CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Cybersecurity “Case Study”

Mike GOODFELLOW, TO/GIS, ICAO

Disclaimer

- This case study presents a scenario
- The scenario is fictional
- The scenario is inspired by actual events
- The scenario is an admittedly contrived but still plausible situation
- The scenario purposely ignores or simplifies many real-life issues
- The scenario is for illustration purposes only

Setting the scene

- We are at a smaller-sized airport
- First day of a long weekend due to a national holiday
- Airport is much busier than usual
- A single large airline accounts for about half of the traffic
- The IT director and their deputy have just returned the day before from an IT conference with lots of free giveaways and are working overtime to catch up

Setting the scene

- The largest airline’s station manager is a tough veteran with decades of experience and a confrontational personality
  - His airline flies exclusively to slotted airports from this destination
- The airport service manager has roughly 5 years experience, and has just moved from another airport mostly served by commuter airlines

The phone call

- The station manager calls the airport service manager
  - He is not happy at all
  - Flights are being delayed due to no-shows
  - Passengers are arriving at their gates late and confused by gate change notifications
  - Other airlines are reporting similar stories
  - He would like “her problem” fixed immediately

The phone rings again

- This time it is someone in baggage claim
- Passengers seem to be all congregating around a single, non-functional carrousel nearest to the exit
- Meanwhile, bags at the other 3 carrousels are not being claimed causing a backlog of passengers in the hall
- The relatively small hall is filling up fast and the baggage hall staff are worried about passenger flow

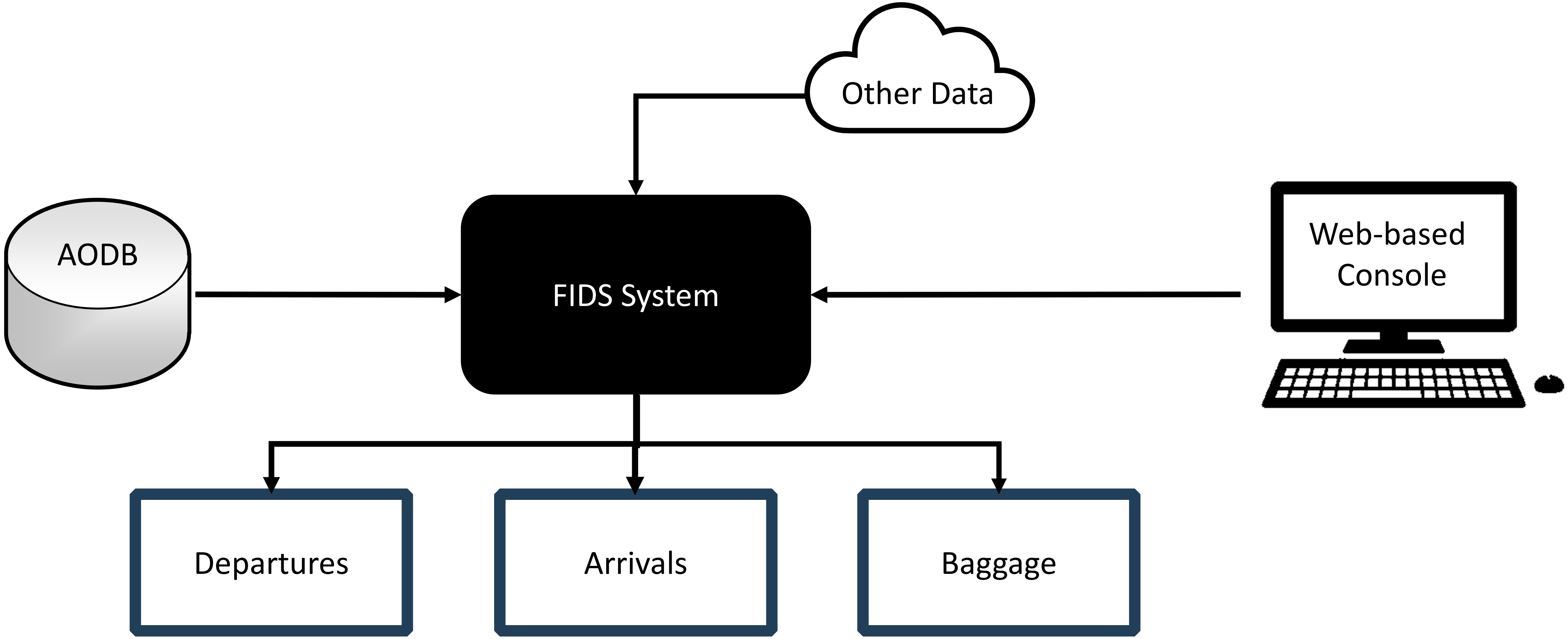
More bad news

- The phone rings for a third time and it’s the station manager again
- He is even angrier than before about the departure gate boards
- He says that the departure gates on “the grid” layout are correct, but that there are large notices on the adjacent screens saying that flights have been canceled or have changed departure gates and to check with airline staff

