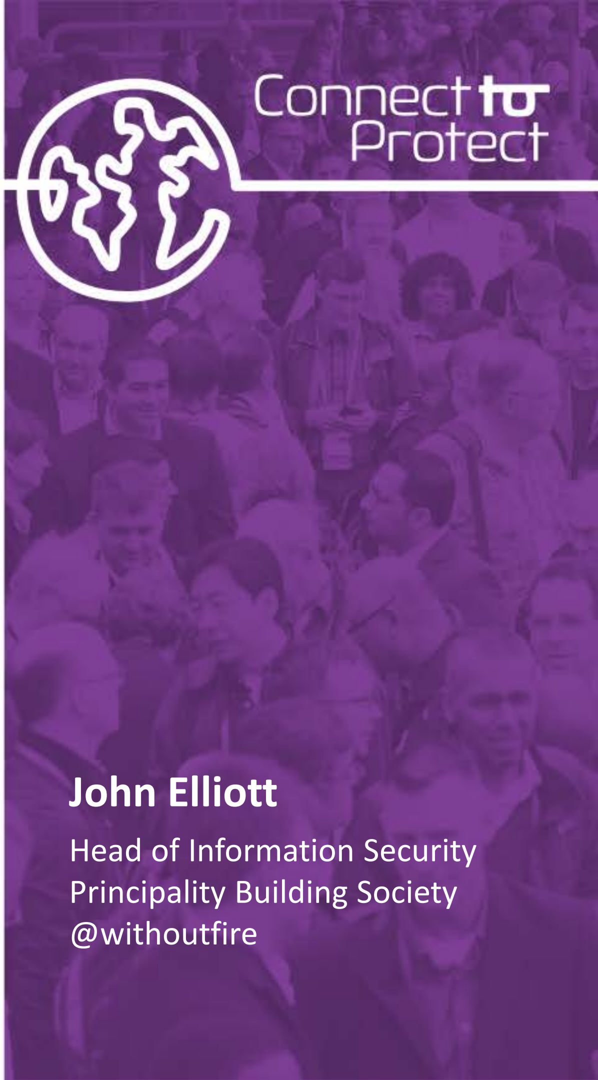
RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



SESSION ID: PROF-M04

# How to Explain Cyber Security to the Board Using a Simple Metaphor: FIRE

**John Elliott**

Head of Information Security
Principality Building Society
@withoutfire

#RSAC

# Why?

Smart people

Time limited

Non-technical

- Talking to the C-suite or the board is  brilliant

Smart people

Get risk

Perspective

**Who grasp concepts quickly and can apply them to the current situation**

Smart people

Time limited

Non-technical

But we’ve spent $x million over the past *n* years making sure this won’t happen to us …

What do you mean by INAMOIBW!

# Why do we have fire extinguishers?

Smart people

Get risk

Perspective

**Who grasp concepts quickly and can apply them to the current situation**

# Everyone has a good sense about fire

ouch

# Everyone has a good sense about fire

drill

# Everyone has a good sense about fire

**not a toy**

# Everyone has a good sense about fire

tell a teacher

# Everyone has a good sense about fire

also not toys

# Everyone has a good sense about fire

strict

rules

# What’s this got to do with cyber security?

> ***“there’s no such thing as common sense,***
> ***just common knowledge”***

**Ira Winkler, RSA Conference 2012**

***"our metaphors comprise the conceptual spectacles through which we view the world"***

**Immanuel Kant, Critique of Pure Reason 1781**

# Why is fire a great metaphor?

- Societal knowledge
- Fire is an **opportunistic threat**
- Fire **does not care** what you did yesterday
  (or plan to do tomorrow)
- Fire is happy to exploit the **smallest vulnerability**
- Fire **does not stop** until it absolutely owns everything
  (Until there are no more assets to compromise)

