

CISO, Your Communications Program  
defines the company **Security Culture**  
( & adoption)



Don't **over-engineer** your  
messages.

# There's more than just the Calendar & Plan...

→ We need templates and  
principles for the 'ad-hoc'

# General Principles to Consider for Communications

Lead with value or business driver

## Planned Change

- If it impacts end users, we tell them first
- If we are transitioning technology, we generally allow for some duplicative time to avoid operational impact
- Avoid mentioning the software by name, better to discuss the functionality
- Always consider the most difficult user groups and the 'easiest' user groups
- Pilot the change and collect feedback within Security first

## Something Happened

- The Incident Commander is empowered to communicate to executive leaders
- Updates occur on a fixed schedule and include the next planned update
- Out of bands communication process is defined and engaged and tested regularly

# CISO Comms Basics

Boil down to these  
*(for now)*



1

## Something is Changing

1. Establish principles around change comms
2. Consider whether it impacts end users
3. Training
4. Stakeholder Considerations
5. Messaging (Format, timing)

2

## Something Happened

1. The notifications include: Executive, triage, client, impacted users, regulatory
2. There are various messages and they include: initial observation, remediation, post-incident

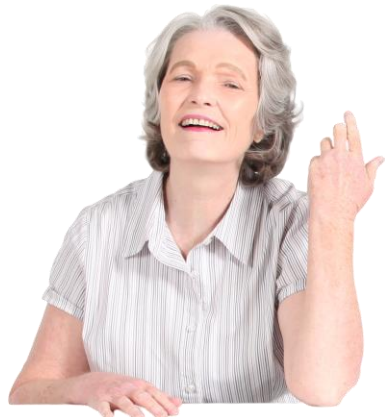
3

## Executive Updates

1. Bi-weekly CISO Update (Risk update)
2. Monthly Program Update
3. Tech & Information Risk Committee

# Maintaining the Comms Program

Don't over-engineer it, but it's not a one and done



1

## Create Annually

Created during the annual strategic planning activities to consider the initiatives, training and employee engagement plans

2

## Review Monthly

With the CISO as part of the Office of the CISO coordination

3

## Owned by the Office of the CISO

CISO Program Manager

Shared with the CISO leadership team

Shared with CISO communications functions

Coordinated with other technology communication pipelines