Trying to get some answers

- The airport service manager calls the IT director in a near panic
- She tells him the story about the gate change notice on the screens
- The IT director, already working late to make up from his conference trip, is a bit annoyed at her but says he told his deputy to make sure the updates were run on the FIDS system earlier
  - The software update requires downloading an executable from the vendor’s website
- The IT director tells her he will ask his deputy as soon as he sees him
- He hangs up and goes back to his work

System overview

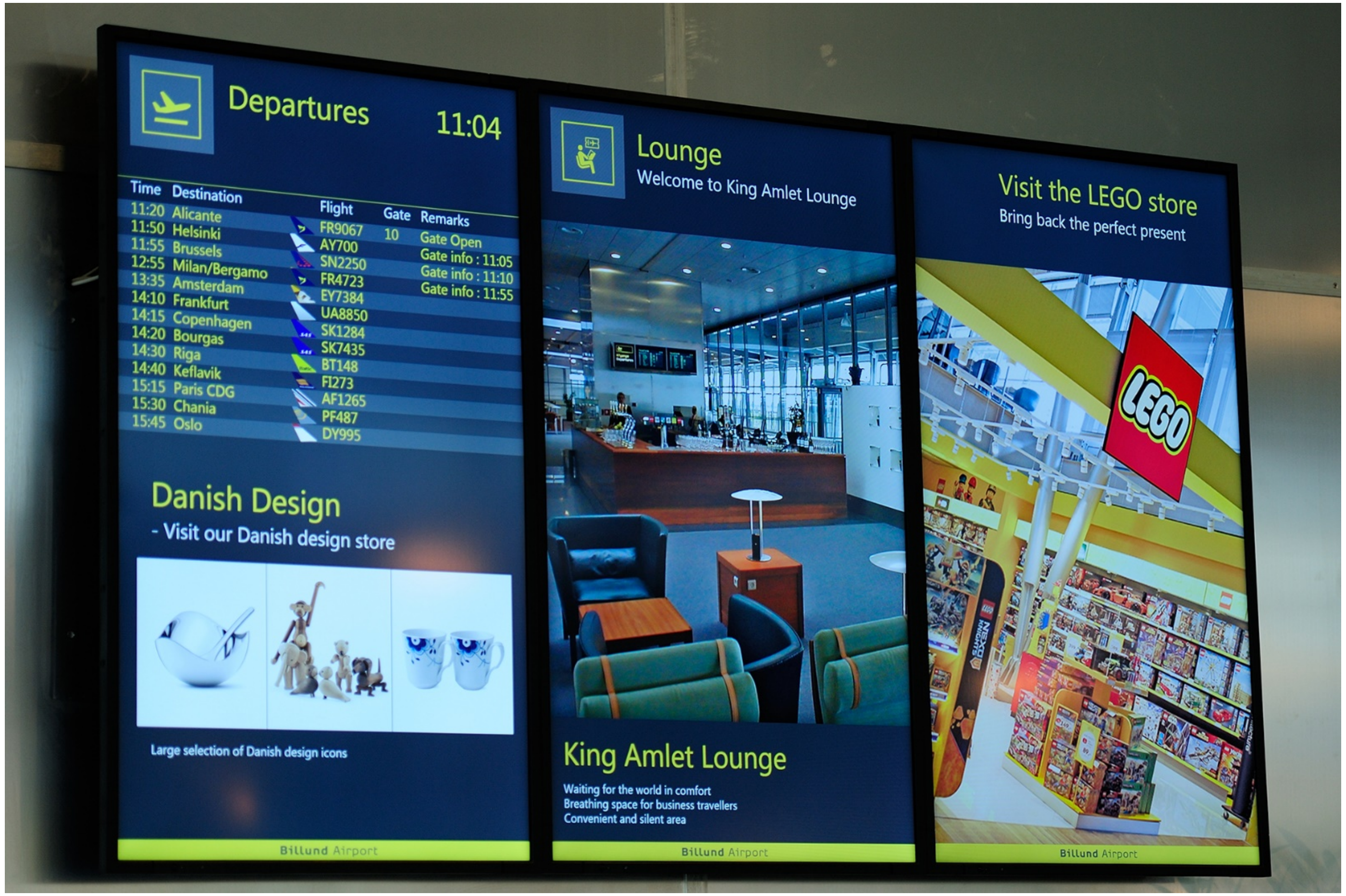


How did we end up here?

