

Visualising an insider threat incident from witness reports using natural language processing

Katie Paxton-Fear, Duncan Hodges, Oliver Buckley



Insider Threat

Nuanced

- Can cover a range of different attacks
- From a range of insiders

Impactful

- Insiders have valid credentials or access
- Insiders can go undetected
- Know the value of systems

Hard to investigate

- Incident response
- Detection of future incidents

People and technology

- A pure technical solution is not enough

Witness Reports



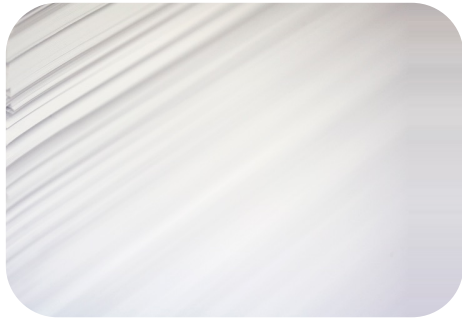
No prescribed writing style



Cognitive load



Selective disclosure



Large number of reports



Able to influence the model over time



Not trained on specific insider threat archetypes

The Goal

Tesla chief executive Elon Musk has accused an employee of "sabotaging" at the electric carmaker.

In an email to staff, Mr Musk said an unnamed employee had "stolen" data to "harm" the company.

The employee, who has not been named, is believed to have worked in the company's software department.

The full extent of this action is not clear, but Musk said the employee had "stolen" data to "harm" the company.

"He is a saboteur, and he is trying to harm the company," Musk said in the email.

"He is a saboteur, and he is trying to harm the company," Musk said in the email.

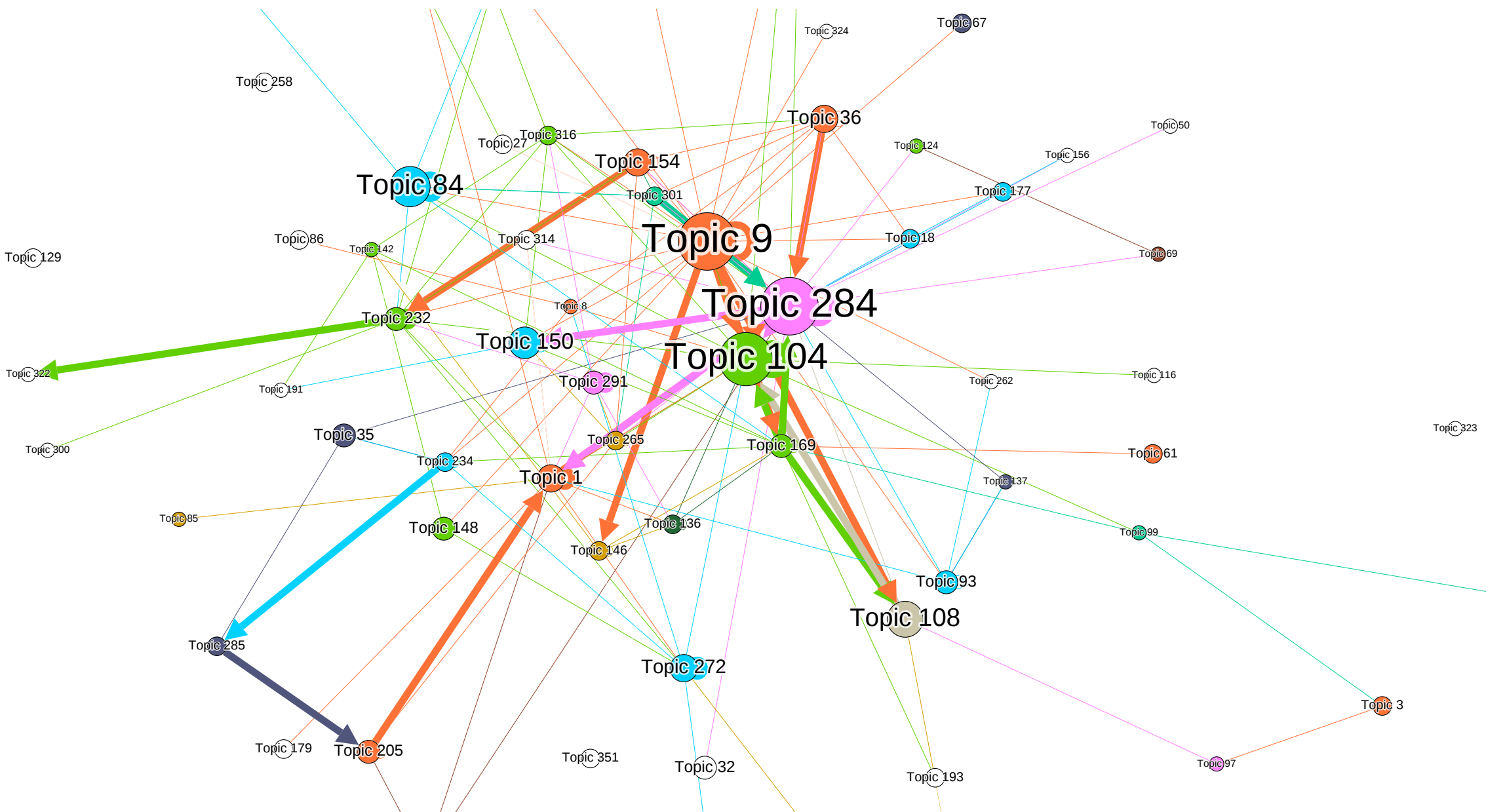
"As you know there are a long list of organisations that want Tesla to die," he added, citing Wall Street short-sellers as being among them.