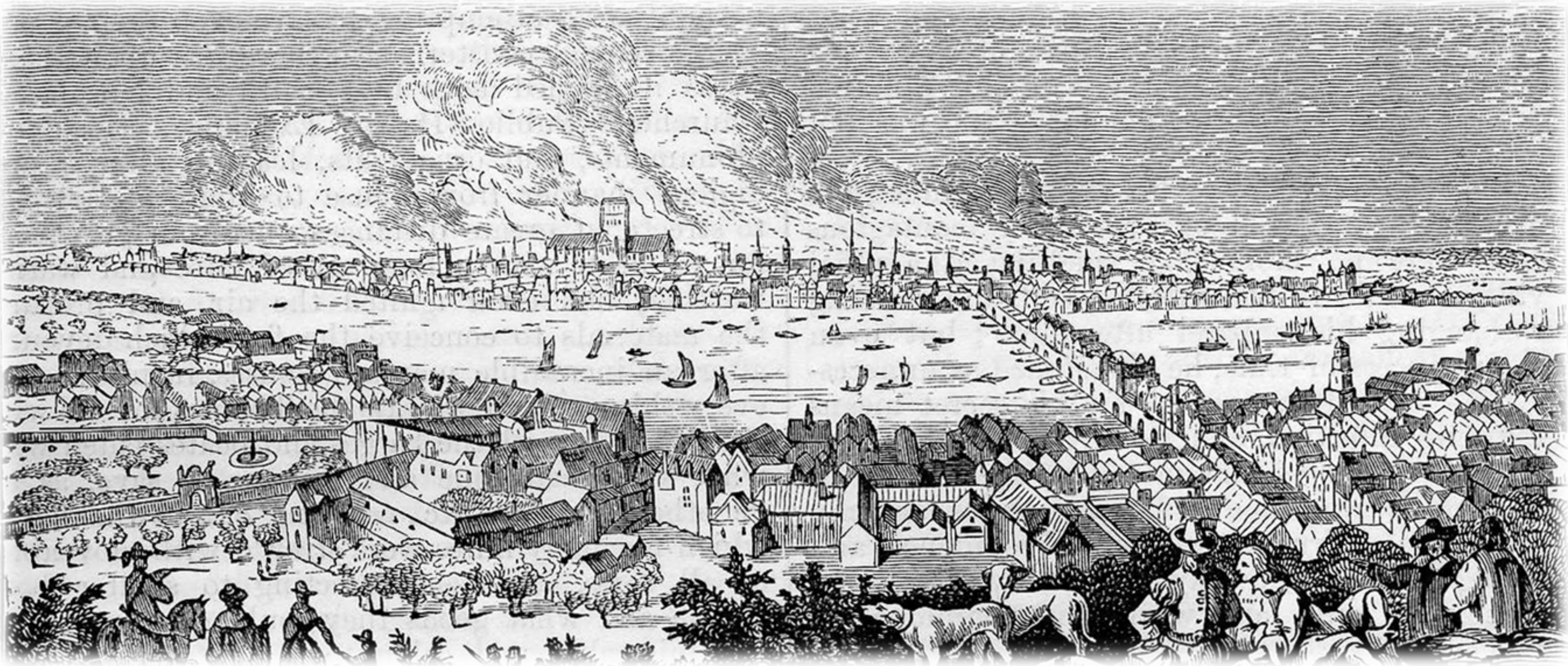
# A brief history of two landmark fires

# London, 1666

fire

# 17th Century fire-fighting techniques

# Three days of fire



# Effects

- 13,200 Homes
- 75,000 Homeless
- 80% of the City of London destroyed
- 10 Dead
- Affects the British economy for years

# Chicago 1871

# But this is 1871

- 17 horse drawn fire engines
- 180 fire fighters
- 1 pumping station (but with a wooden roof)

# Effects

- 120 miles of wooden sidewalk burnt
- 33% of buildings destroyed
- 100,000 people homeless

