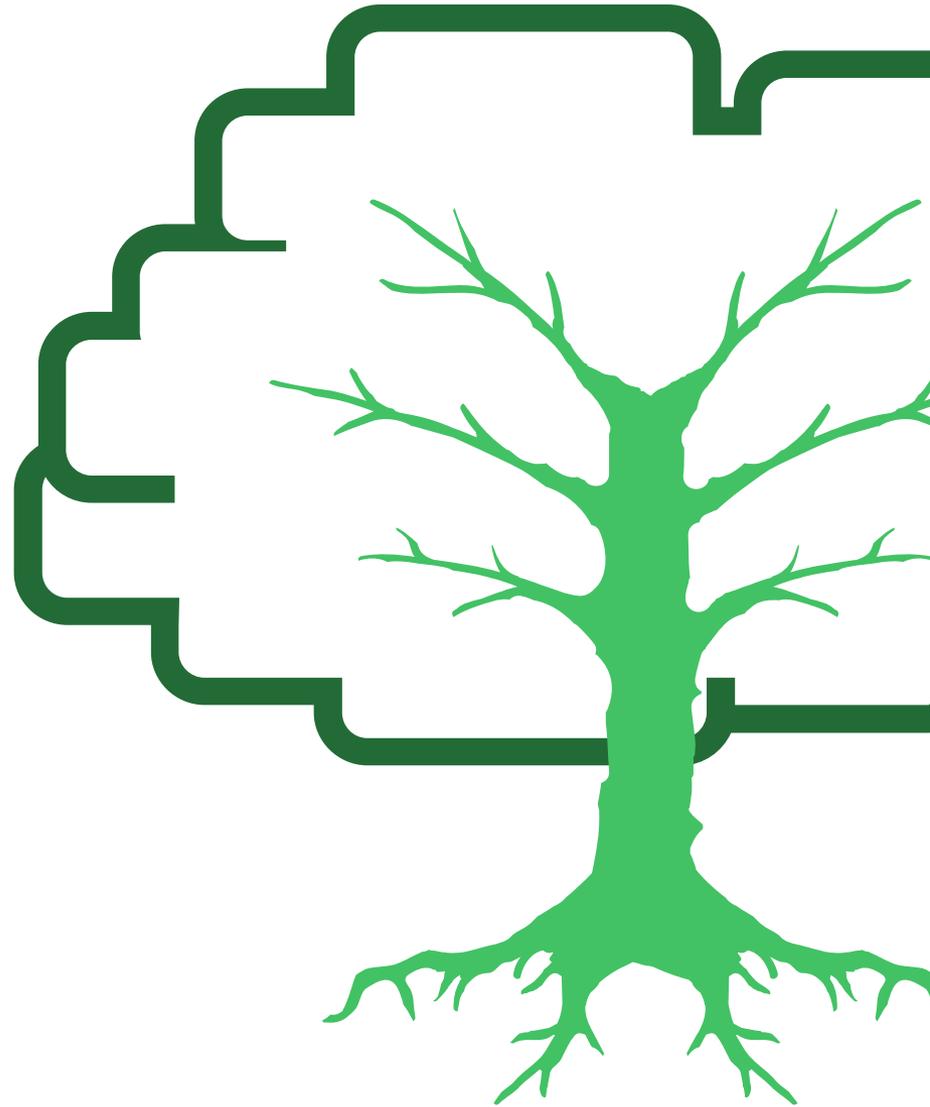
FOCUS ON VALUE

- Proving ROI is difficult at best
- Link activities to biggest threats facing your organization



ROOT CAUSES

- Many cyber incidents are caused by lack of awareness, or insider issues:
 - Phishing
 - Intentional and non-intentional non-compliance
- People are at the root of many problems with security