BBC News: Tesla chief Elon Musk accuses worker of sabotage 19 June 2018

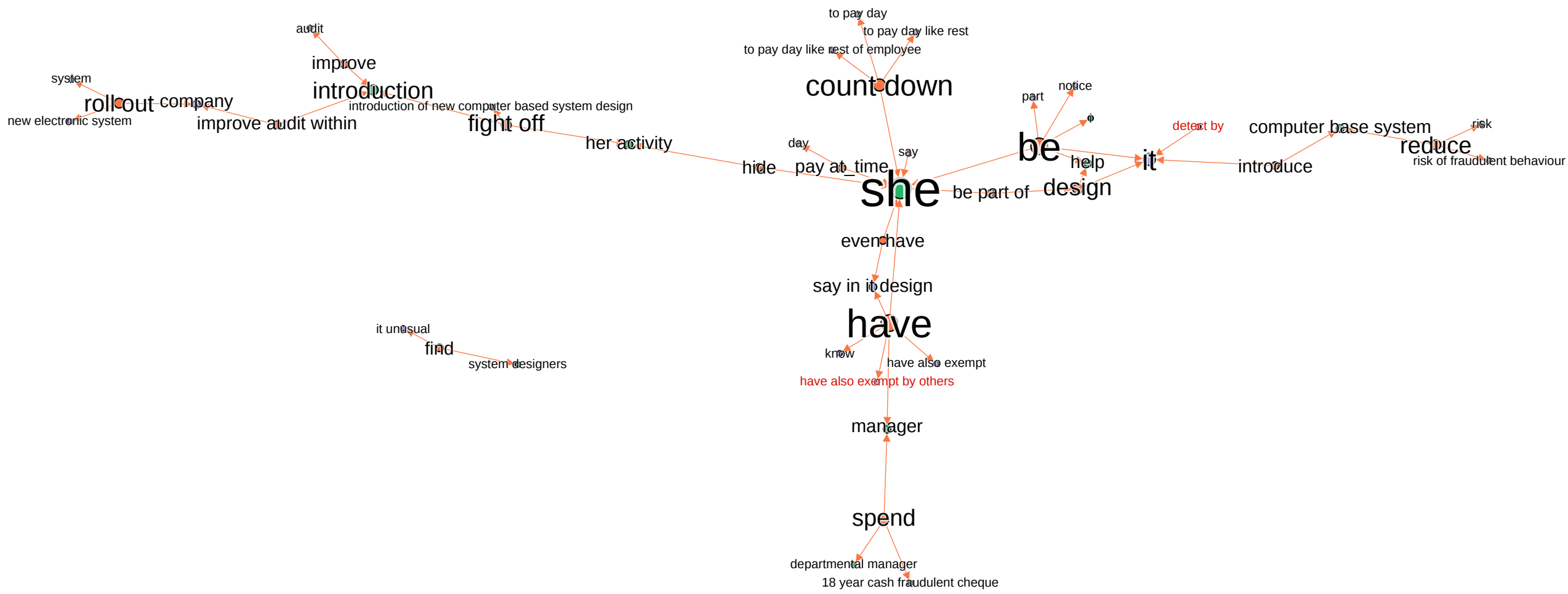


Time





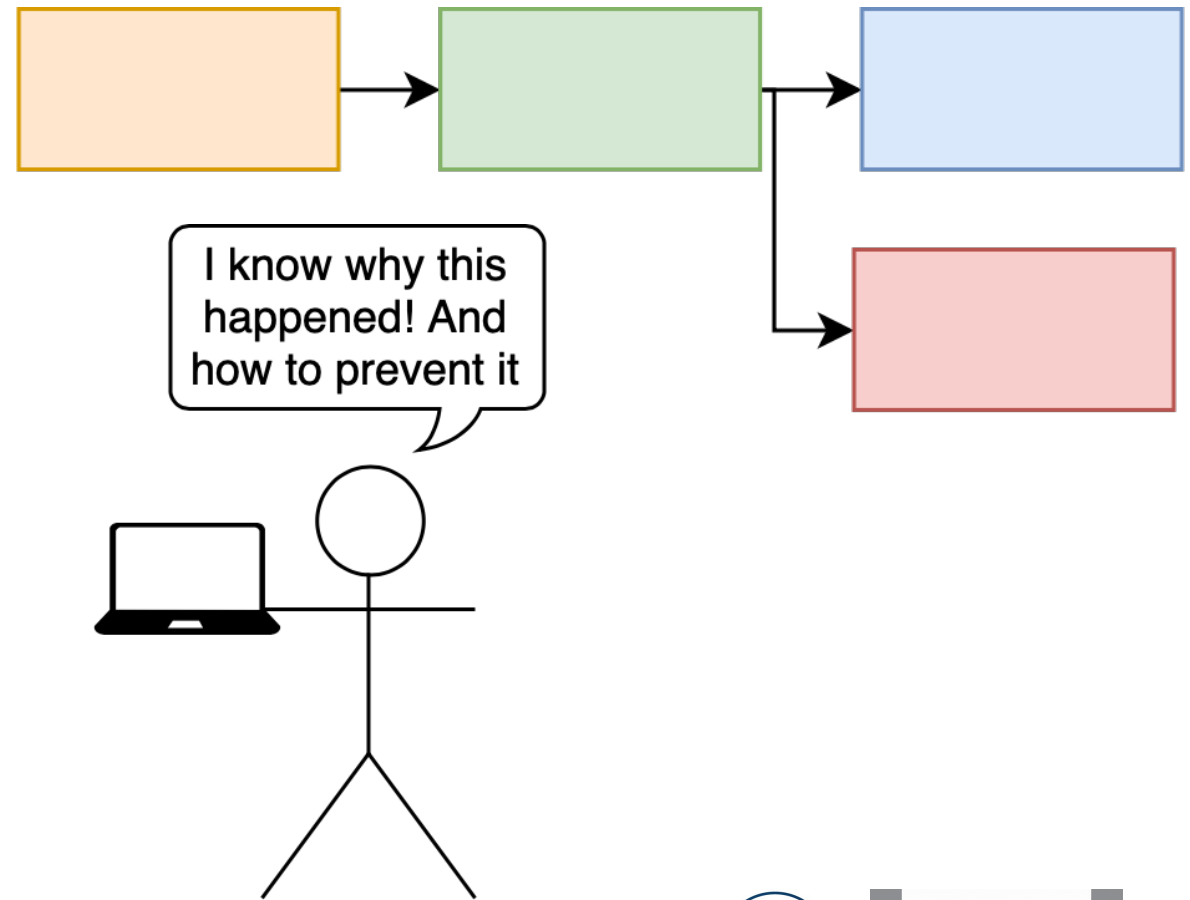
Temporal Graph



A single topic

Using the system

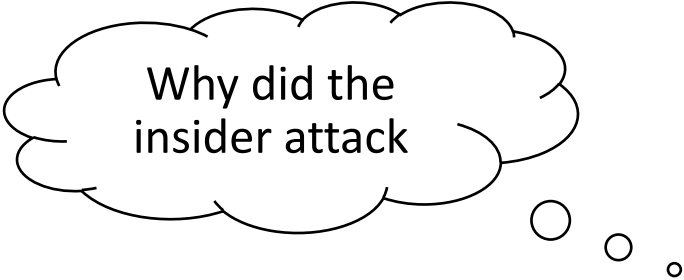
1. Find topics that seem relevant
 - The code e.g. Attack Step
 - A causal/temporal chain
 - A topic with a high amount of causality
2. Investigate individual topics
3. Build up an understanding of the attack
 - Why did it happen?
 - What assets were targeted?
 - Where could interventions be placed?



