



Open Information Security Risk Universe

Robin Oldham & Phil Huggins & Petra Vukmirovic
Cydea & CISO Mentor & Glasswall



Objectives of this session

1. Introduction to the *Open Information Security Risk Universe*
2. Apply the OISRU to previous incidents
3. Explore other use cases

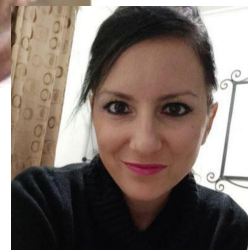
 [Follow along on Twitter](#)



Phil Huggins
[@oracuk](#) / [LinkedIn](#)
CISO Mentor



Robin Oldham
[@RTO](#) / [LinkedIn](#)
Cydea



Petra Vukmirovic
[@PetraVuk1311](#) / [LinkedIn](#)
Glasswall



CISO Mentor

cydea



AUDIENCE PARTICIPATION AHEAD



The plan...

- 14:00 What's the universe?
- What problem are we solving?
 - OISRU Components
 - Use case: Risk statements vs risk scenarios
- 14:30 Putting it into practice
- Group exercise
 - Present back
- 15:00 Other use cases
- Risk coverage
 - Bow tie diagrams
 - Graphs!
- 15:40 Questions & feedback



A tall, white lighthouse with a black band around its upper section stands on a grassy hill. The lighthouse is illuminated from within, casting a warm glow. To its right is a small, white, single-story building with a red roof. In the background, the Milky Way galaxy is visible in the dark blue night sky, along with numerous stars. A tall, thin antenna or mast extends from the right side of the hill into the sky. The overall scene is serene and evokes a sense of exploration and discovery.


RISK SPACE THE FINAL FRONTIER

Example risk register

ID	Risk	Impact	Likelihood	...
1	The data loss prevention system may fail	HIGH	LOW	...
2	Third-party risk	MED	MED	...
3	Our SIEM solution is not following best practice	LOW	MED	...
4	Enormous GDPR fine	LOW	LOW	...
5	APT	HIGH	MED



Example risk register

ID	Risk	Impact	Likelihood	...
1	The data loss prevention system may fail	HIGH	LOW	...
2	Third-party risk ...and?	MED	MED	...
3	Our SIEM solution is not following best practice	LOW	MED	...
4	Enormous GDPR fine	LOW	LOW	...
5	APT!!!111one 	HIGH	MED

These are control failures



Consequence / risk factor

Threat actor != risk scenario!

C-



Problem?

- Huge, unmanageable risk registers
- Poor risk statements
- Difficult to compare
- Difficult to check coverage



OPEN INFORMATION SECURITY RISK UNIVERSE

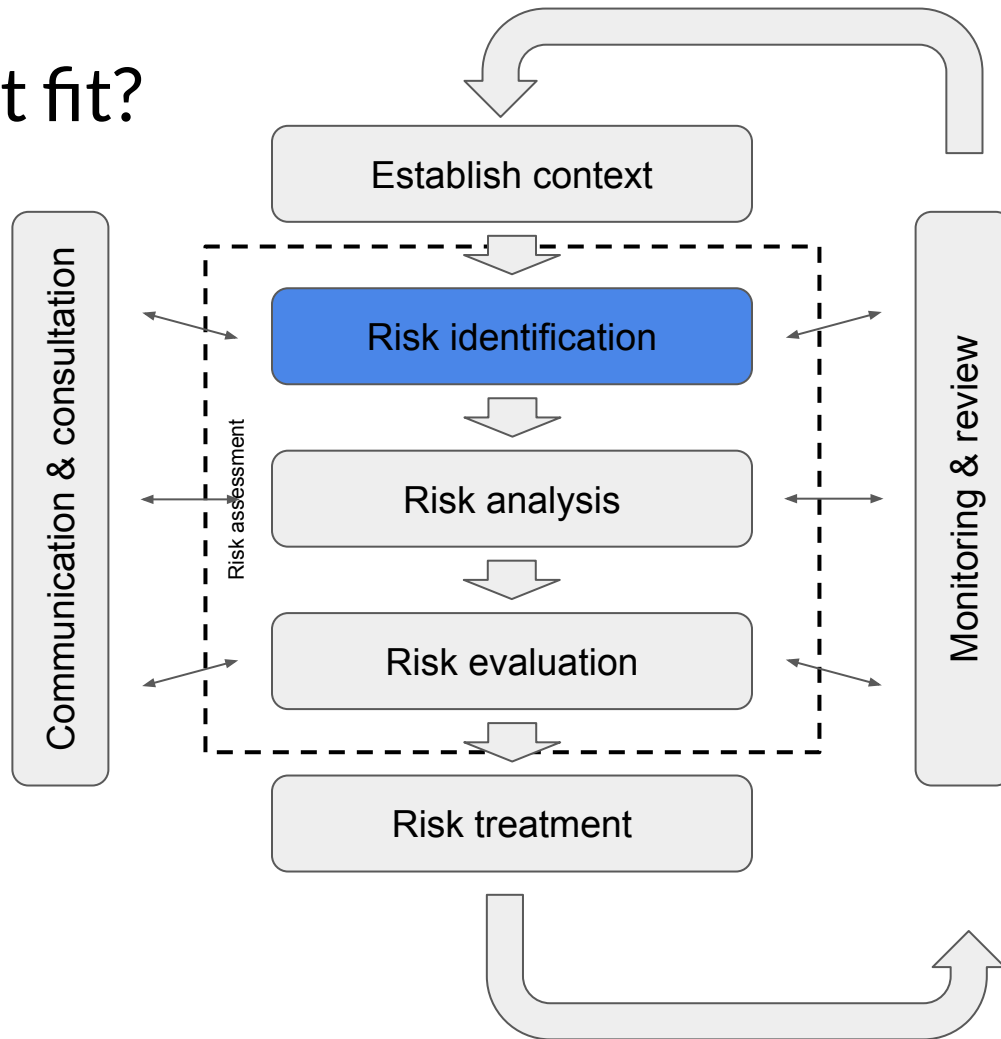
(OISRU)