- The airport service manager has moved from near-panic to full panic
- The departure area is now in complete chaos
- The backup in baggage claim now extends to passport control, which has shut down due to the excessive traffic not clearing
- Arriving passengers are now beginning to accumulate in the arrivals area
- The airport service manager phone is now ringing non-stop

So, what happened?

FIDS



Departures 11:04

Time	Destination	Flight	Gate	Remarks
11:20	Alicante	FR9067	10	Gate Open
11:50	Helsinki	AY700		Gate info : 11:05
11:55	Brussels	SN2250		Gate info : 11:10
12:55	Milan/Bergamo	FR4723		Gate info : 11:55
13:35	Amsterdam	EY7384		
14:10	Frankfurt	UA8850		
14:15	Copenhagen	SK1284		
14:20	Bourgas	SK7435		
14:30	Riga	BT148		
14:40	Keflavik	FI273		
15:15	Paris CDG	AF1265		
15:30	Chania	PF487		
15:45	Oslo	DY995		

Danish Design
- Visit our Danish design store

Large selection of Danish design icons

Billund Airport

Lounge
Welcome to King Amlet Lounge

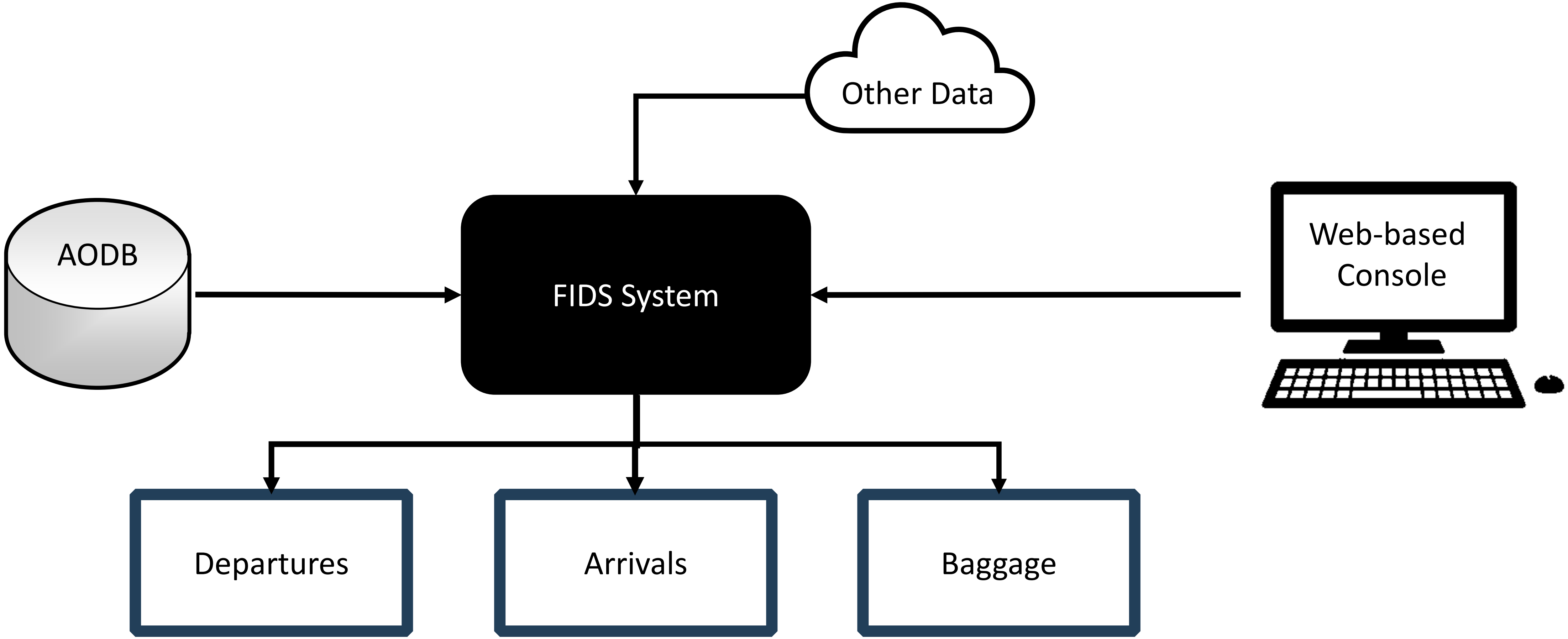
King Amlet Lounge
Waiting for the world in comfort
Breathing space for business travellers
Convenient and silent area

