Edinburgh Napier UNIVERSITY

School of Computing

Ontology of Online Risk

Demo by David Haynes

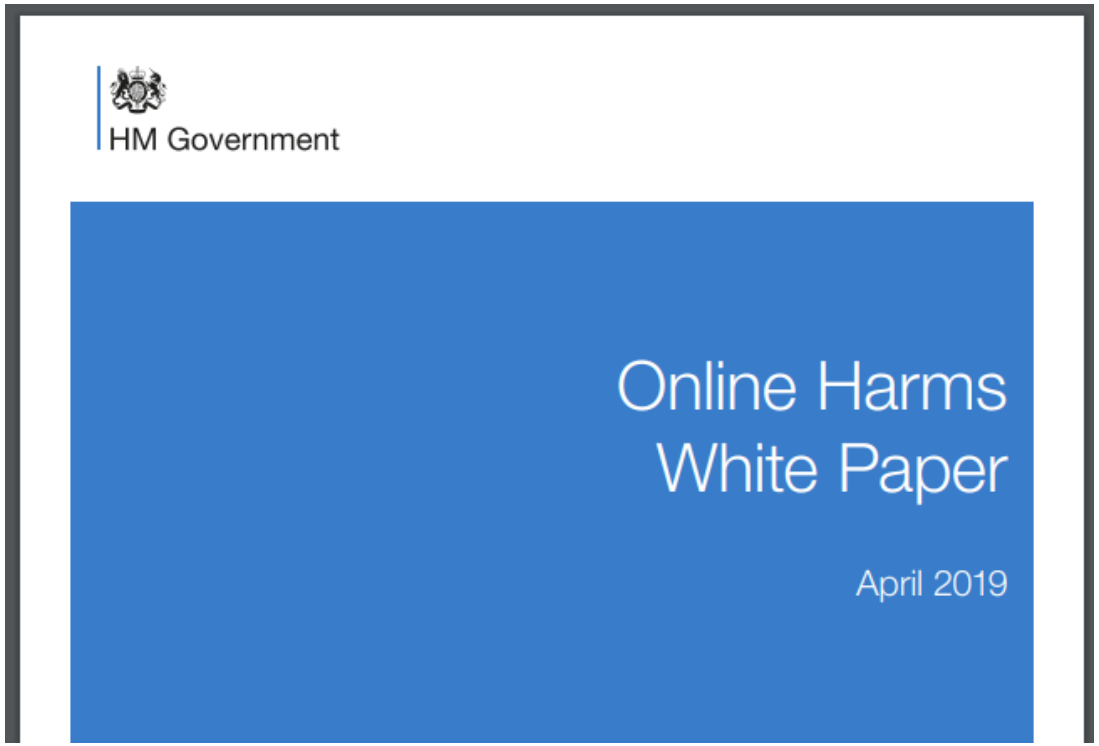
June 2020

Overview

- Background
- Method
- Risk model
- Ontology demo
- Further work
- Potential applications
- Questions
- Acknowledgement

Background

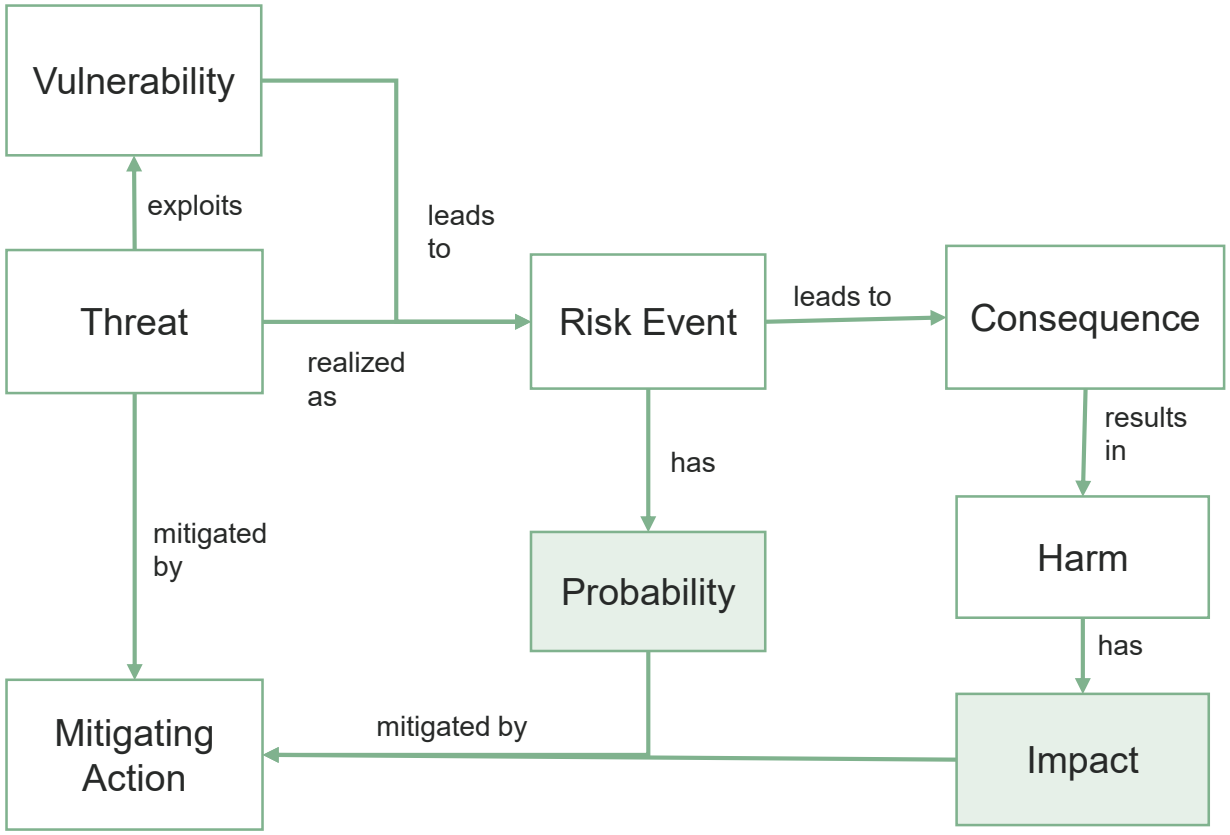
- Concern about online safety
- A number of initiatives by ICO, Police forces and DCMS
- Shift of focus from corporate risk to individual risk
- Privacy calculus – individual assessment of benefits versus risks