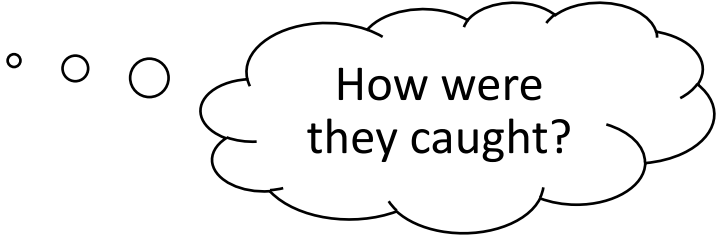
Asking questions



How did they
attack?



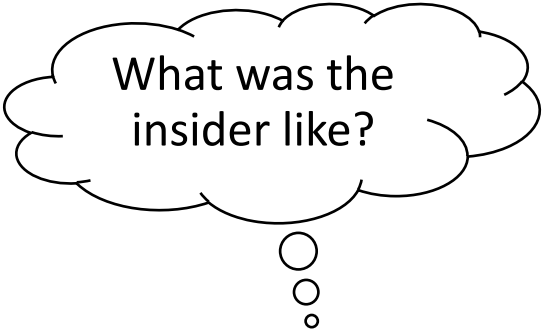
Why did the
insider attack



How were
they caught?