# Metaphors and lessons

# A reminder

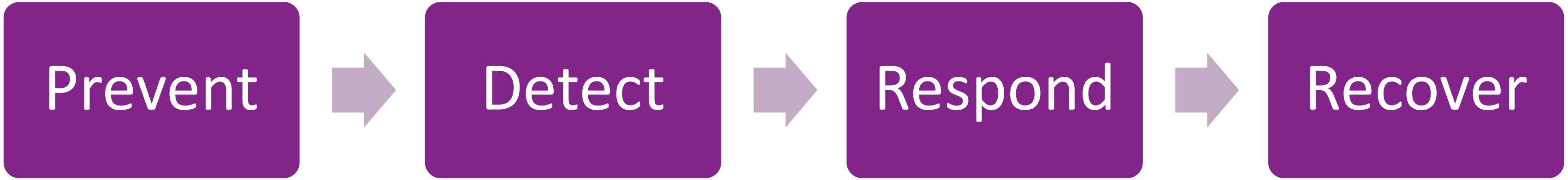
I know you know this

Aim: How to better explain things

# Metaphors and lessons

***“those who cannot remember the past are condemned to repeat it”***

**George Santayana, The Life of Reason 1905**



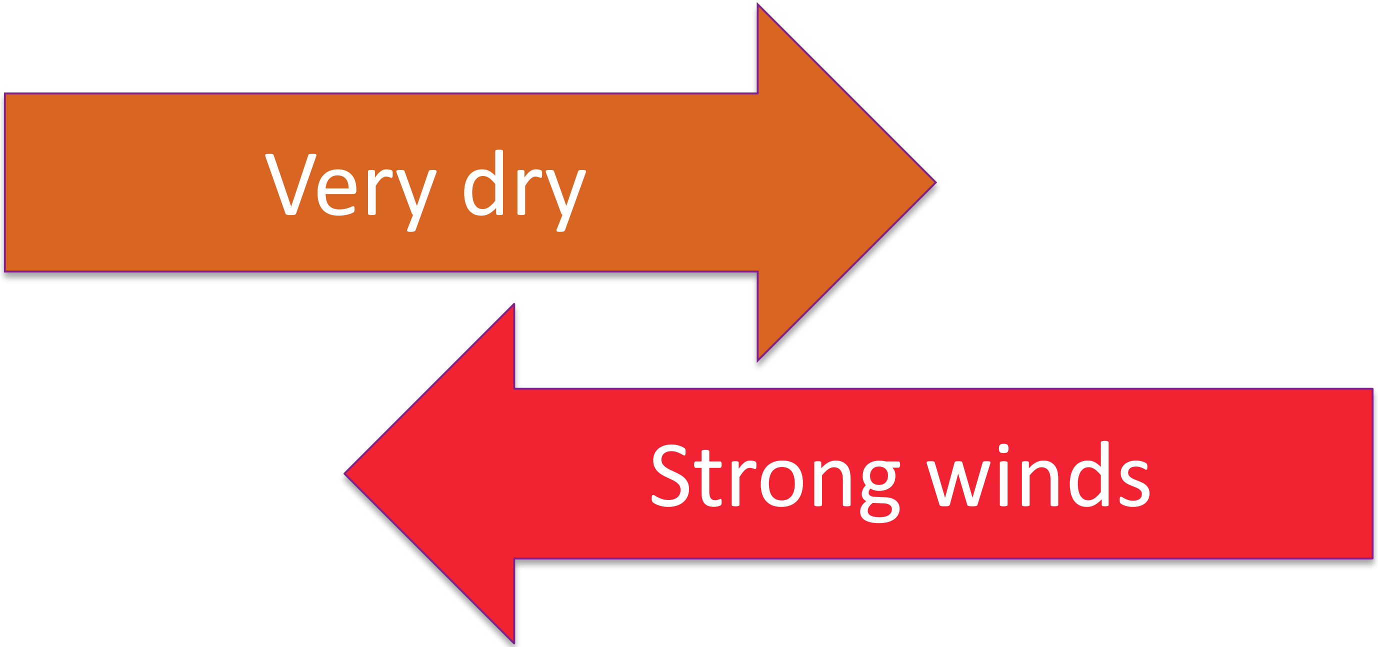
Prevent

Detect

Respond

Recover

# “Perfect threat storm”



Very dry

Strong winds

# Prevent

## London

- **Vulnerable construction of basic components.**
  Wood & straw

- **No segmentation.**
  Narrow streets, overhanging buildings

- **Manual controls**

## Chicago

- **Better construction but significant vulnerabilities**: tar roofing, decorative wooden cornices and advertisements

- **Segmentation easily defeated.**
  Wooden sidewalks, wind blew sparks across the river

- **Manual controls**

# Prevent

## It is too late to fix architectural problems when you’re on fire

Unpatched applications?

Flat networks

Vulnerable OS?

Too many admins?

# Detect

## London

- Detection too late to prevent total compromise of the asset.

## Chicago

- Detection too late to prevent total compromise of the asset.

# Detect

There is a ‘golden hour’

Treat every incident as unique

# Respond

## London

- **Strategy relied on sacrifice of compromised asset and neighboring assets.**
  Unprepared to follow strategy

- **No plan B.**
  Everyone acted individually. Lack of skilled resources. Lost control quickly.