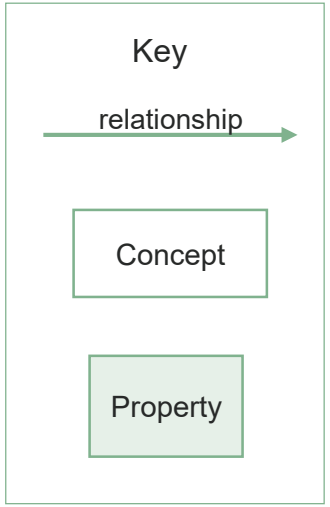


Method

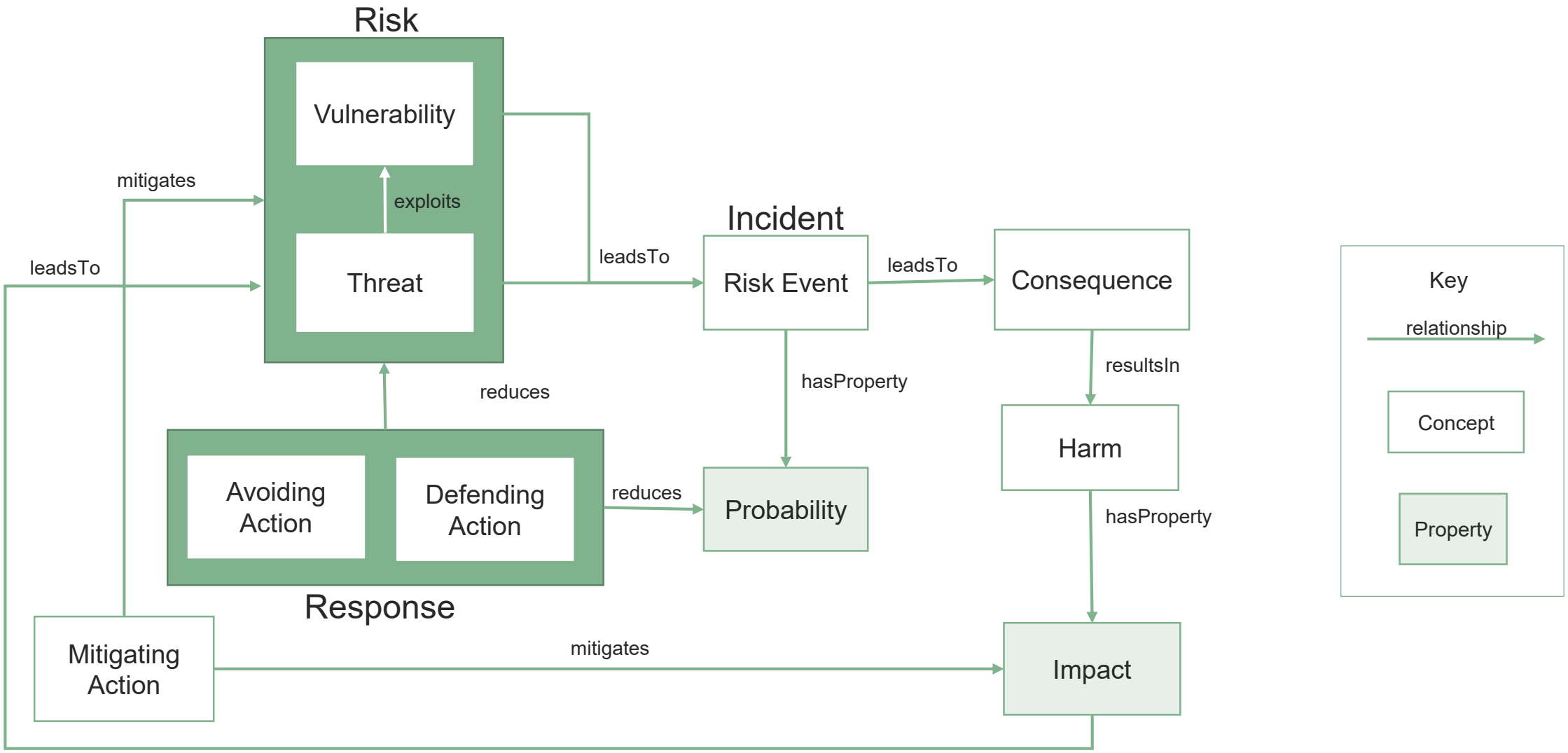
- Identified common risks by monitoring individual online use
- Used this to develop a scope for the ontology
- Imported existing terminology and definitions
- Developed scenarios where individuals are exposed to online risk
- Created relationships between different elements of risk
- Tested scenarios in a workshop and modified the ontology