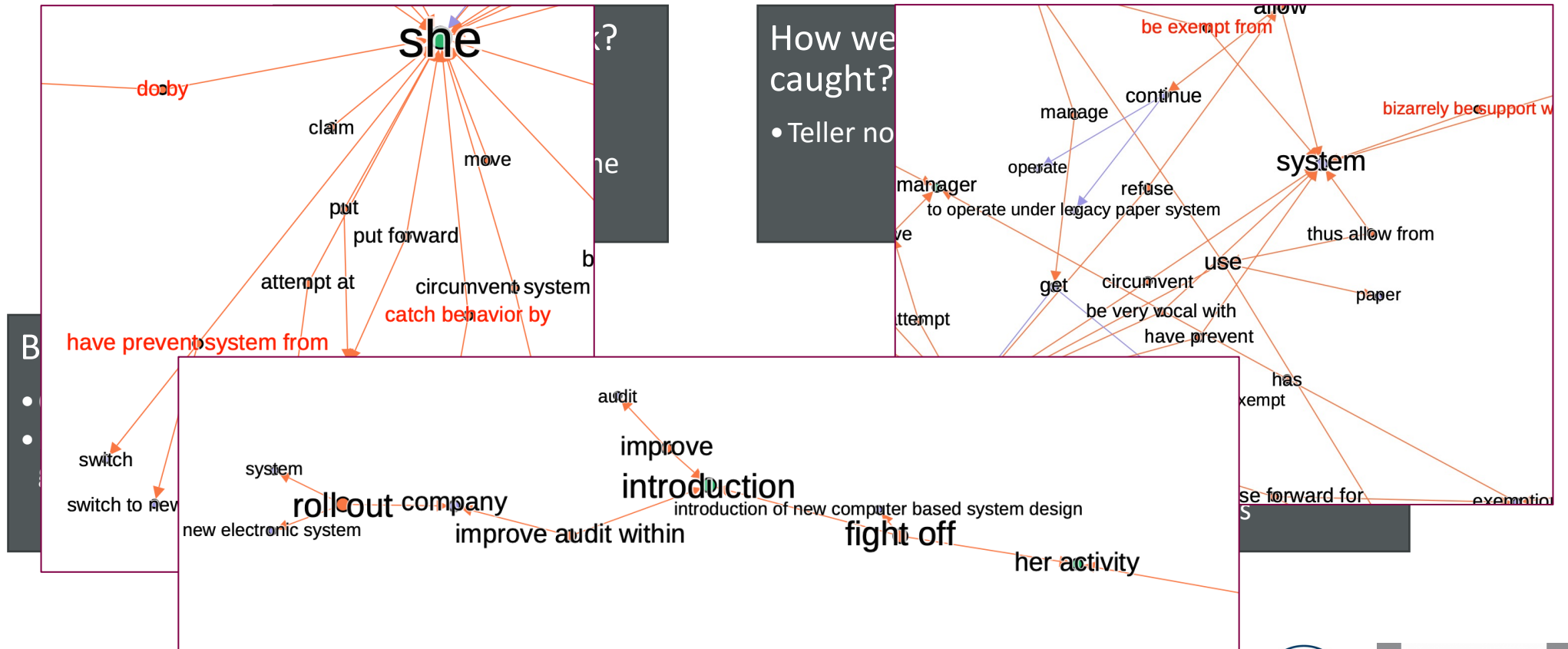


Behavioural clues?



What was the
insider like?

Answering questions



Answering questions

How did they attack?

- By using paper-based records
- Became e new system

How were they caught?

ake check

excessively large cheque

teller **saw**

cheque

Behavioural clues?

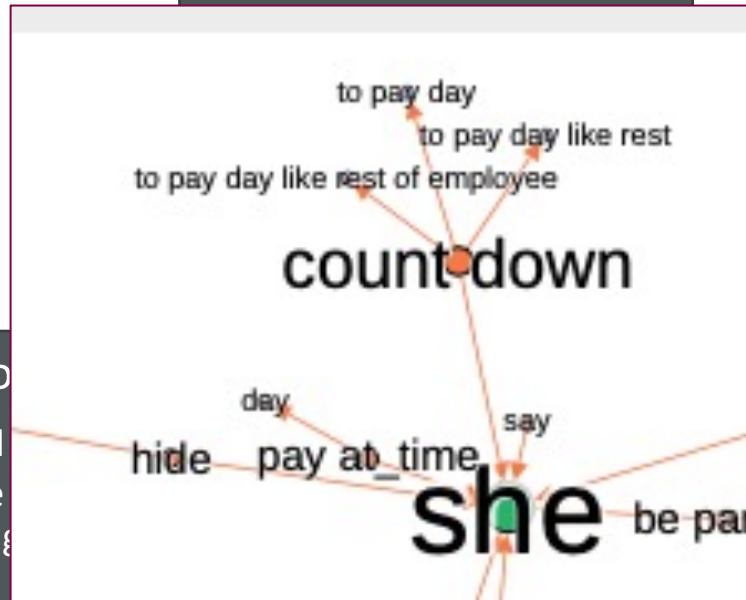
- Claimed a large inheritance
- Possible issues with gambling

What was the insider like?

- Charming + friendly - allowed her to bypass security controls

Answering questions

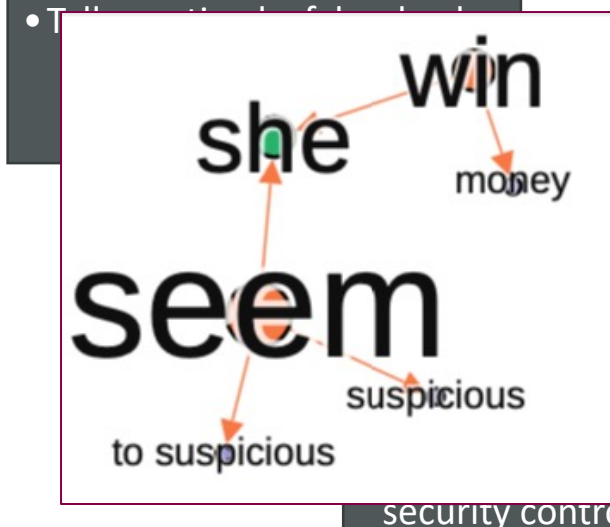
How did they attack?



Behavior

- Claimed
- Possible gambling

How were they caught?