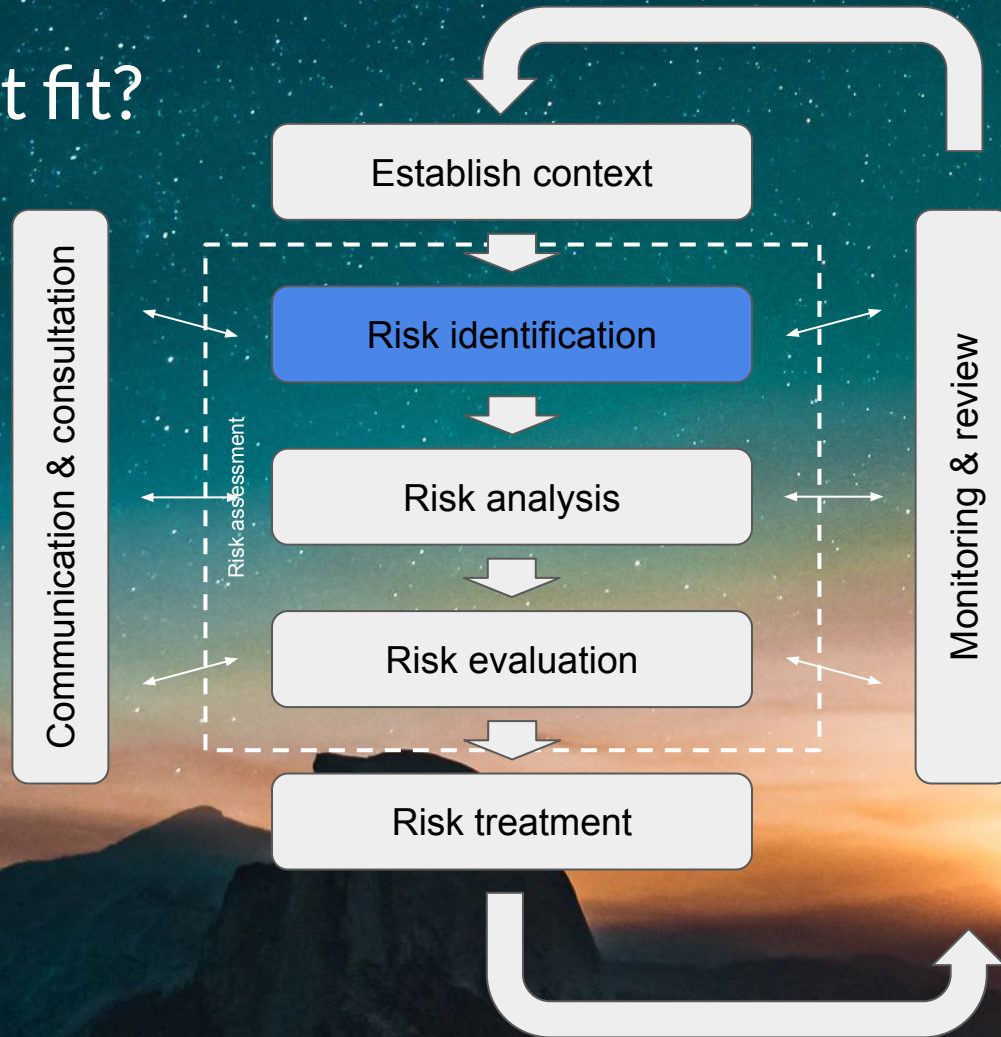
A framework for budding astronauts infosec pros to explore risk