Modelling Risk





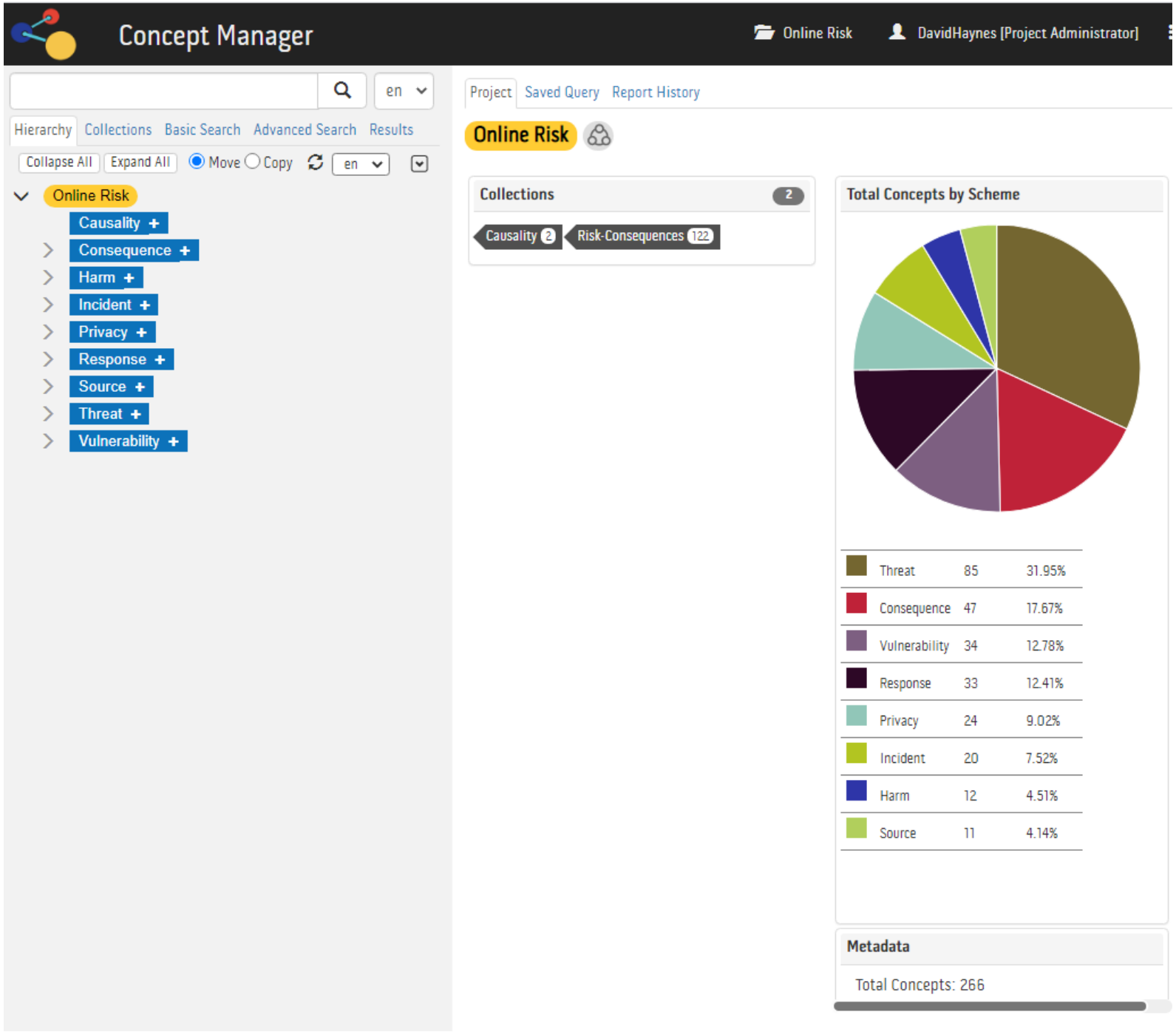
Modified Model



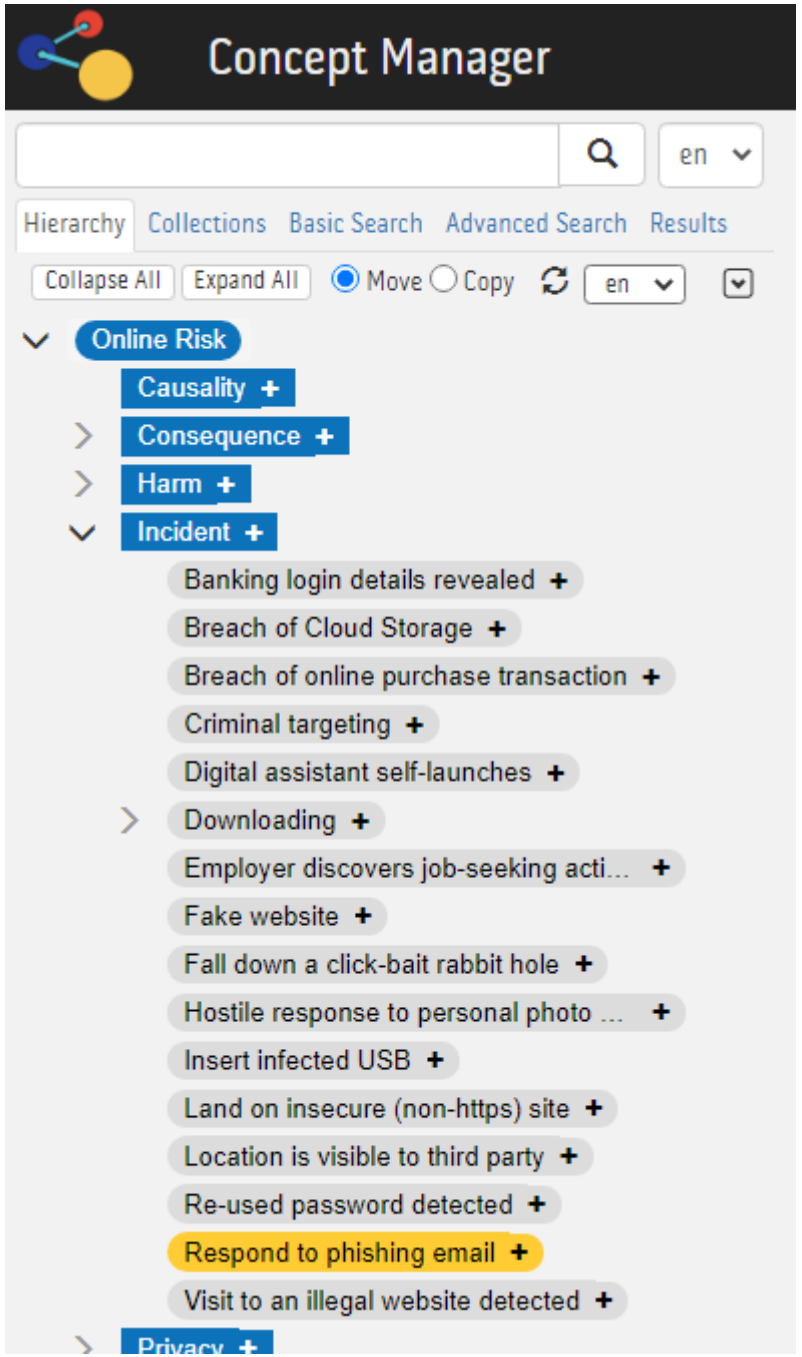
Ontology demo