Billund Airport

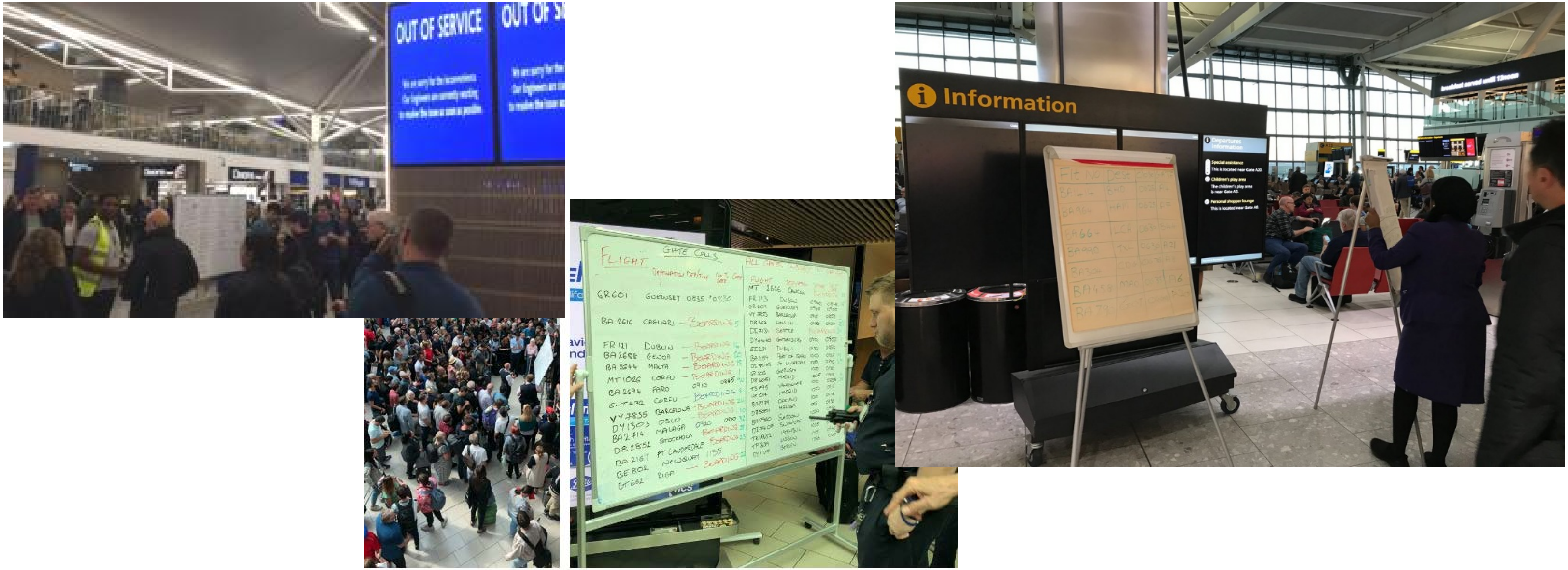
Visit the LEGO store
Bring back the perfect present

Billund Airport

FIDS


Other Data
AODB
FIDS System
Web-based Console
Departures
Arrivals
Baggage

This is a thing



Why FIDS?

- High visibility
- Normally the first thing people check at an airport
- Generally classified as “digital signage”
    - Advertising material can come from external sources and is often prominent on screen
- Normally fed by Airport Ops DB (AODB)
    - Sometimes not
    - Manual/emergency override an option
- Can be cloud hosted

The next day…

Setting the scene

- The mayhem from yesterday has (mostly) subsided
- System-wide knock-on effects of the delays are still being felt by the airlines
- The airport itself is in full reputational damage control mode
- The airport service manager is now on stress leave
- Press have been calling the media office non-stop since they heard about the problems
- The airport media coordinator is a new hire who just graduated from university

I have an idea!

- The media coordinator has been given the latitude to deal with press calls as quickly as possible
- Apologies about yesterday’s mess have been posted on social media
- He does not feel comfortable or confident doing a full press conference in the press hall of the airport
- He reasons that the airport can project a more “personal” by him giving the interview in their offices
- He contacts the 2 biggest broadcasters in the area and schedules recorded interview with them for the evening news at 18:00

The evening news

- The media coordinator proudly watches himself on TV, happy with his performance and with the more intimate feeling that the in-office interview has provided
- About one hour later, he looks out the window facing the terminal entrance and notices that it seems a lot busier than usual for this time of day
- Some time later he gets a call from his colleague at the airport information desk asking if he knows anything about a discount flight voucher.