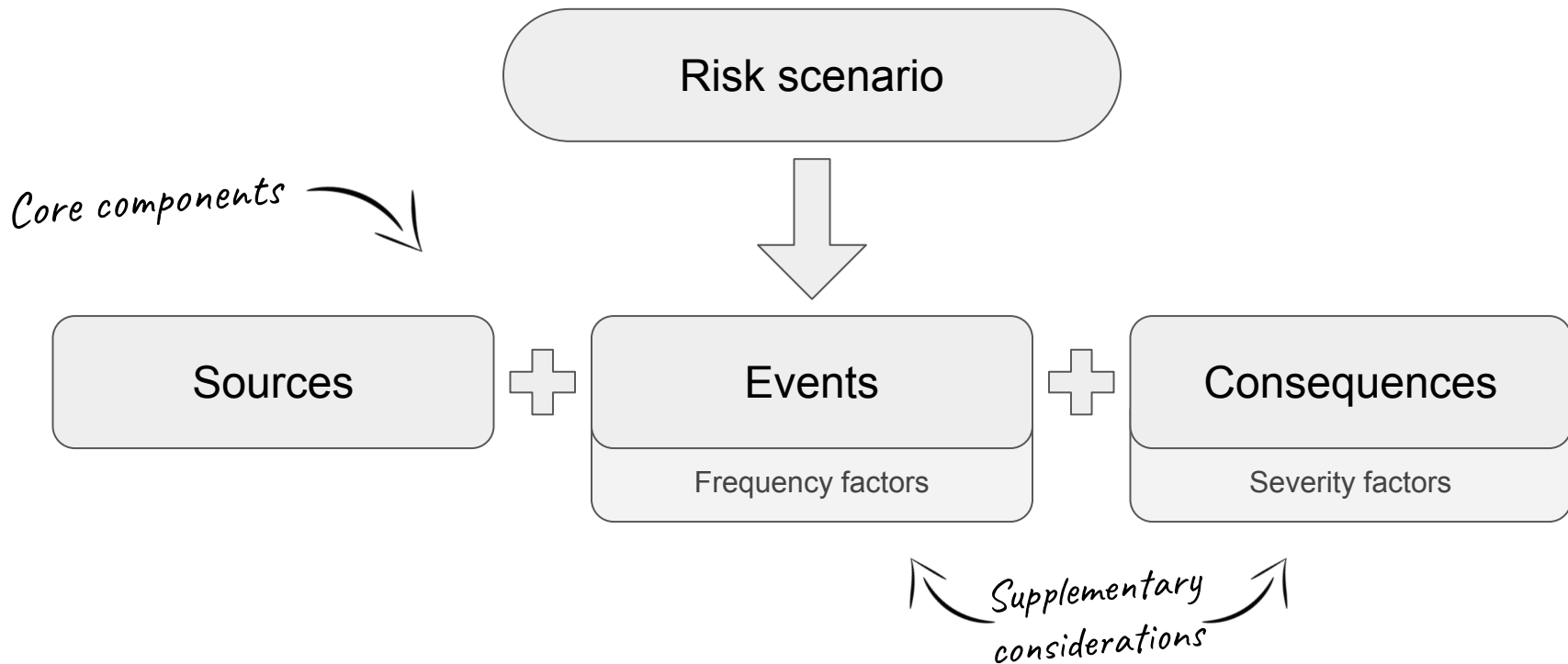
Where does it fit?



Where does it fit?