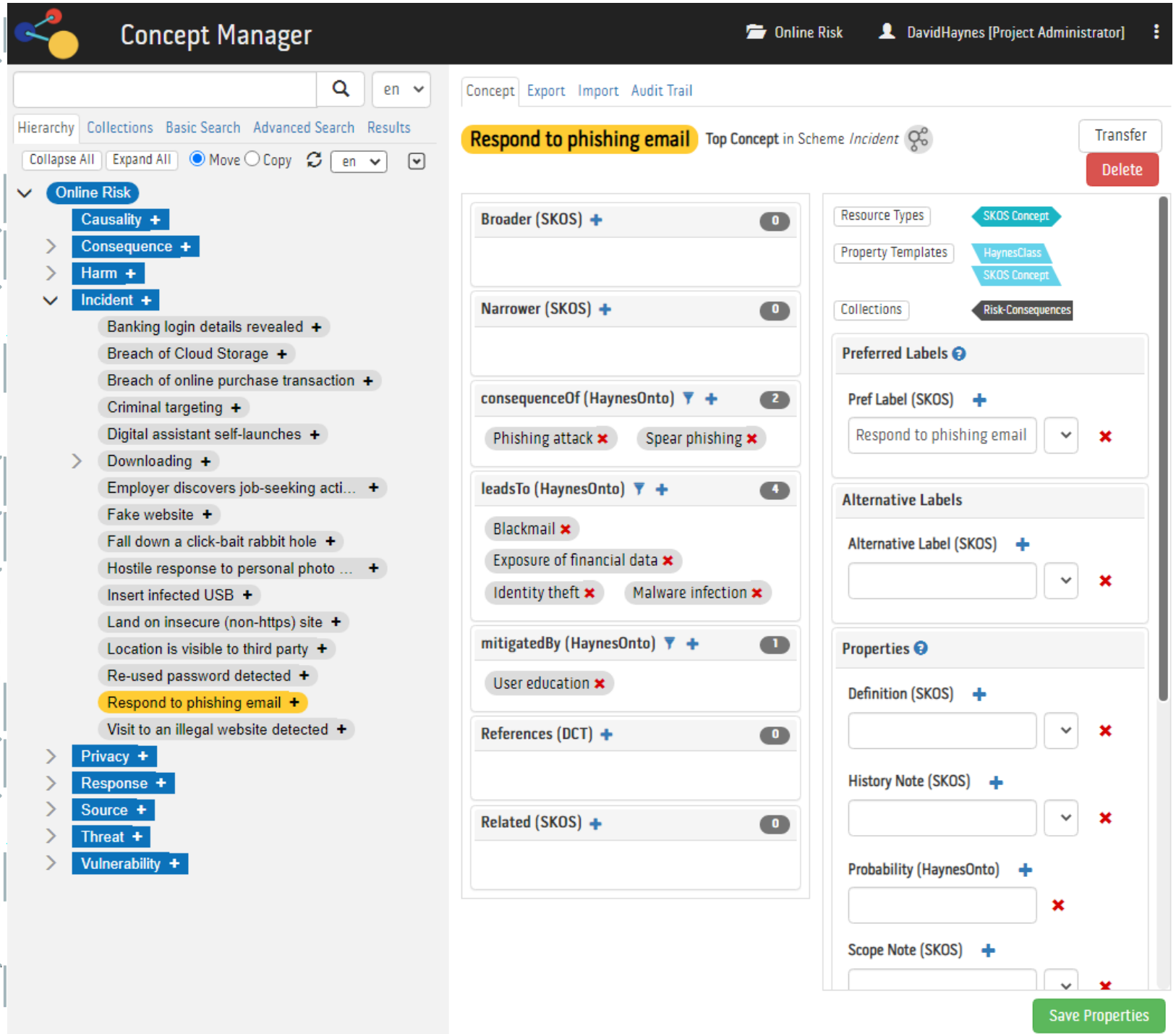
- Using Synaptica's Graphite system


Graphite
Online Risk
DavidHaynes [Project Administrator]
Online Risk