## Chicago

- **Strategy relied on fast response to limit fire to a single asset.**
  Too hot, wind too strong so fire spread too quickly on wind

- **Response mechanisms vulnerable to attack.**
  Wooden roof on pumping station

# Respond

## Be decisive

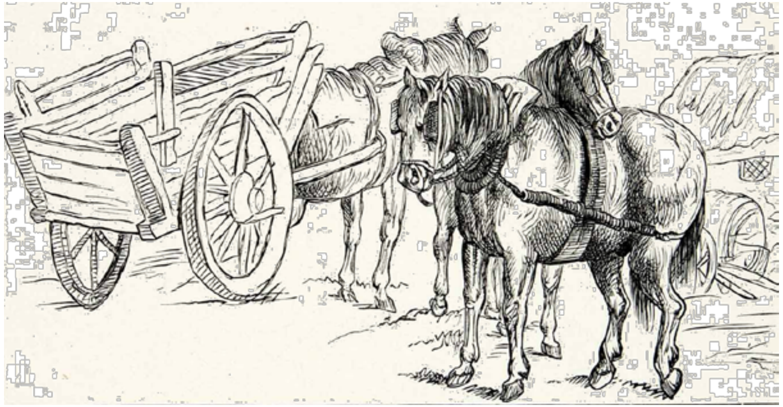
## What if your response mechanisms are vulnerable?

Are there known issues?

# Recovery: individual

## London

- Move assets

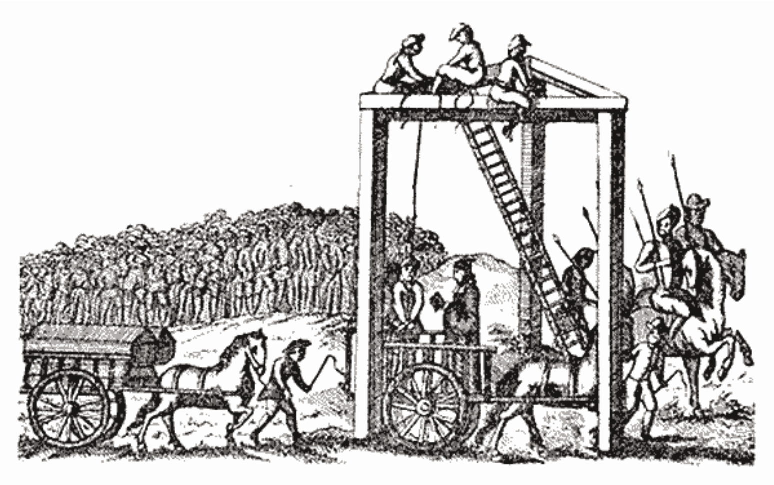


## Chicago

- Secure assets

# Attribution

## London



## Chicago

# Attribution

**Attribution close to the event is unreliable**

# Comparison

| London | Chicago |
|---|---|
| Surprise! | Again? |

# Or…

*“that men do not learn very much from the lessons of history is the most important of all the lessons of history”*

**Aldous Huxley, Collected Essays 1959**

# Comparison

**RSA, Google etc.**

Surprise!