Risk statement components



Risk statement components

Sources 

Source	Internal/External	Malicious/Non-Malicious
Disgruntled	Internal	Malicious
Accidental	Internal	Non-Malicious
Ineffective	Internal	Non-Malicious
Criminal	Internal	Malicious
Coerced	Internal	Malicious
Criminals	External	Malicious
Hacktivists	External	Malicious
Compromised suppliers	External	Non-Malicious
State-Sponsored	External	Malicious
Competitor	External	Malicious
Press	External	Non-Malicious
Researcher	External	Non-Malicious
Regulator	External	Non-Malicious

Events 

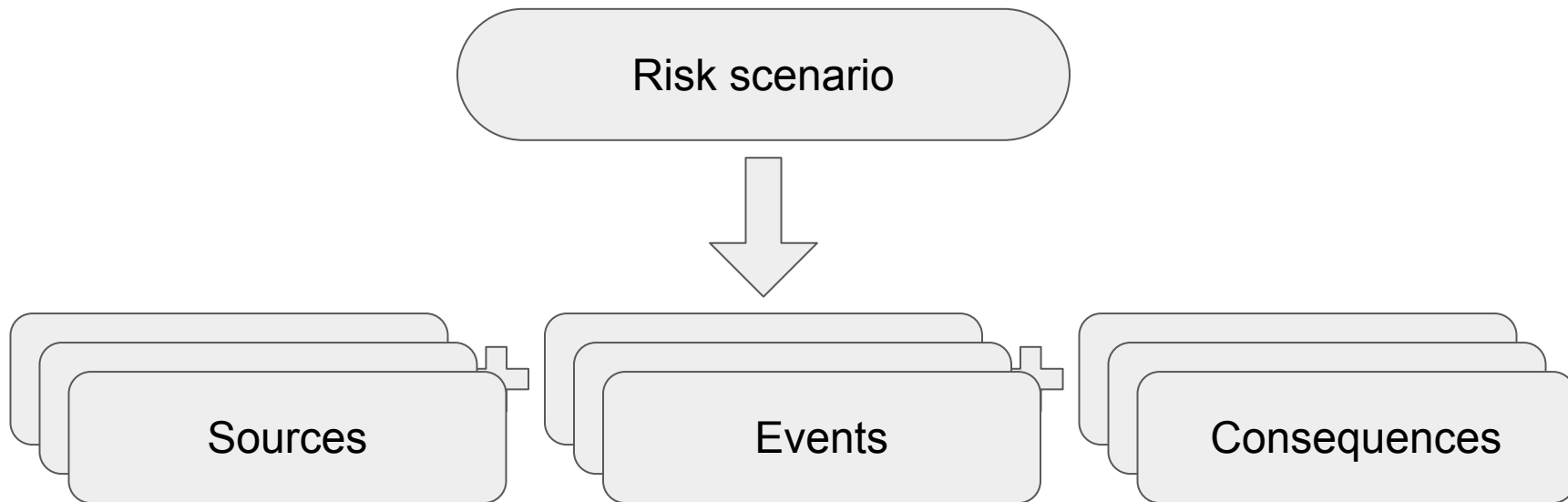
Level 1	Level 2	CIA
Abusive Content	Harmful Speech	
	Child / Sexual / Violent Content	
	Harassment	
Malware	Ransomware	Availability
	Worm	Confidentiality, Integrity, Availability
	Spyware	Confidentiality
	Rootkit	Confidentiality, Integrity, Availability
	Dialler	
Availability Interruption	Distributed / Denial of Service	Availability
	Sabotage	Integrity, Availability
Information Gathering	Open Source Intelligence Analysis	Confidentiality
	Network Scanning	

Consequences 

Level 1 Consequences	Level 2 Consequences
Operations	Reduced growth
	Business Disruption
	Ineffective Change
	Slow recovery
	Reduced access to staff / skills
	Loss of suppliers
	Environmental harm
	Safety failure
	Social harm
	Medical harm
Compliance	Non-compliance
	Poor conduct / integrity



May not be singular!



What are the use cases?

- Writing (good!) risk statements and drafting risk scenarios
- Creating 'bow tie' diagrams
- Checking coverage of risk assessment
- Graphing...

You tell us! 🙏 @RTO @oracuk



CISO Mentor

cydea

Risk scenarios vs risk statements

Risk scenarios

- Provide business-context
- Narrative form
- Stakeholder communication

Risk statements

- Provide structure
- Aids easy comparison
- Practitioner communication

Aid the understanding, in the same way as [threat personas](#) do with the actors.



Risk scenarios vs risk statements

Risk scenarios

Accidental market sensitive information leak

During the reporting period a member of the accounting team, under time pressure, accidentally sends a draft of the annual report to an employee at our technology outsourcer who has the same name as our Chief Financial Officer as a result of address auto-complete in their email software. If the draft leaks it could lead to market sensitive information being published ahead of the publication of the report which could lead to a regulatory sanction and trigger insider trading investigation.