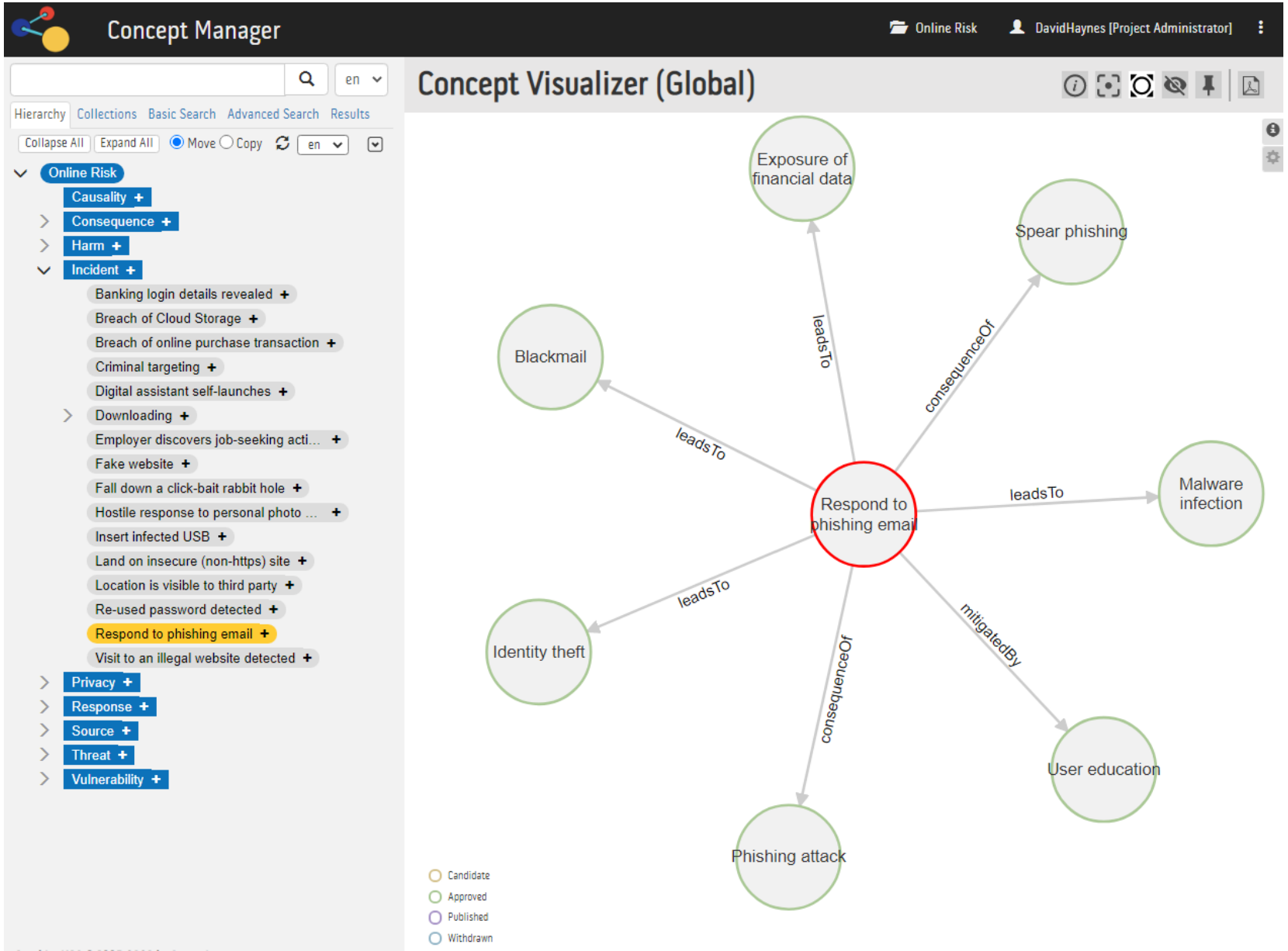


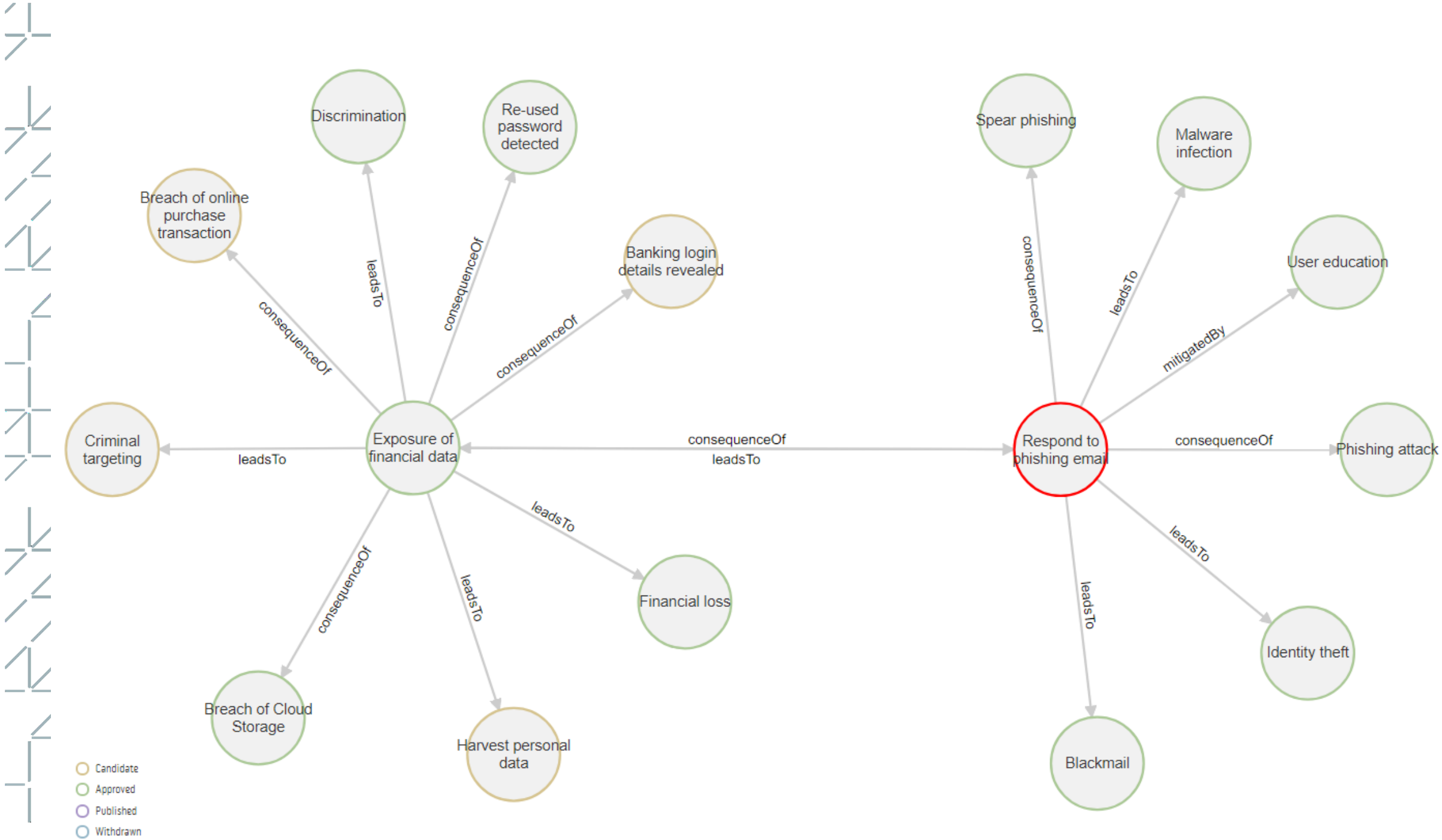
Edinburgh Napier UNIVERSITY | School of Computing