We may have a problem

- The crowd at the information desk seems to be getting bigger and bigger
- People are demanding flight vouchers, but airport staff have no clue what they are talking about
- Shortly it becomes clear that these are the people who were stuck in the baggage and arrival halls yesterday
- They say that they have come to claim a voucher for yesterday’s inconvenience that was posted about on the airport’s social media

We definitely have a problem

- The media coordinator checks the airport’s social media and sees the following:
    - Passengers inconvenienced by yesterday’s events should come to the airport information desk to claim a 50% discount flight voucher, valid on any future trip. Limited quantities – first come, first served.
- The media coordinator quickly goes to the login page of the airport’s social media account administration system

Perhaps bigger than expected

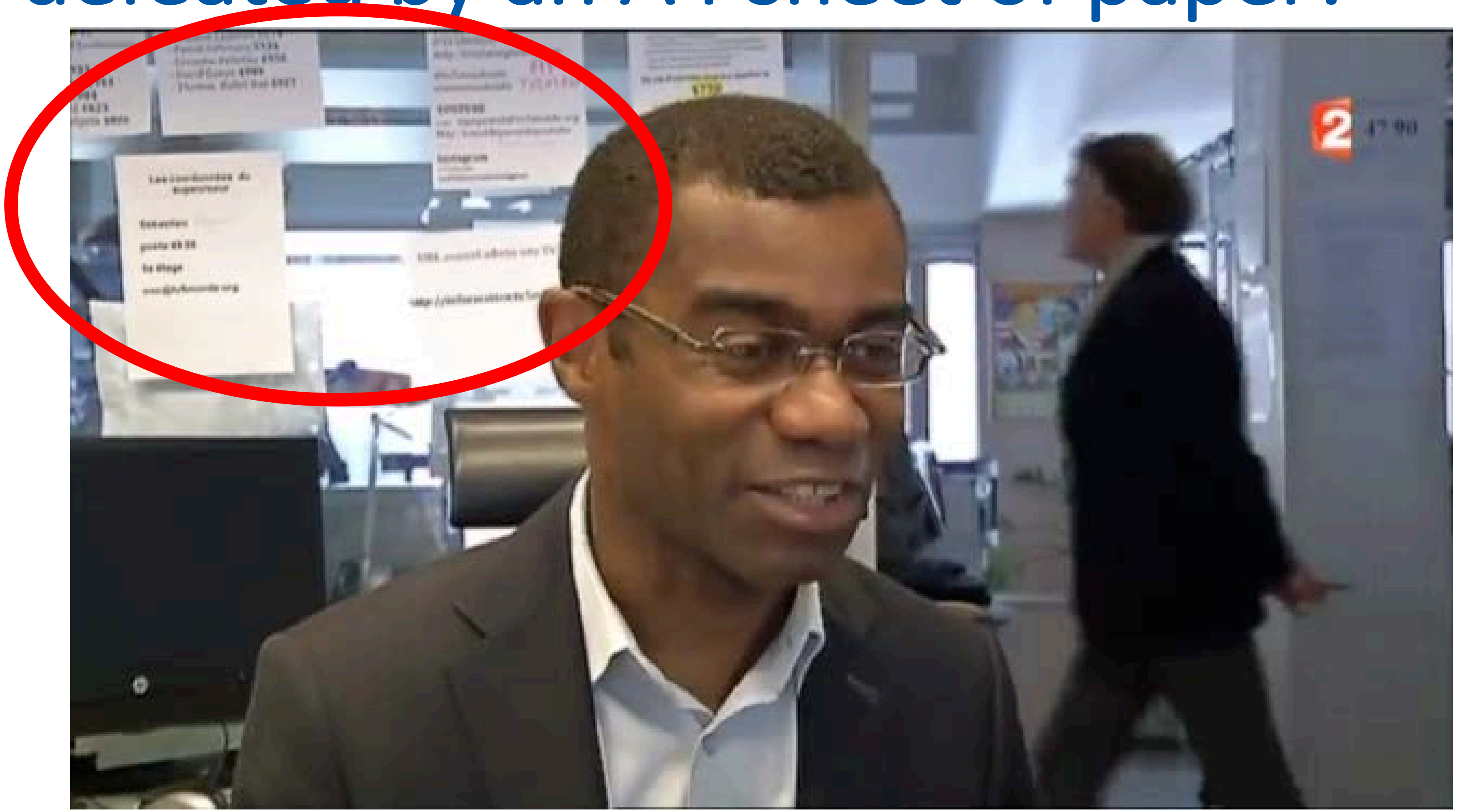
- His credentials are rejected
- He tries a second time, and his credentials are rejected
- He clicks on the password reset button
- The reset page asks him to enter the email address registered with the administration of the account and tells him to expect a confirmation email with a reset link
- The email never comes…
- The media coordinator is now calling his boss in a panic

So, what happened?