Risk statements

Employee
+
Information Breach
+
Regulatory Fine
Damaged Regulator Relations

Your turn! ↘

We're putting you into **groups**

Each gets a different **historic security incident**

Put yourself in the risk manager's shoes, *prior* to the event...
reverse engineer it and **write a risk statement + scenario**

Open this: [OSS2020 - OISRU Activity Slides](#)

And this: [oisru.org](#)

(links in chat)



(Groups present back activity slides)



(*Phew* short break... Start back 15:10!)



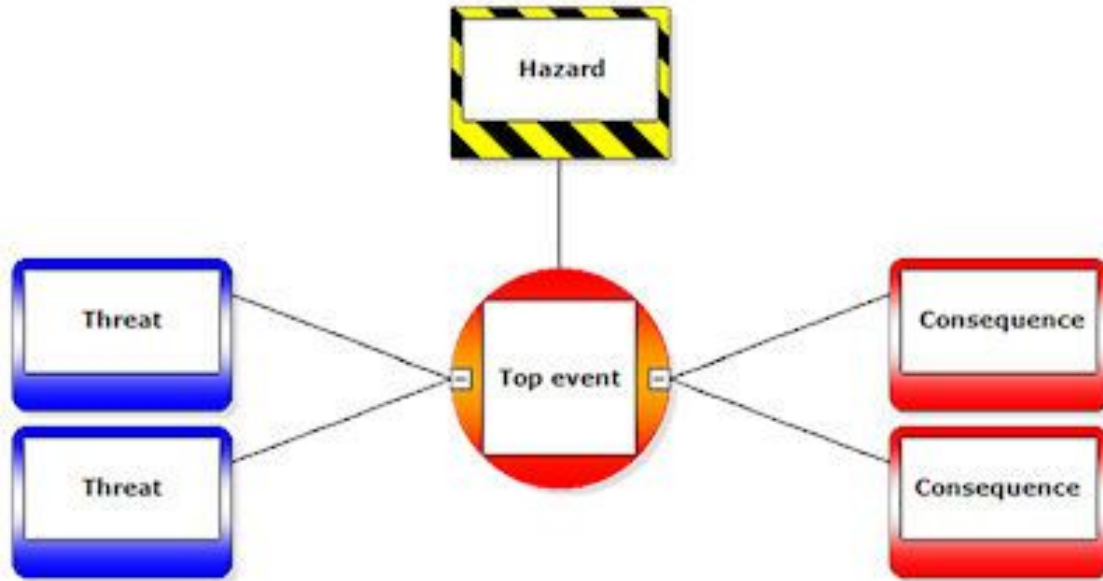
Welcome back!

Three more use cases:

- Bow tie diagrams
- Risk coverage
- Graphs!