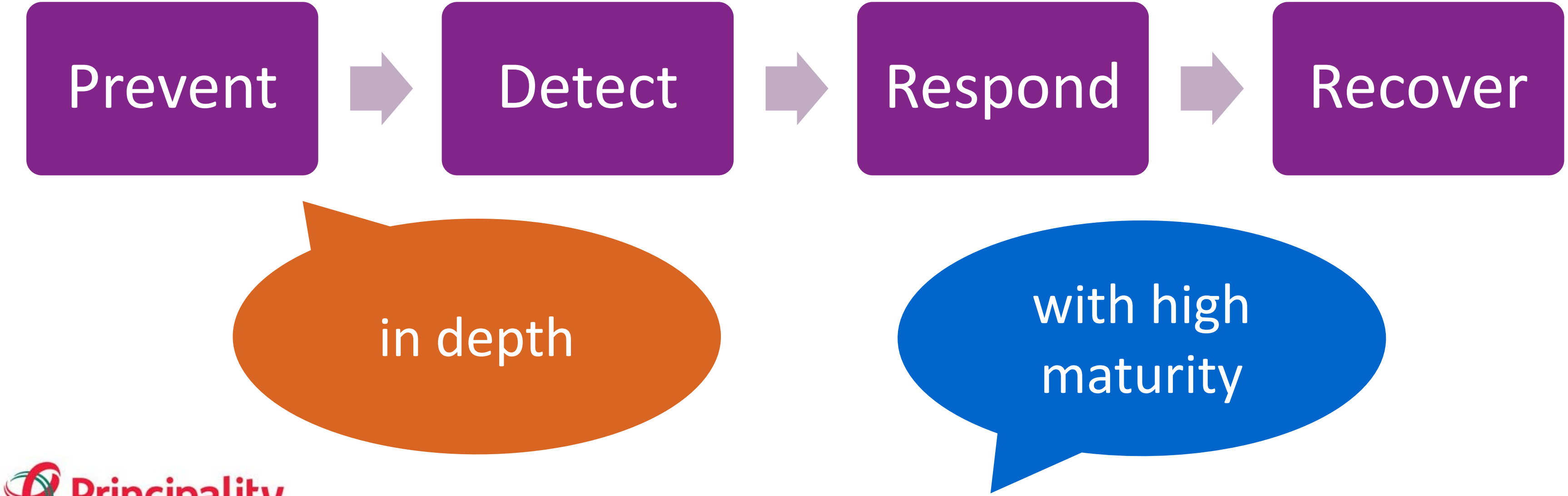
**Sony**

Again?

