



Security Awareness & Creating a Culture of Cyber Resilience

Executive Perspective on Cybersecurity Awareness

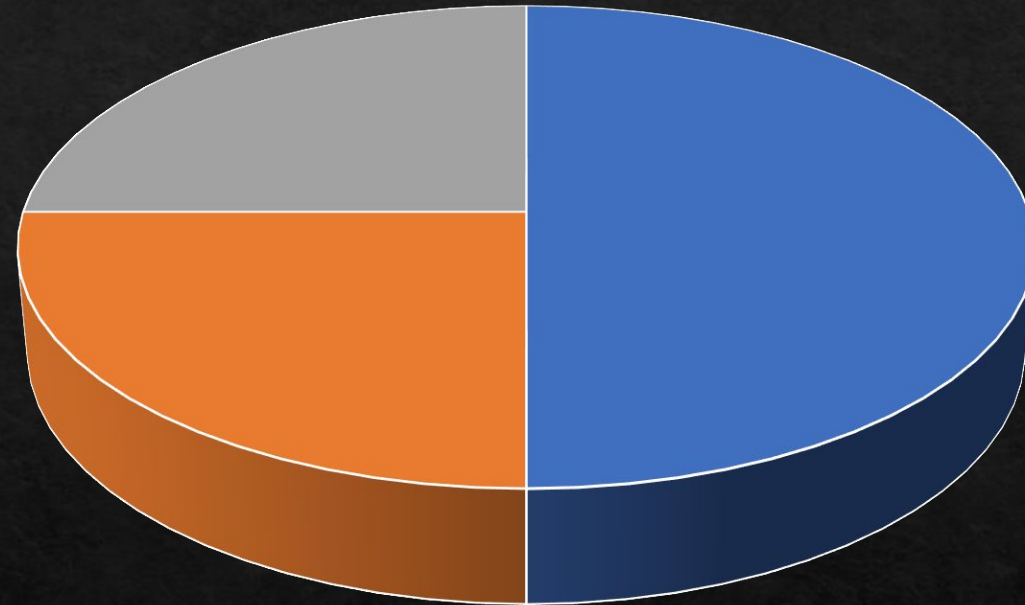
- ❖ A review of recent surveys with dozens of organizational leaders regarding security awareness - covering a variety of topics including what works, what doesn't, what is needed, what is the perceived risk, what is their exposure, and what are the potential gains
- ❖ Participants

Title	Industry	Organization Size
IT Director	IT Consulting	Small Medium
Chief Technology Officer	Managed Services	Large
Chief Info Officer	Healthcare	International
Chief Info Security Officer	Manufacturing Audit	
VP Business Development	Banking	
Chief Privacy Officer		

How confident are you that adequate protections are in place to prevent cyber breaches?

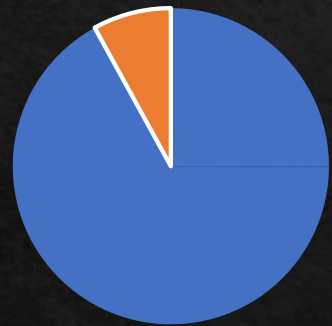
Quotes & Notes

- ❖ Bad guys are ahead of the curve
- ❖ Too much complexity
- ❖ Lack of organizational willingness to support program or spend appropriate funds

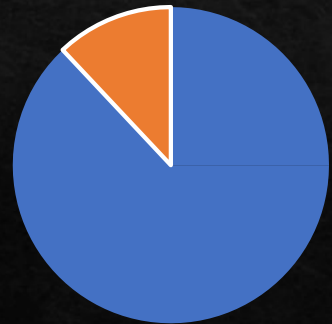


■ Hig
■ Med ■ Low
h

What is the opportunity to improve?



9.2% - 'People' component was improvable.



8.8% - 'People' component had the biggest opportunity for improvement.

Quotes & Notes

- ❖ All can be improved
- ❖ Process and People are the hardest to improve
- ❖ People component has the largest potential for improvement

Regarding Awareness: Describe your Culture

Quotes & Notes

- 
- NO TIME
 - UNNECESSARY
 - LACKING SUPPORT
 - NOT UNDERSTANDING RISK
 - NOT UNDERSTANDING VALUE
 - NO VISIBILITY

- ❖ Executive support is required
- ❖ Executive support is unseen
- ❖ Expecting an easy and immediate fix
- ❖ Visible metrics needed
- ❖ Management not allocating time
- ❖ User not allocating time
- ❖ Users sees self as not needed awareness (lawyers, doctors, execs)
- ❖ Business do not understand risk
- ❖ Businesses not understand layered security

Regarding Awareness: Describe your Users

Quotes & Notes

- 
- NO USER IMPACT
 - OVERCONFIDENCE
 - LACKING ATTENTION
 - IT ISSUE
 - LACKING MINDFULNESS
 - NOT MY RESPONSIBILITY

- ❖ Users feel not their responsibility
- ❖ More in tune in personal lives, due to direct impact
- ❖ Not appreciate threat
- ❖ IT Issue
- ❖ Overwhelmed
- ❖ Varied sophistication
- ❖ Difficult to convert user with bad habits
- ❖ Will never reach 100% awareness

Contrast someone who is secure aware versus someone who is not secure aware.

Bad Bob

Not paying attention

Goes through the motions

Clicks with no discretion

“Loose Lips.” Does not adhere to policy.

Utilizes shadow IT.

Not their problem

Doesn't get it. Older.



Contrast someone who is secure aware versus someone who is not secure aware.

Good Bob

Mindful, thoughtful

Takes message to heart

Conscious of decisions. On top of personal finance.

Utilizes password complexity. Secures own device.

Cares

Empowered. Accepts responsibility.

Contacts help desk

Aware. Knows the value of data.

Digital Native



What is the Value Proposition for Awareness

Value Prop

Can positively impact incident response

Reduced risk

Benefit users 24/7

Cut costs to cyber insurance policy


Partnership can strengthen complementary programs

Reduce false positives

Reduce costs



Painting a Picture



Picture

Not aim for 100%

Want users contributing to success of cyber security

Mindful, engaged, empowered, literate

Program must discuss both desired and undesired behavior.

Don't aim for "business hours" awareness

Risk Based

Know your users and culture

Know what Good Bob looks like for your org