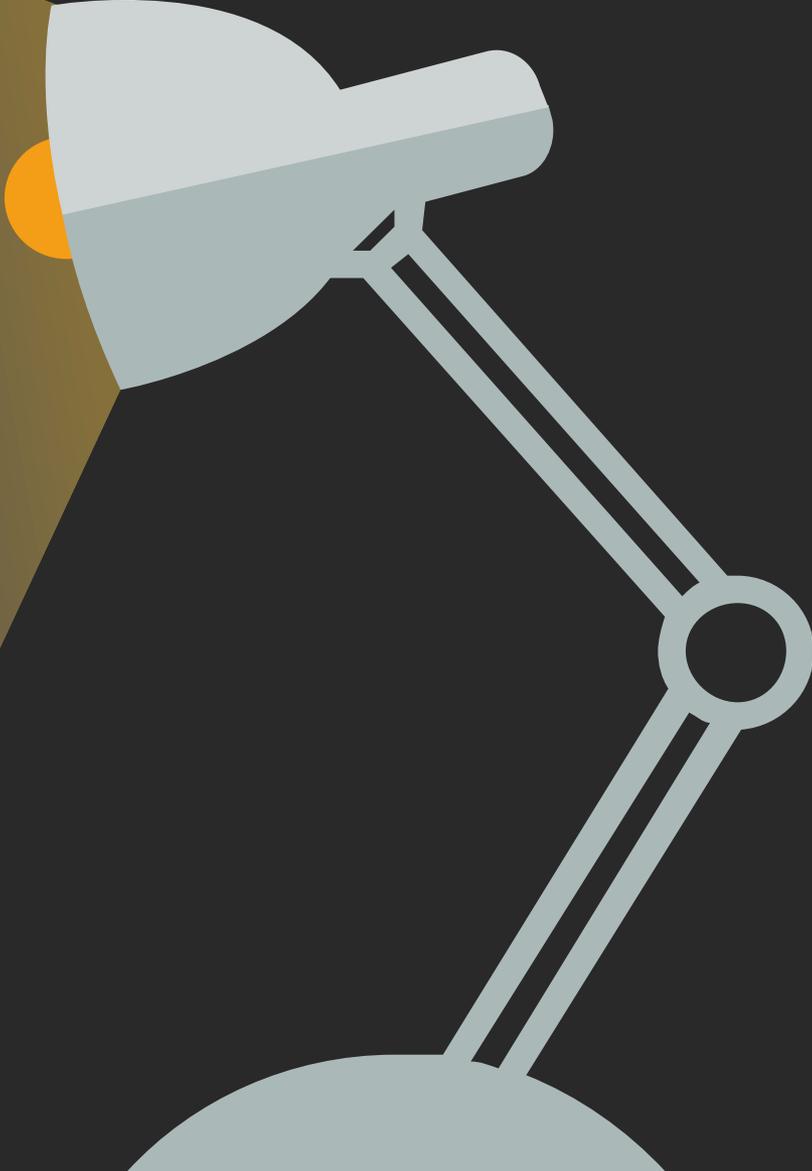


STRENGTHEN YOUR PEOPLE

- Arm them with the tools they need to face the challenges they will encounter
- Engage them fully



ENLIGHTEN



Everyone....

- Executives
- Managers
- Employees
- Contractors
- Vendors

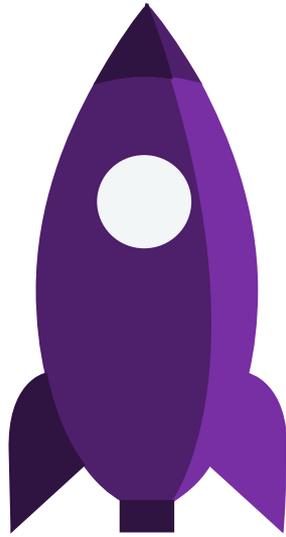
- Wherever a threat vector resides
- Wherever funding comes from

HAVE FUN!

This work can be fun when done properly!

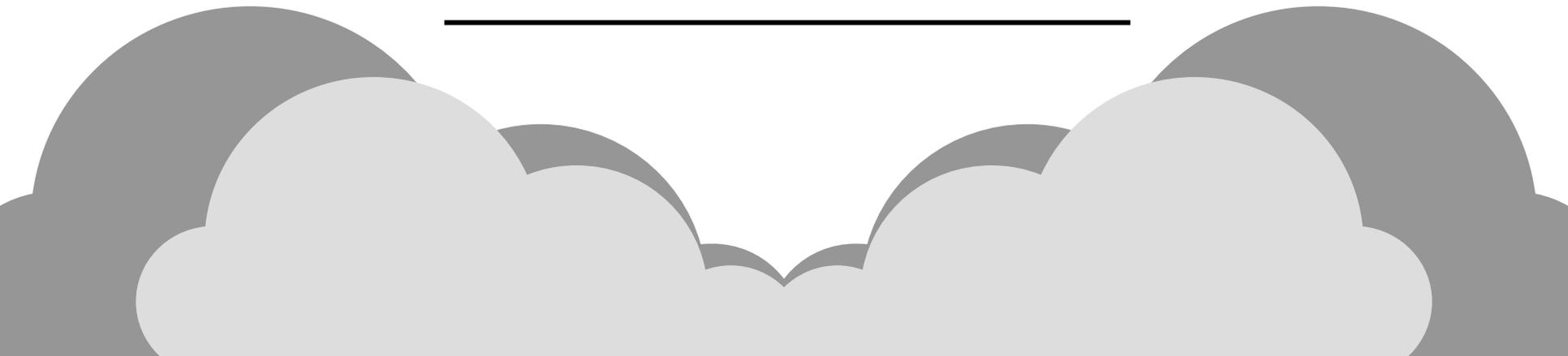
Your work can have a tremendous impact on the security of your organization.





The Sky Is

THE LIMIT!



THANK YOU