# What about today?

# What about today?

## What did fire safety get right?

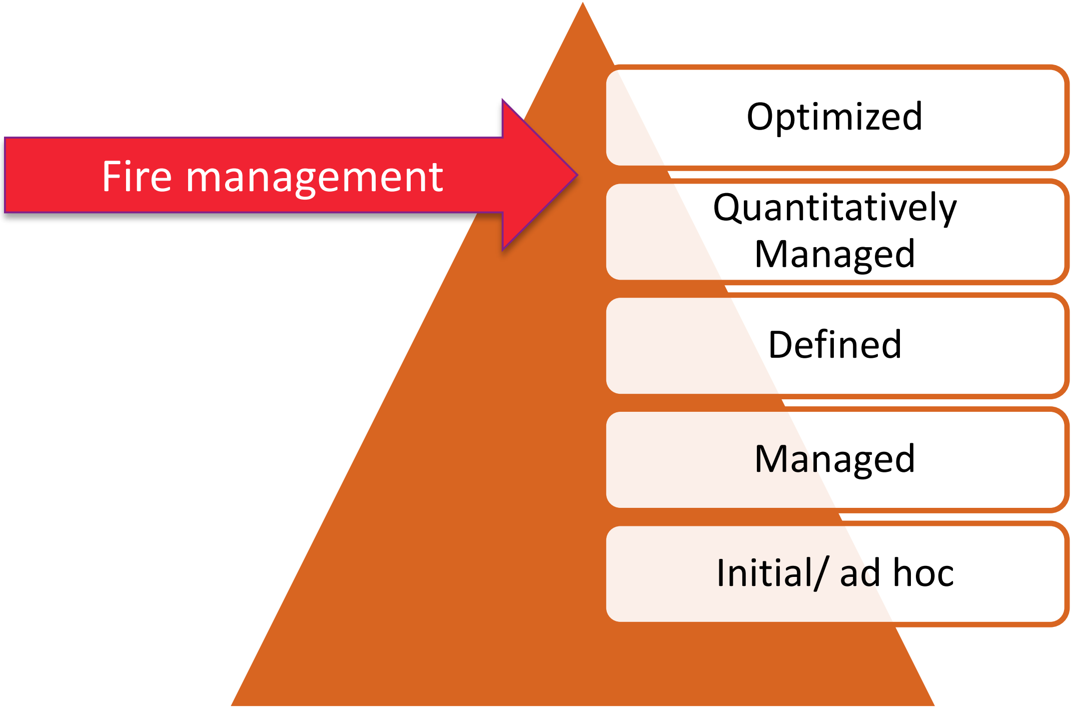


Prevent → Detect → Respond → Recover

in depth

with high maturity

# Control maturity (CMMI)



# Why?

*“fire has a low tolerance for control failure”*

**John Elliott, 2016**

# Prevent

in depth

with high maturity

# Detect

reliable

almost eliminate false positives

with high maturity

# Respond

in depth

with high maturity

# Recover

with high maturity

# Always learning

**When fire starts in a tall building**

restrict to a floor

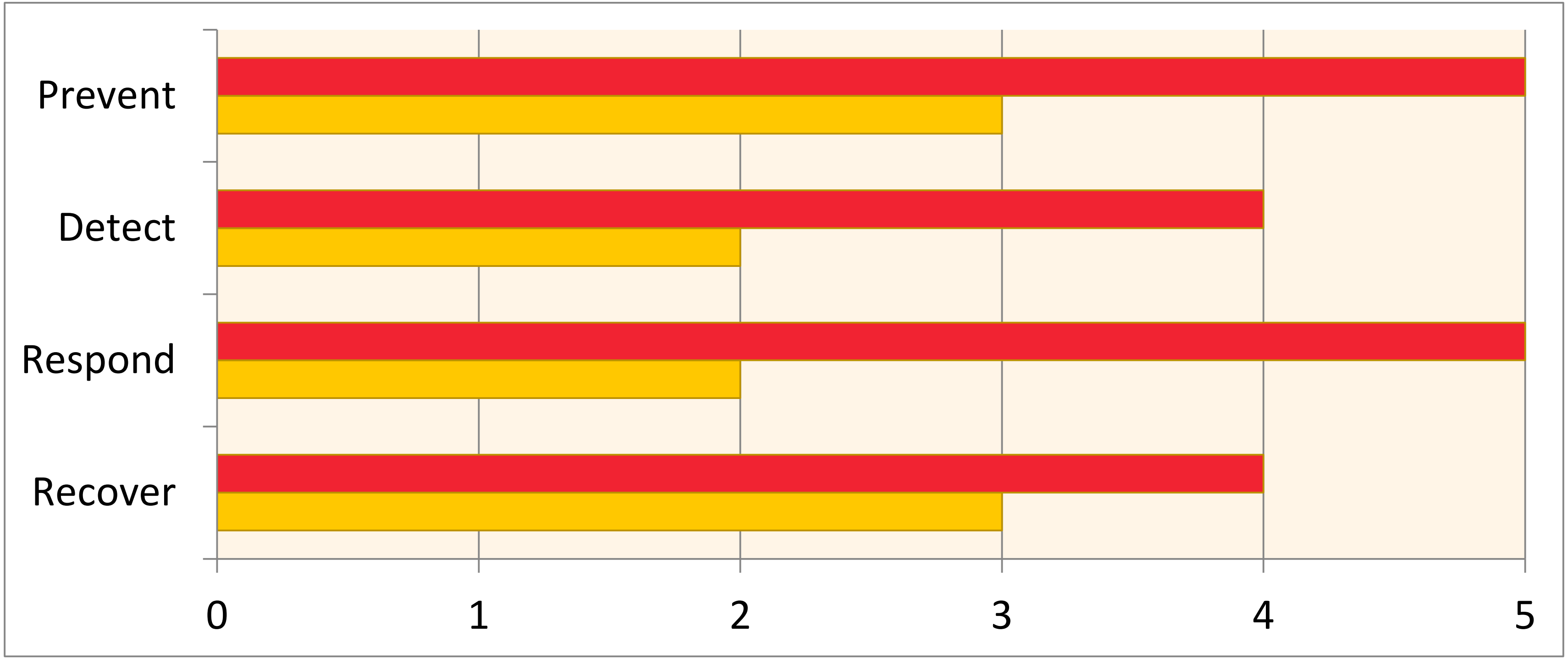
safe evacuation route

sprinklers

dry riser

# Always learning

# Fire v Cyber security



# How did we get better at FIRE?

**insurance** | **regulation**

effect, bring
ation from LEG
legislation /lɛdʒ
laws. 2. a la
lēgis lātio the
legislative /'lɛ
ing laws: a
legislative

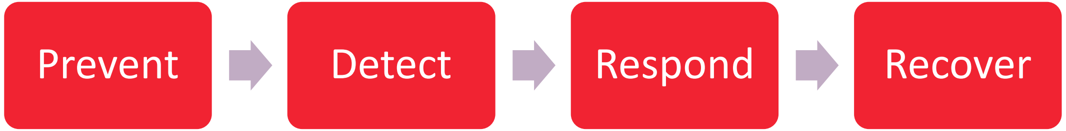
# So what?