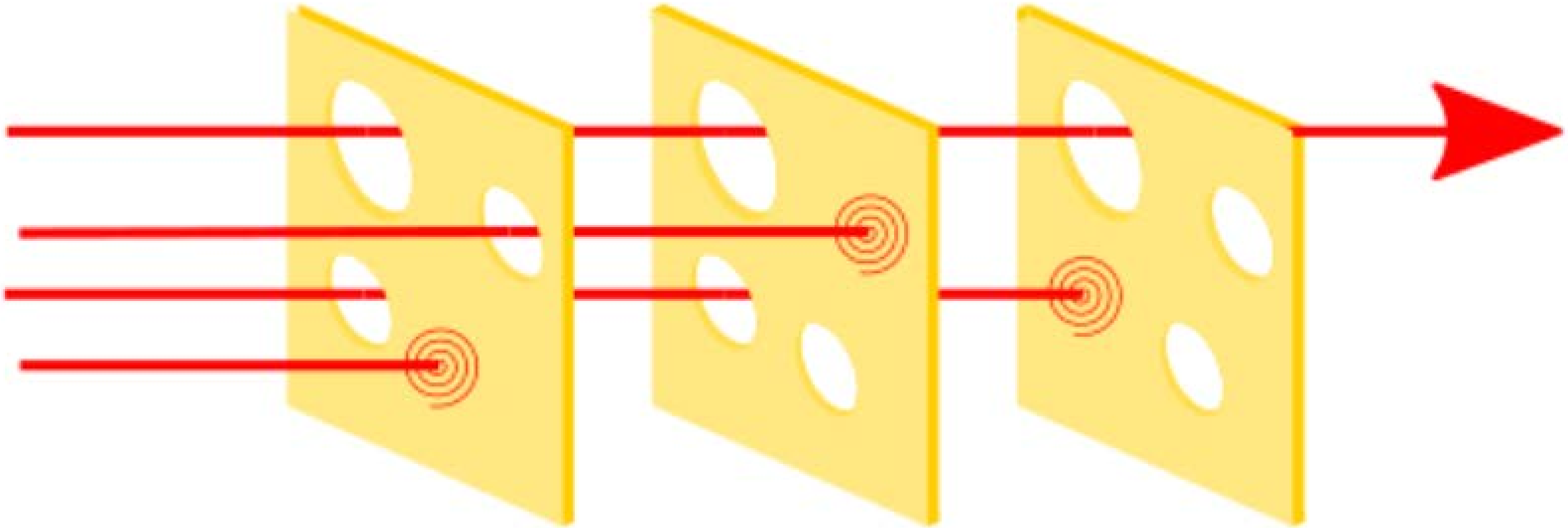
Great defenses

- Best firewalls
- Best IDS
- Best IPS
- Best cybersecurity practices
- 24/7/365 Security Operations Center

All defeated by an A4 sheet of paper!