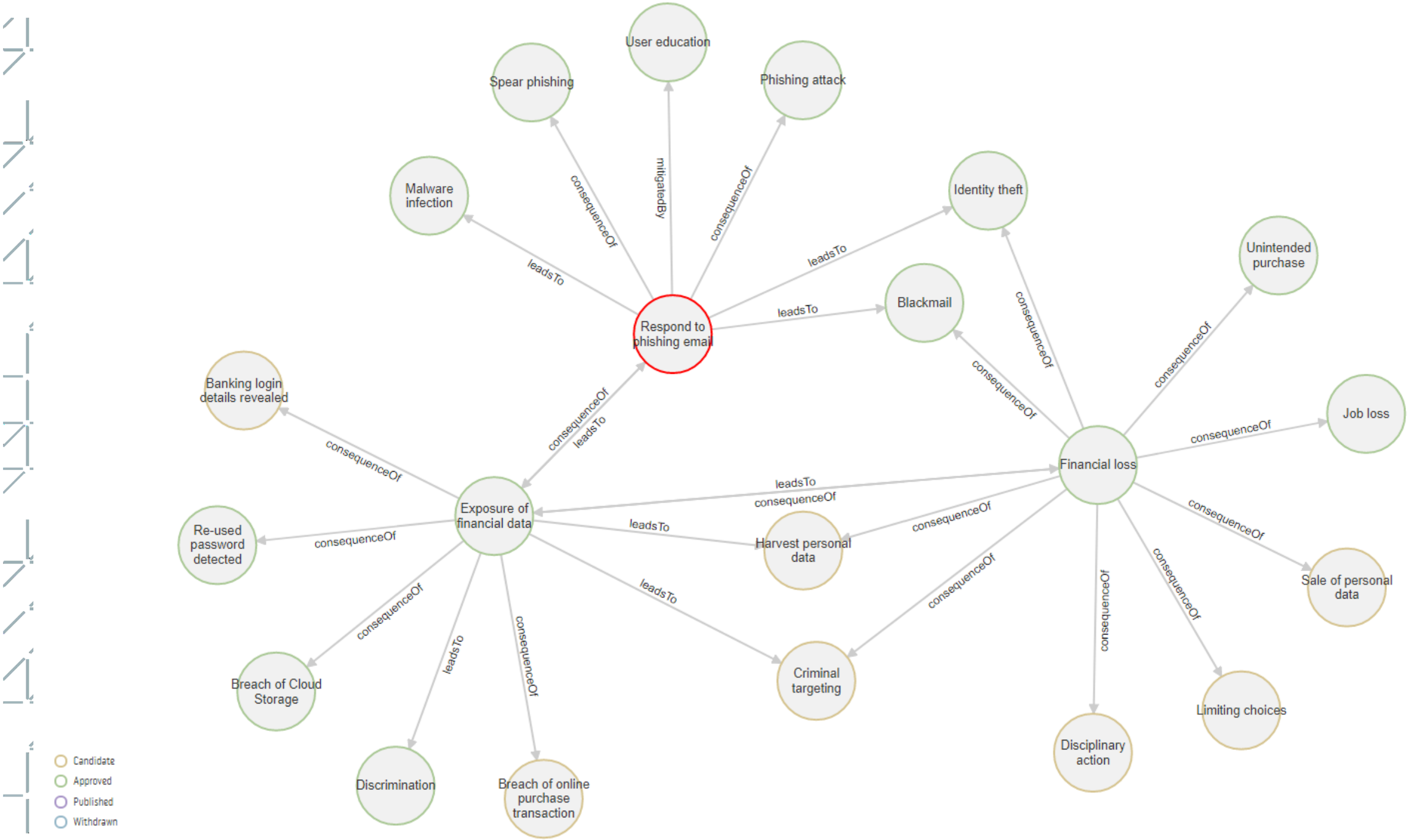

Concept Manager
en
Hierarchy
Collections
Basic Search
Advanced Search
Results
Collapse All
Expand All
Move
Copy
en
Online Risk
Causality +
Consequence +
Harm +
Incident +
Banking login details revealed +
Breach of Cloud Storage +
Breach of online purchase transaction +
Criminal targeting +
Digital assistant self-launches +
Downloading +
Employer discovers job-seeking acti... +
Fake website +
Fall down a click-bait rabbit hole +
Hostile response to personal photo ... +
Insert infected USB +
Land on insecure (non-https) site +
Location is visible to third party +
Re-used password detected +
Respond to phishing email +
Visit to an illegal website detected +
Privacy +