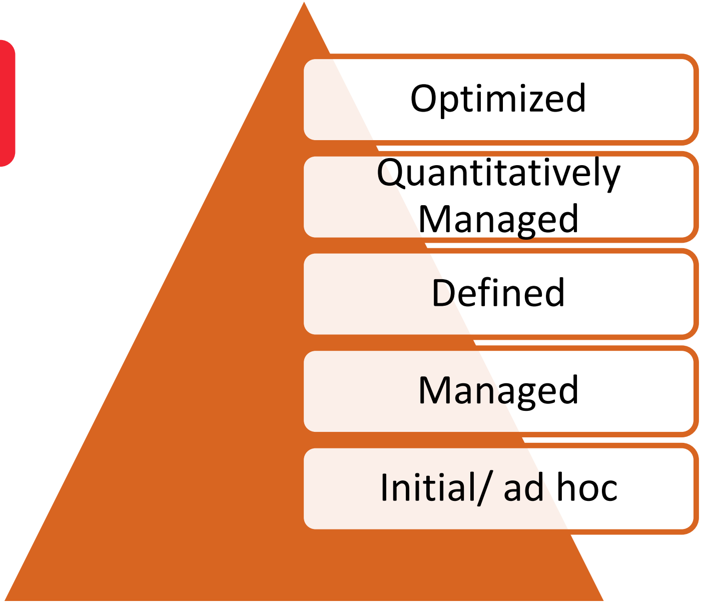
# Reminder

## I know you know this

## Aim: How to better explain things

# How to use this when you talk to …


Prevent → Detect → Respond → Recover


Optimized

Quantitatively Managed

Defined

Managed

Initial/ ad hoc

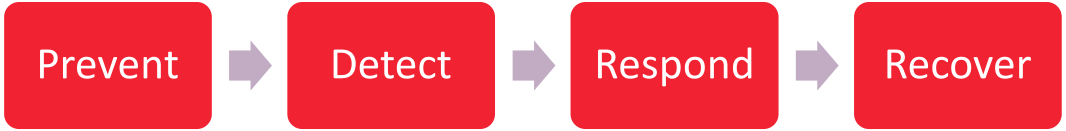
## Find a story

# Pick your favorite metaphors

- LONDON: Indecisive management
  - “This is not a problem”
- CHICAGO: Wooden sidewalks, wooden advertisements
- BOTH: Sparks carried on the wind defeated firebreaks
- CHICAGO: Fire safes that were not
- PROBABILITY: Dry, strong winds, failure of manual preventative control

# Understand your own environment

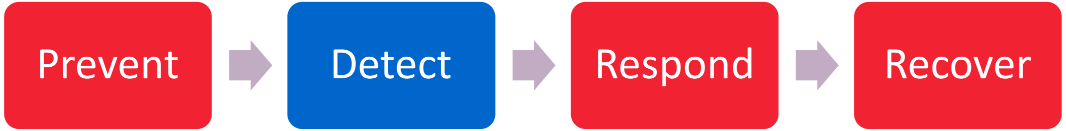
- What are your fire controls
- How mature are they?
- Can you describe your current



Prevent → Detect → Respond → Recover

In respect of maturity?