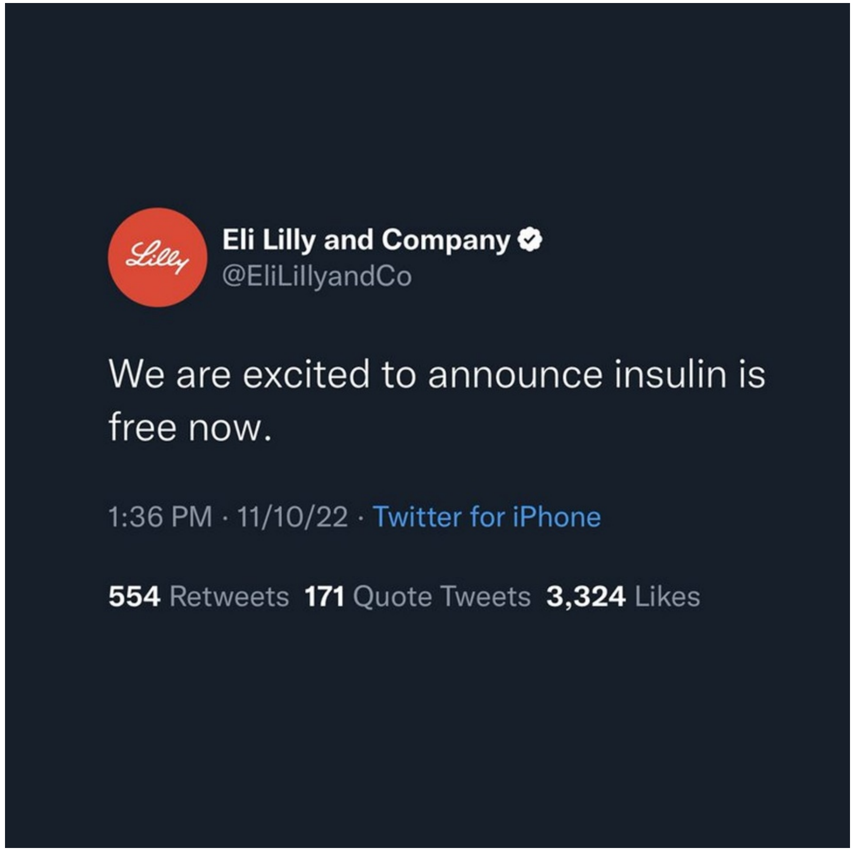


Defense in depth is great



But things still happen

Black swan events

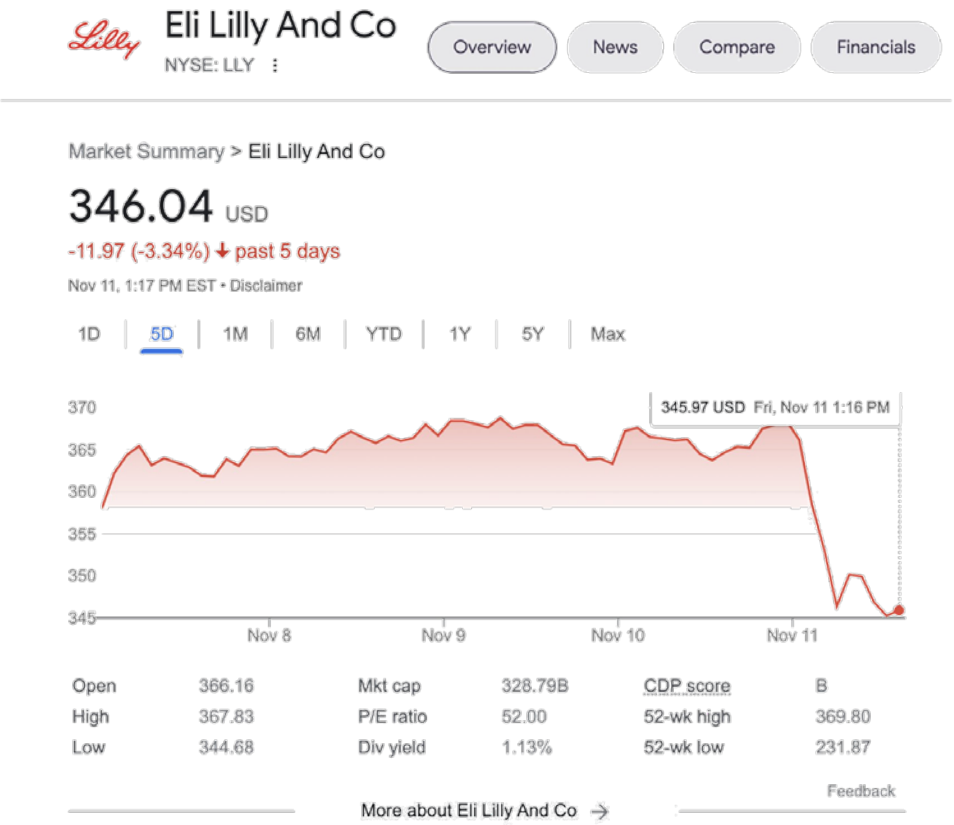


Eli Lilly and Company ✓
@EliLillyandCo

We are excited to announce insulin is free now.

1:36 PM · 11/10/22 · Twitter for iPhone

554 Retweets **171** Quote Tweets **3,324** Likes



Eli Lilly And Co
NYSE: LLY

Market Summary > Eli Lilly And Co

346.04 USD

-11.97 (-3.34%) ↓ past 5 days

Nov 11, 1:17 PM EST • Disclaimer

Open	366.16	Mkt cap	328.79B	CDP score	B
High	367.83	P/E ratio	52.00	52-wk high	369.80
Low	344.68	Div yield	1.13%	52-wk low	231.87

How would you work with your operators and service providers in a case like this?

Cyber Resilience

My favorite quote

“Everyone has a plan until they get punched in the mouth.”

Mike Tyson

Resiliency defined

“The ability of a substance to return to its usual shape after being bent, stretched, or pressed.”