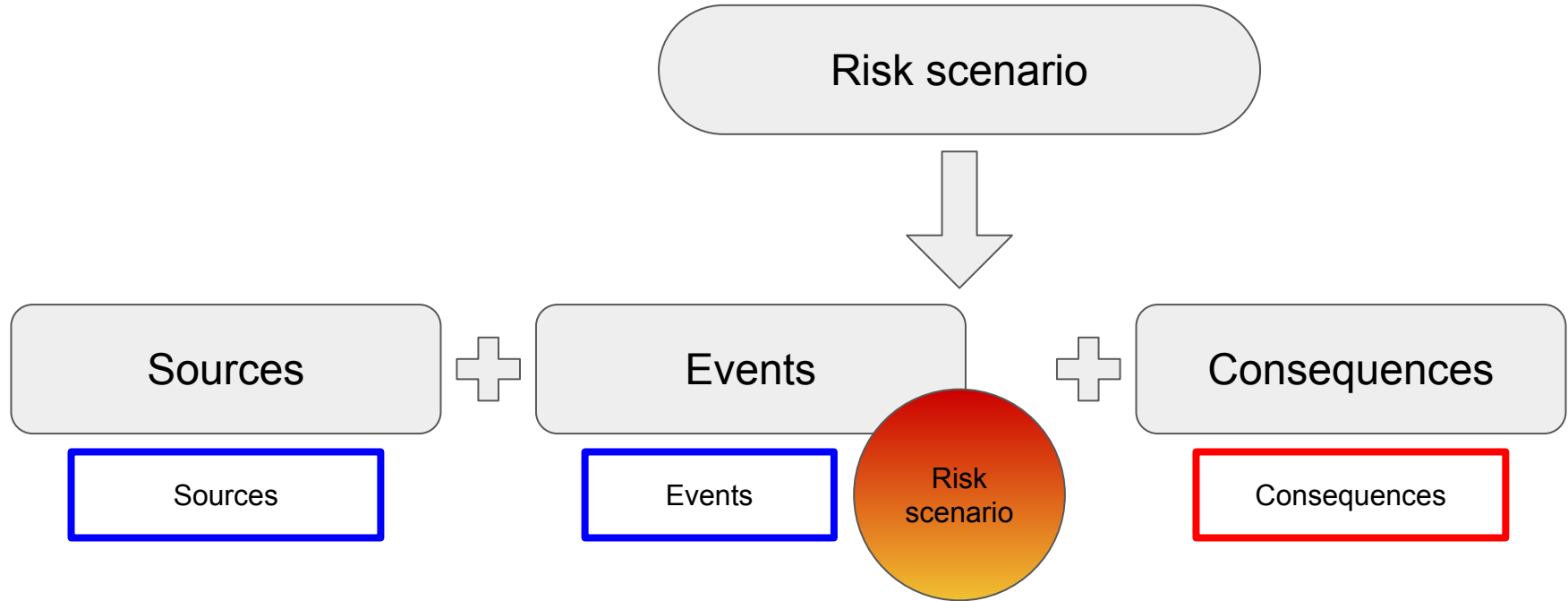
Bow tie diagrams



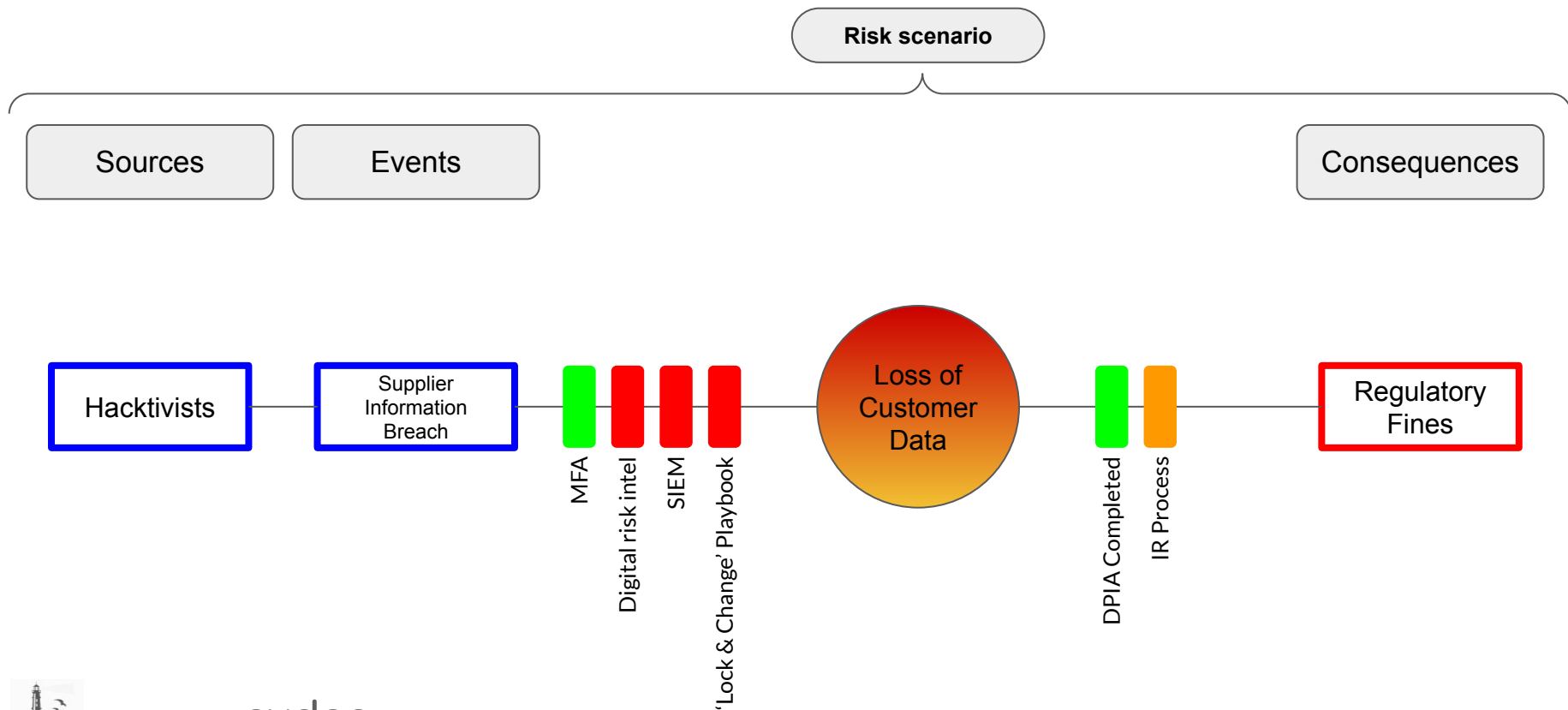
Source: [Civil Aviation Authority](#)