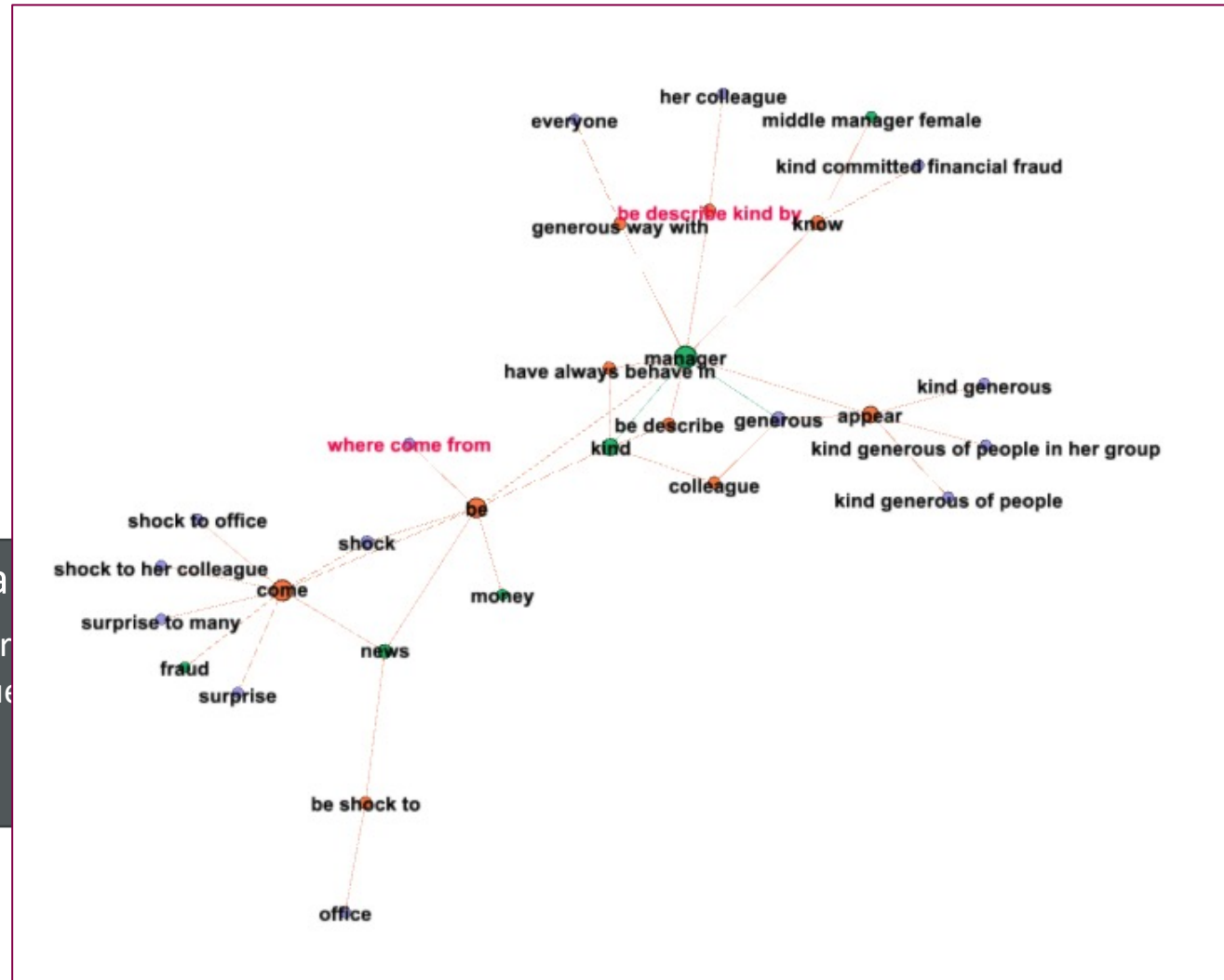


insider

ndly -
bypass

security controls

Answering questions



Behavioural

- Claimed a large
- Possible issues with gambling

the insider

friendly -

to bypass

tools

Answering questions

Behavioural cl
• Claimed a large in
• Possible issues w
gambling



ck

at was the insider
?
arming + friendly -
wed her to bypass
curity controls

Answering questions

How did they attack?

- By using paper-based records
- Became exempt from the new system

How were they caught?

- Teller noticed a fake check

Behavioural clues?

- Claimed a large inheritance
- Possible issues with gambling

What was the insider like?

- Charming + friendly - allowed her to bypass security controls

Implications



Insider Threat

- New method for mapping out an incident
- New method for extracting insider threat characteristics



Natural Language Processing

- Created new approaches for mapping topic models to existing formal models
- Created a method of classifying documents



Other fields

- Grounded theory and Topic Modelling used together
- Applying a grounded theory model to organic narratives