# How to use this when you talk to …

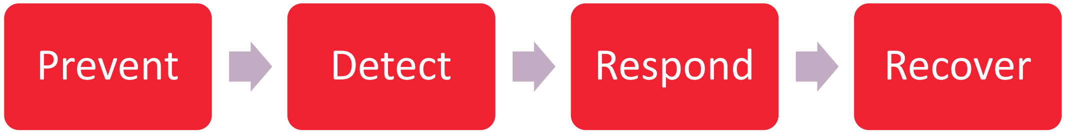

Prevent → Detect → Respond → Recover

**Fire management is based on the premise that fires will happen**

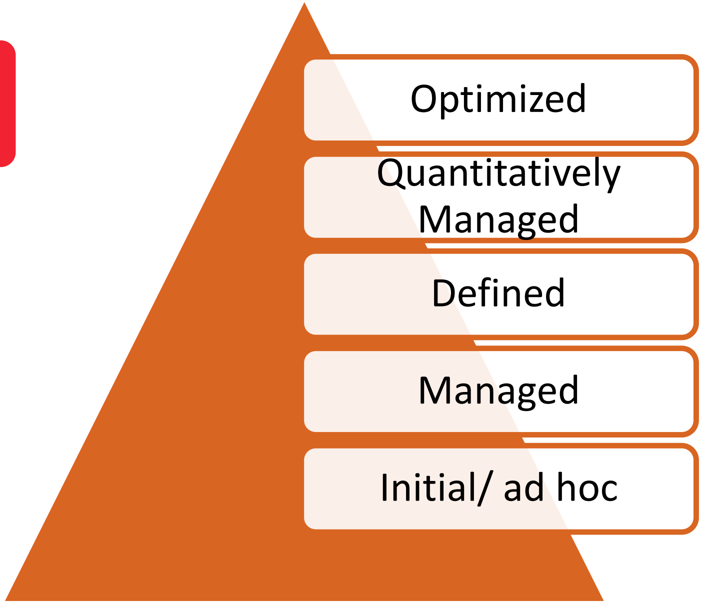
What do you mean by INAMOIBW!

🚫 **false positives**

# How does what you propose …



Prevent → Detect → Respond → Recover



Optimized

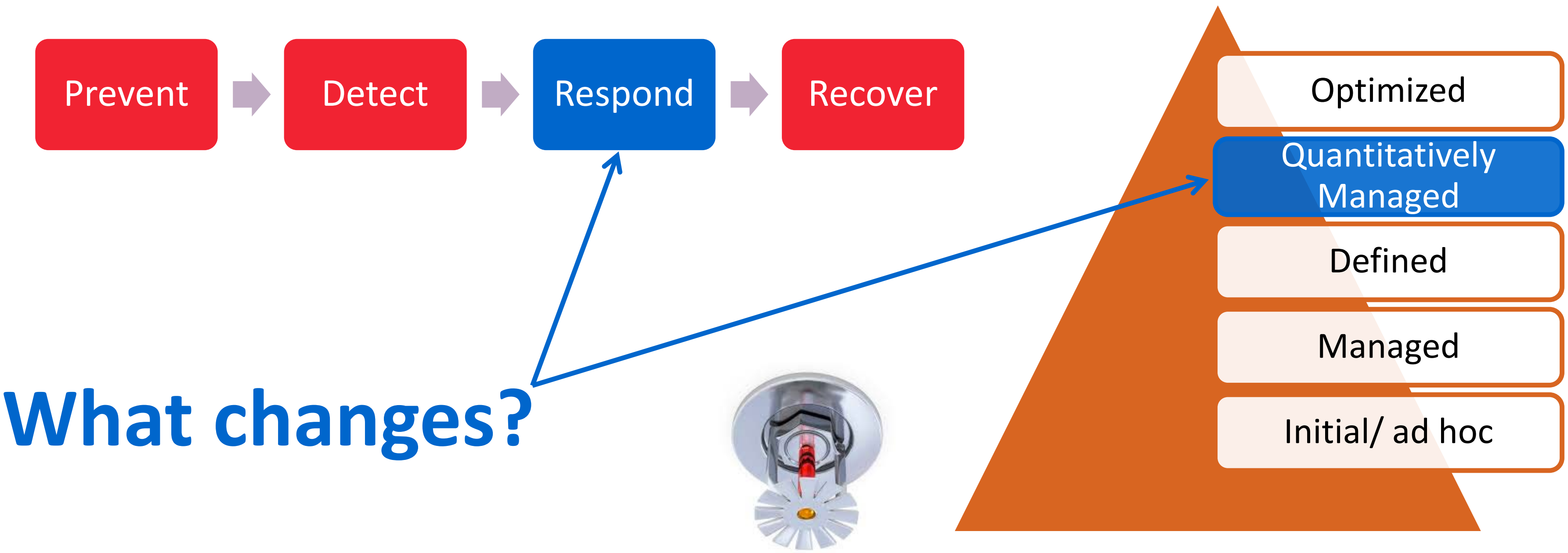
Quantitatively Managed

Defined

Managed

Initial/ ad hoc

# How does what you propose …



Prevent → Detect → Respond → Recover

Optimized

Quantitatively Managed

Defined

Managed

Initial/ ad hoc

**What changes?**

Principality
Building Society
Cymdeithas Adeiladu

# But most importantly

Get comfortable with the metaphor

# and remember …

## Like an attacker, fire has zero tolerance for control failure

# Questions …