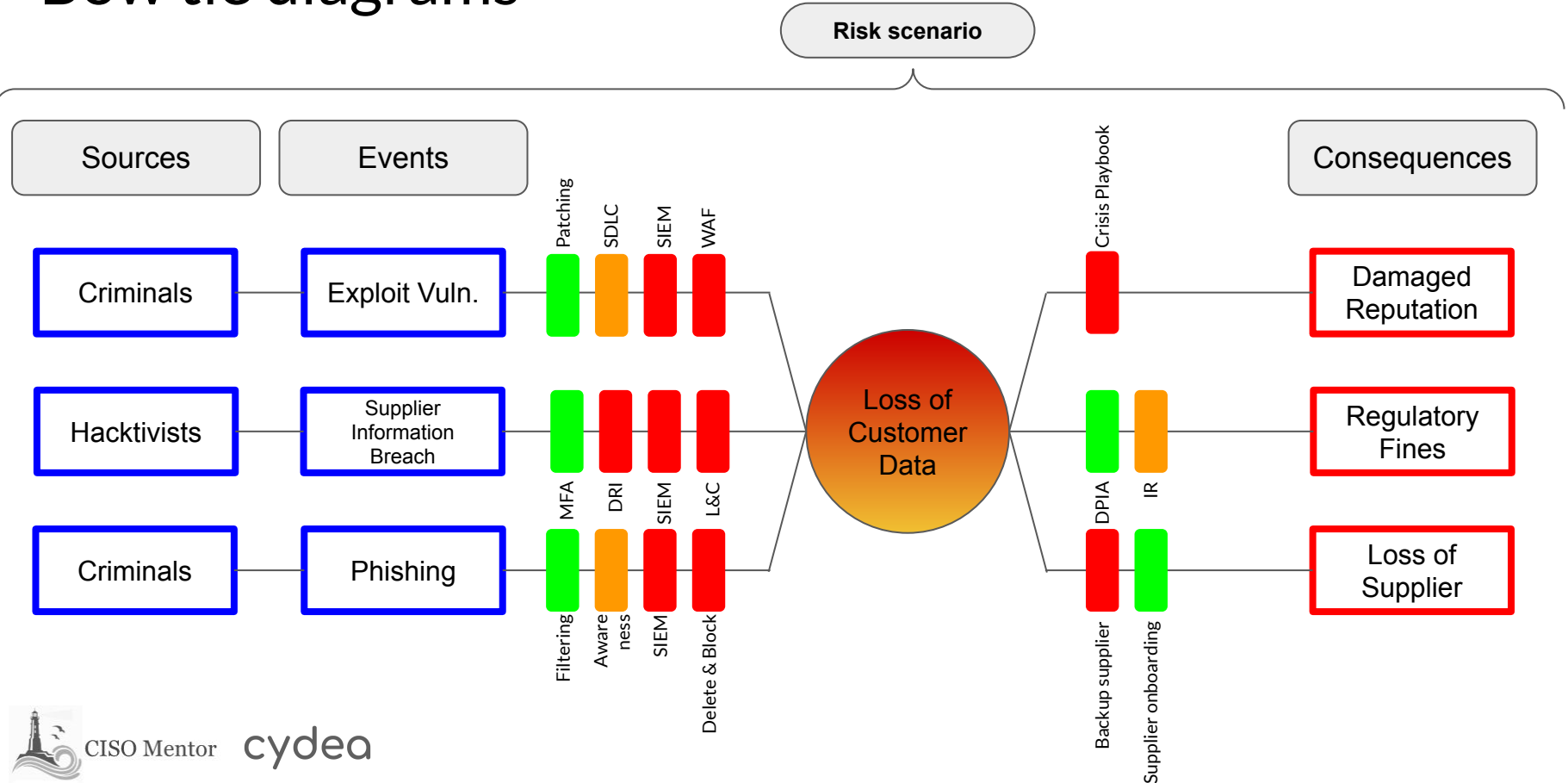
Bow tie diagrams



Bow tie diagrams



Bow tie diagrams



Use case: Risk coverage

Decompose and compare risk

... between statements

... between systems

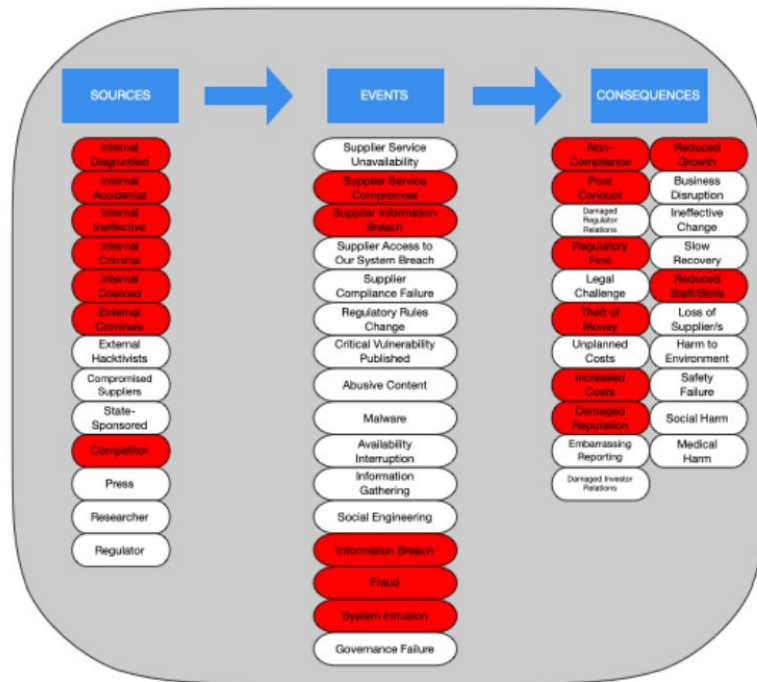
... between business units

Coverage maps

... your 'Top 10' scenarios

... checklist for risk identification

... Useful for auditors (!)



Graphs! All the graphs!

glasswall.atlassian.net/browse/INCIDENT-23?ql=project%20%3D%20INCIDENT

Learning ... Clearly Not Work Azure ML Work and maybe w... Access Panel Applic... https://app.datad... Your applications A... AWS Management... https://www.ishrd...

Info leak

Accid. Empl.

Smart querying activated. Run search without smart query

API Keys Found in gw-proxy.com

INCIDENT-23

has fact

FACT-79

API keys are confidential data and according to Confidential Data policy they need to be encrypted while stored

has fact

FACT-87

No customer data was exposed

has fact

FACT-88

Security Awareness program for developers to be released and implemented from 28th of May 2020

has fact

FACT-89

Automated code review for secrets/keys to be implemented from 25th of May 2020

has fact

FACT-90

The code is not found on any current repo and the API key is no longer valid - incident is contained

is created by

has incident manager

VULNERABLE-3

Visible API key in XHR requests at gw-proxy.com

is vulnerability of

PERSON-78

Petra Vukmirovic

has risk

RISK-6