Cambridge Dictionary

Resiliency defined

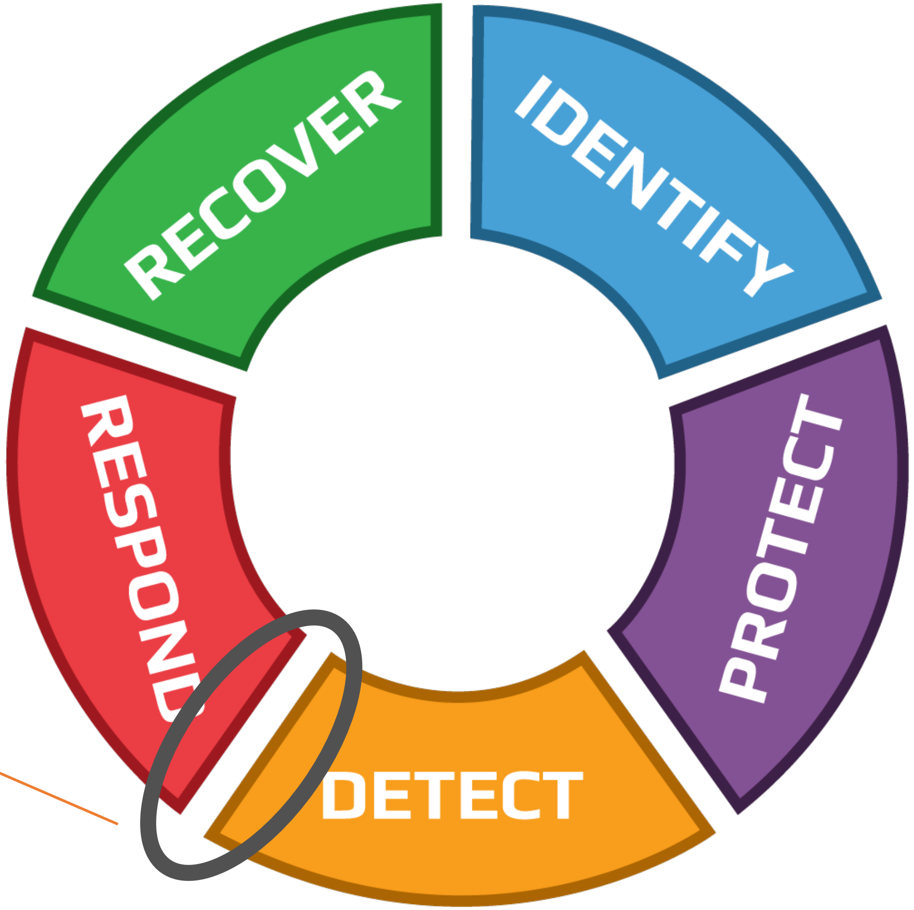
“The ability to absorb and adapt in a changing environment.”

ISO

Cyber Resiliency

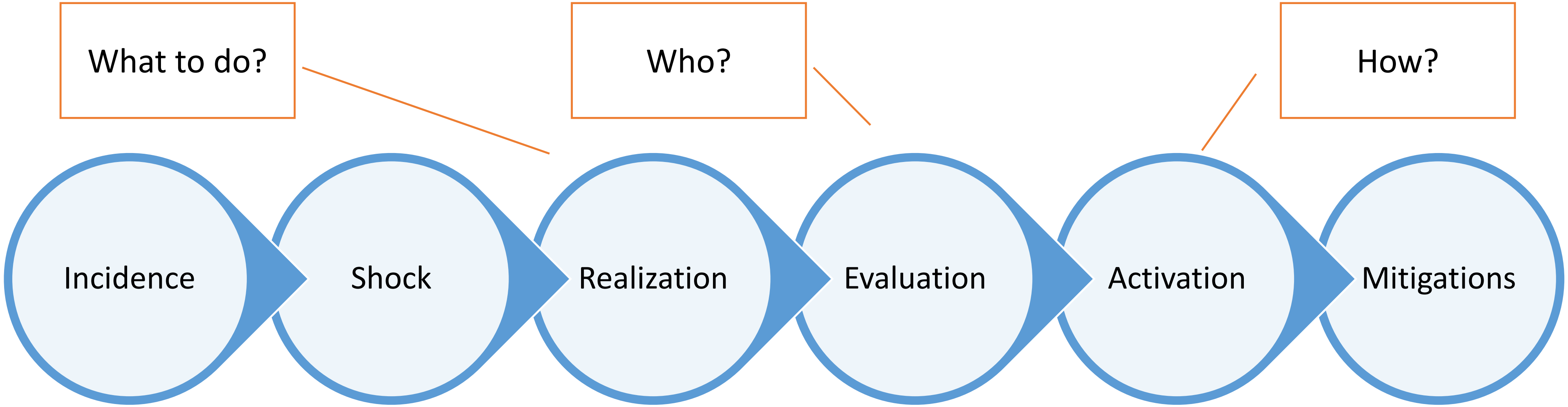
“The ability to absorb the abuse being received over enough time for response mitigations to become effective.”

NIST Cybersecurity Framework



This may not be an instant transition

Incidence to mitigation



What to do?

Who?

How?

Incidence

Shock

Realization

Evaluation

Activation

Mitigations

Emergency Response Planning

- ERP is an entire discipline (and art) unto itself
- No plan is perfect
- Adaptability is key
- Incident management is a bad time to be making new friends

Emergency Response Plan Questions

- Do you have a plan?
- Do you socialize the plan?
- When is the last time you drilled your plan?
- Did you drill activating your plan?
- What did you learn from the drill?

THANK YOU