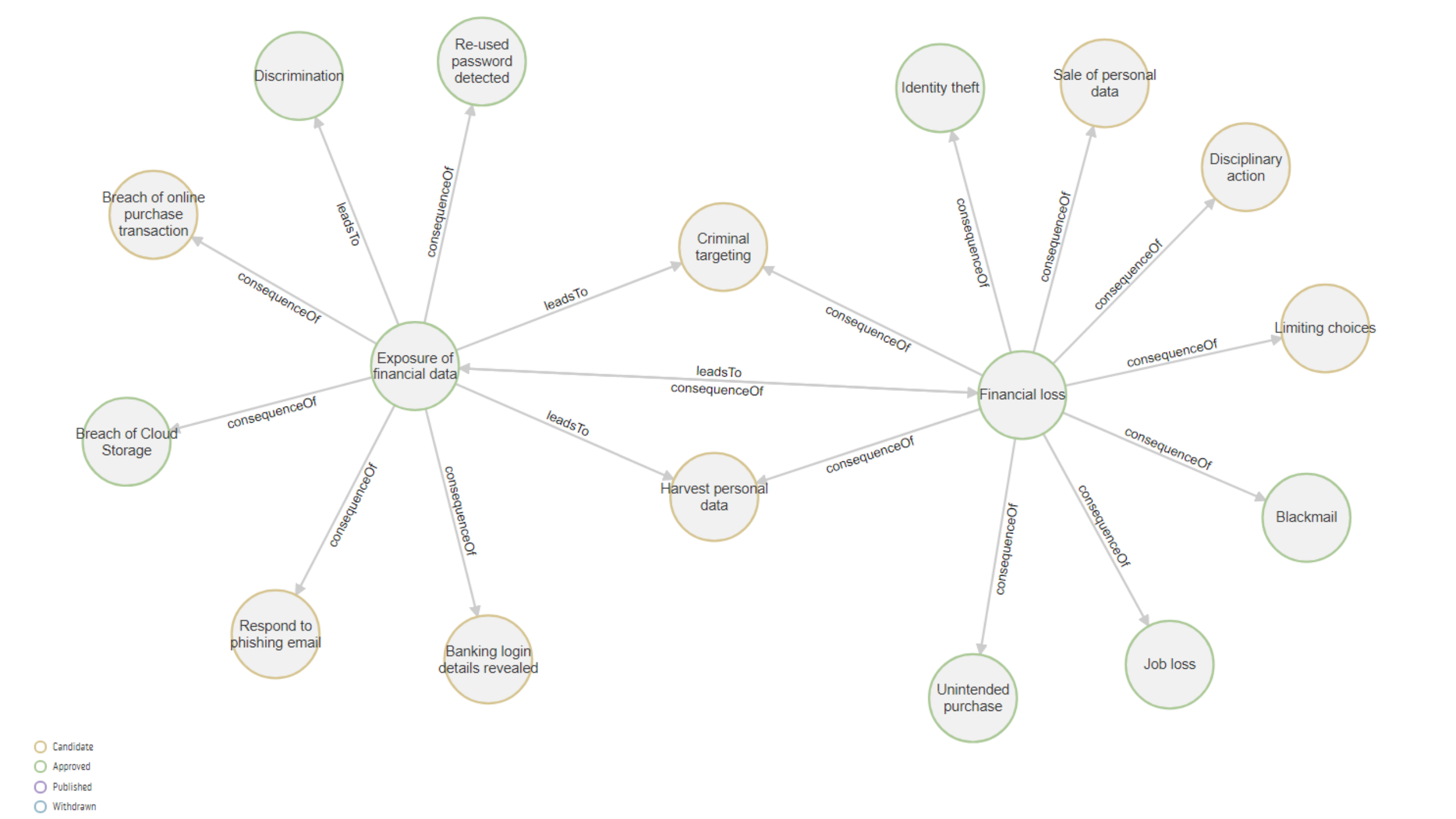


Edinburgh Napier UNIVERSITY | School of Computing

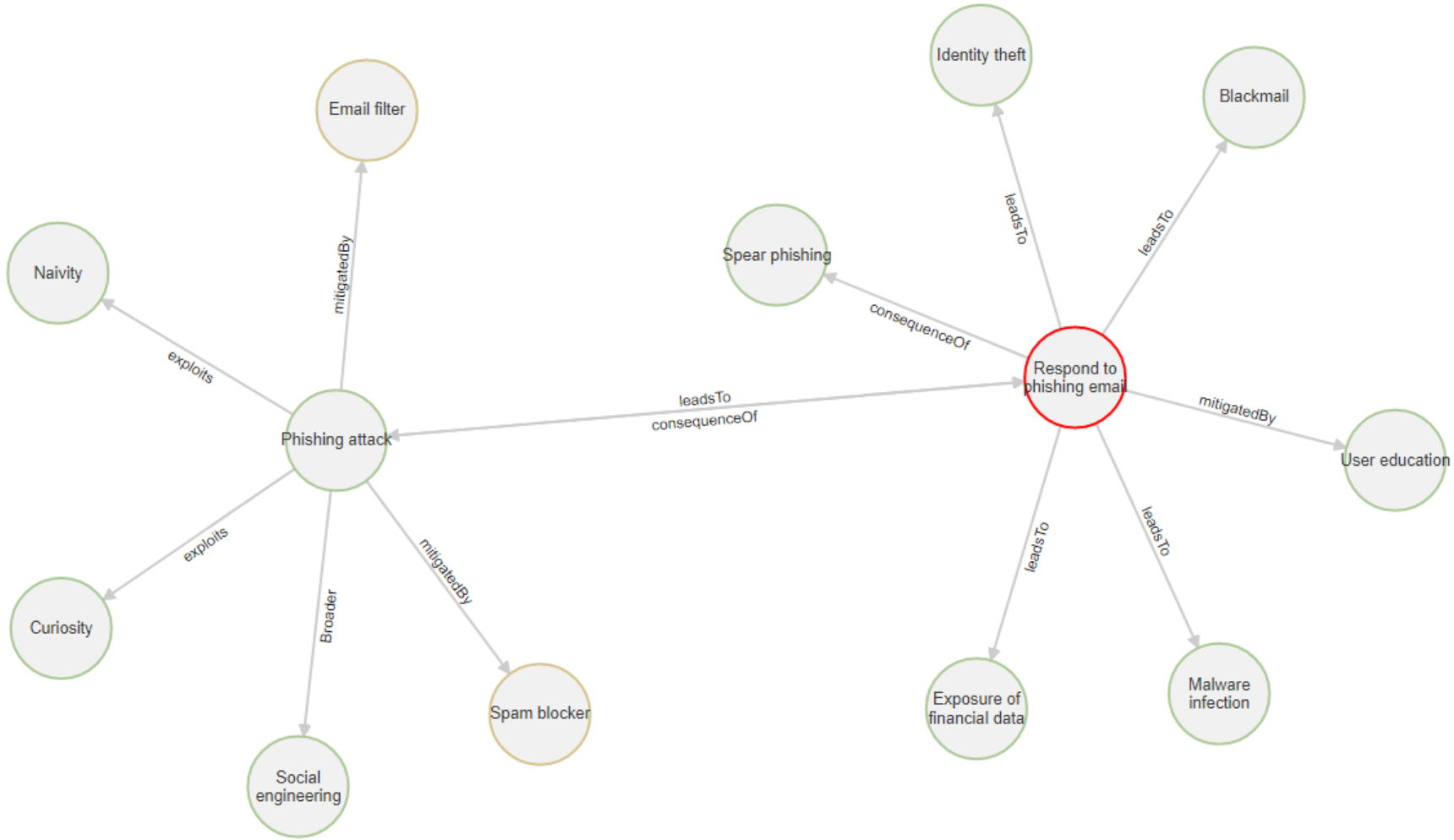

Concept Manager
Online Risk
DavidHaynes [Project Administrator]
en
Hierarchy
Collections
Basic Search
Advanced Search
Results
Collapse All
Expand All
Move
Copy
Online Risk
Causality
Consequence
Harm
Incident
Banking login details revealed
Breach of Cloud Storage
Breach of online purchase transaction
Criminal targeting
Digital assistant self-launches
Downloading
Employer discovers job-seeking acti...
Fake website
Fall down a click-bait rabbit hole
Hostile response to personal photo ...
Insert infected USB
Land on insecure (non-https) site
Location is visible to third party
Re-used password detected
Respond to phishing email
Visit to an illegal website detected
Privacy
Response
Source
Threat
Vulnerability
Concept Visualizer (Global)
Exposure of financial data
Spear phishing
Blackmail
leadsTo
consequenceOf
leadsTo
Respond to phishing email
leadsTo
Malware infection
leadsTo
Identity theft
consequenceOf
mitigatedBy
User education
Phishing attack
Candidate
Approved
Published
Withdrawn


Discrimination
Re-used password detected
Breach of online purchase transaction
Banking login details revealed
Spear phishing
Malware infection
User education
Criminal targeting
Exposure of financial data
Respond to phishing email
Phishing attack
Financial loss
Breach of Cloud Storage
Harvest personal data
Identity theft
Blackmail
leadsTo
consequenceOf
mitigatedBy
Candidate
Approved
Published
Withdrawn

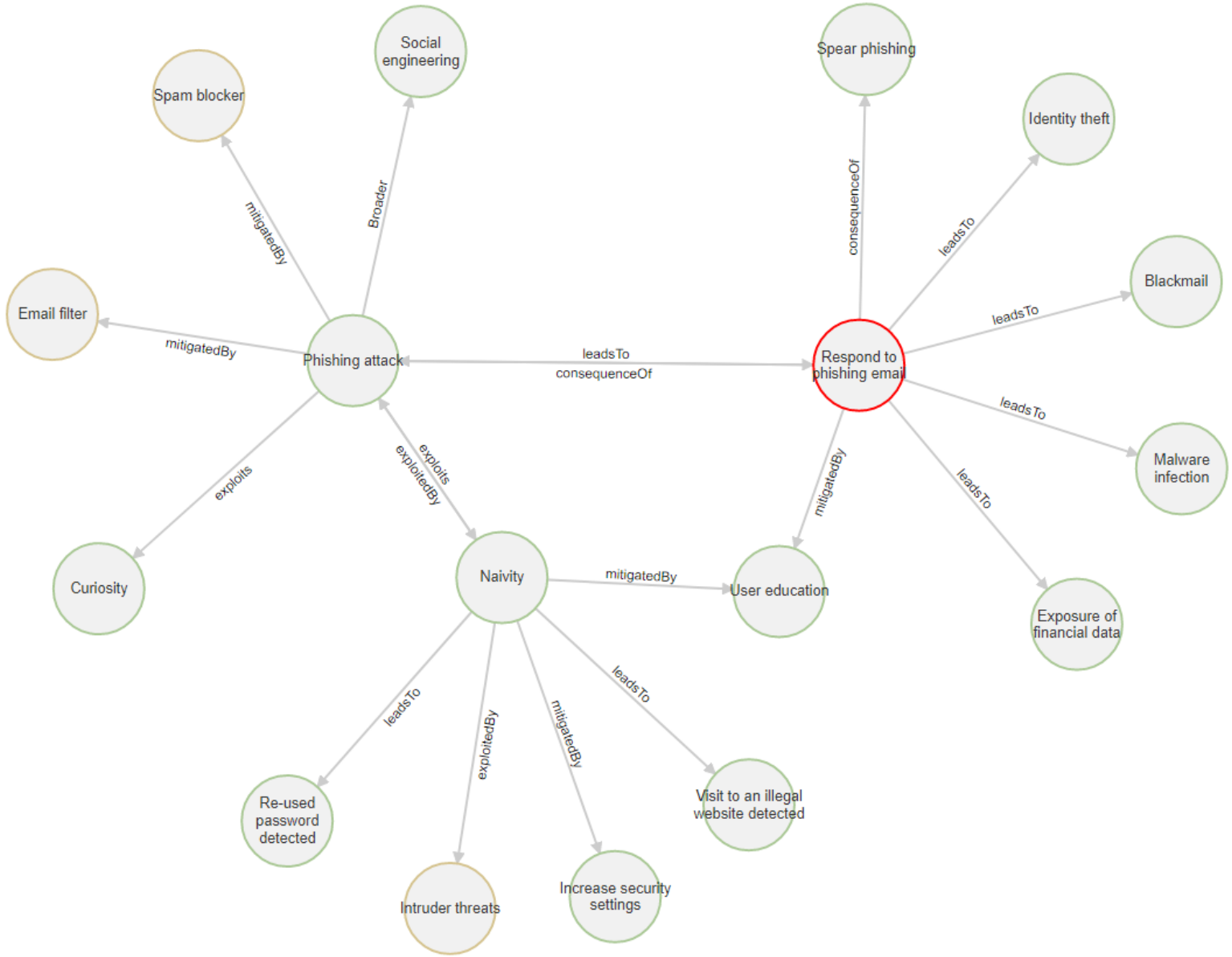

User education
Spear phishing
Phishing attack
Malware infection
consequenceOf
mitigatedBy
consequenceOf
leadsTo
leadsTo
Identity theft
Unintended purchase
Respond to phishing email
leadsTo
Blackmail
consequenceOf
consequenceOf
consequenceOf
Banking login details revealed
consequenceOf
leadsTo
consequenceOf
Job loss
Financial loss
consequenceOf
leadsTo
consequenceOf
Exposure of financial data
consequenceOf
Re-used password detected
leadsTo
Harvest personal data
consequenceOf
consequenceOf
Sale of personal data
consequenceOf
leadsTo
consequenceOf
consequenceOf
Breach of Cloud Storage
leadsTo
consequenceOf
Criminal targeting
consequenceOf
consequenceOf
Limiting choices
Discrimination
Breach of online purchase transaction
Disciplinary action
Candidate
Approved
Published
Withdrawn


Discrimination
Re-used password detected
Breach of online purchase transaction
leadsTo
consequenceOf
consequenceOf
Criminal targeting
leadsTo
Exposure of financial data
consequenceOf
Breach of Cloud Storage
leadsTo
consequenceOf
leadsTo
consequenceOf
consequenceOf
Harvest personal data
Respond to phishing email
Banking login details revealed
Identity theft
Sale of personal data
Disciplinary action
consequenceOf
consequenceOf
consequenceOf
Limiting choices
consequenceOf
Financial loss
consequenceOf
consequenceOf
consequenceOf
consequenceOf
Blackmail
Unintended purchase
Job loss
Candidate
Approved
Published
Withdrawn


Phishing attack
Exposure of financial data
consequenceOf
leadsTo
Blackmail
leadsTo
Respond to phishing email
Malware infection
leadsTo
consequenceOf
mitigatedBy
leadsTo
Identity theft
Spear phishing
User education


Email filter
Naivity
mitigatedBy
exploits
Phishing attack
leadsTo
consequenceOf
Identity theft
Blackmail
Spear phishing
leadsTo
leadsTo
consequenceOf
Respond to phishing email
mitigatedBy
User education
exploits
Curiosity
Broader
mitigatedBy
Spam blocker
Social engineering
leadsTo
leadsTo
Exposure of financial data
Malware infection

Edinburgh Napier UNIVERSITY | School of Computing



Further work

- Further development of the risk model
- Making the ontology available and discoverable
- Integration with high-level ontologies such as the Basic Fundamental Ontology
- Population of the ontology with instances using linked open data sets
- Explore strengths of relationships and associations between concepts in a populated ontology

Potential applications

- Identify commonalities between incidents
- Facilitate responses based on common characteristics
- Inform policy-making
- Better understanding for estimating risk probability and impact

Edinburgh Napier UNIVERSITY | School of Computing

Acknowledgement

This research was supported by the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Fellowship Programme (Grant No. ICRF1718\1\54)

The work was conducted at the Centre for Information Science at City, University of London

Synaptica LLC provided their Graphite platform for the development and presentation of this ontology

Edinburgh Napier UNIVERSITY

School of Computing

Thank you!

Blog: davidhaynes.co.uk

Twitter: jdavidhaynes

Email: d.haynes@napier.ac.uk