Exposed API key can enable access to the API causing financial loss (due to unauthorised use without compensation) and reputational loss (client loss of trust as secrets/keys not managed properly)

has incident handler

PERSON-21

Abbas Haidar

Unplanned costs (CON1)

SECRET

draw.io-13.2.2-win...exe
Failed - Download error

Show all

End

Graphs! All the graphs!

glasswall.atlassian.net/browse/INCIDENT-23?ql=project%20%3D%20INCIDENT

Learning ... Clearly Not Work Azure ML Work and maybe w... Access Panel Applic... https://app.dataato... Your applications A... AWS Management... https://www.ishrcd...

Smart querying activated. Run search without smart query

API Keys Found in gw-proxy.com
INCIDENT-23

has fact

API keys are confidential data and according to Confidential Data policy they need to be encrypted while stored
FACT-79

has fact

No customer data was exposed
FACT-87

has fact

Security Awareness program for developers to be released and implemented from 28th of May 2020
FACT-88

has fact

Automated code review for secrets/keys to be implemented from 25th of May 2020
FACT-89

has fact

The code is not found on any current repo and the API key is no longer valid - incident is contained
FACT-90

is created by

Visible API key in XHR requests at gw-proxy.com
VULNERABLE-3

has incident manager

Petra Vukmirovic
PERSON-78

has risk

Exposed API key can enable access to the API causing financial loss (due to unauthorised use without compensation) and reputational loss (client loss of trust as secrets/keys not managed properly
RISK-6

is vulnerability of

has incident handler

Abbas Haidar
PERSON-21

SRC

RISK-6

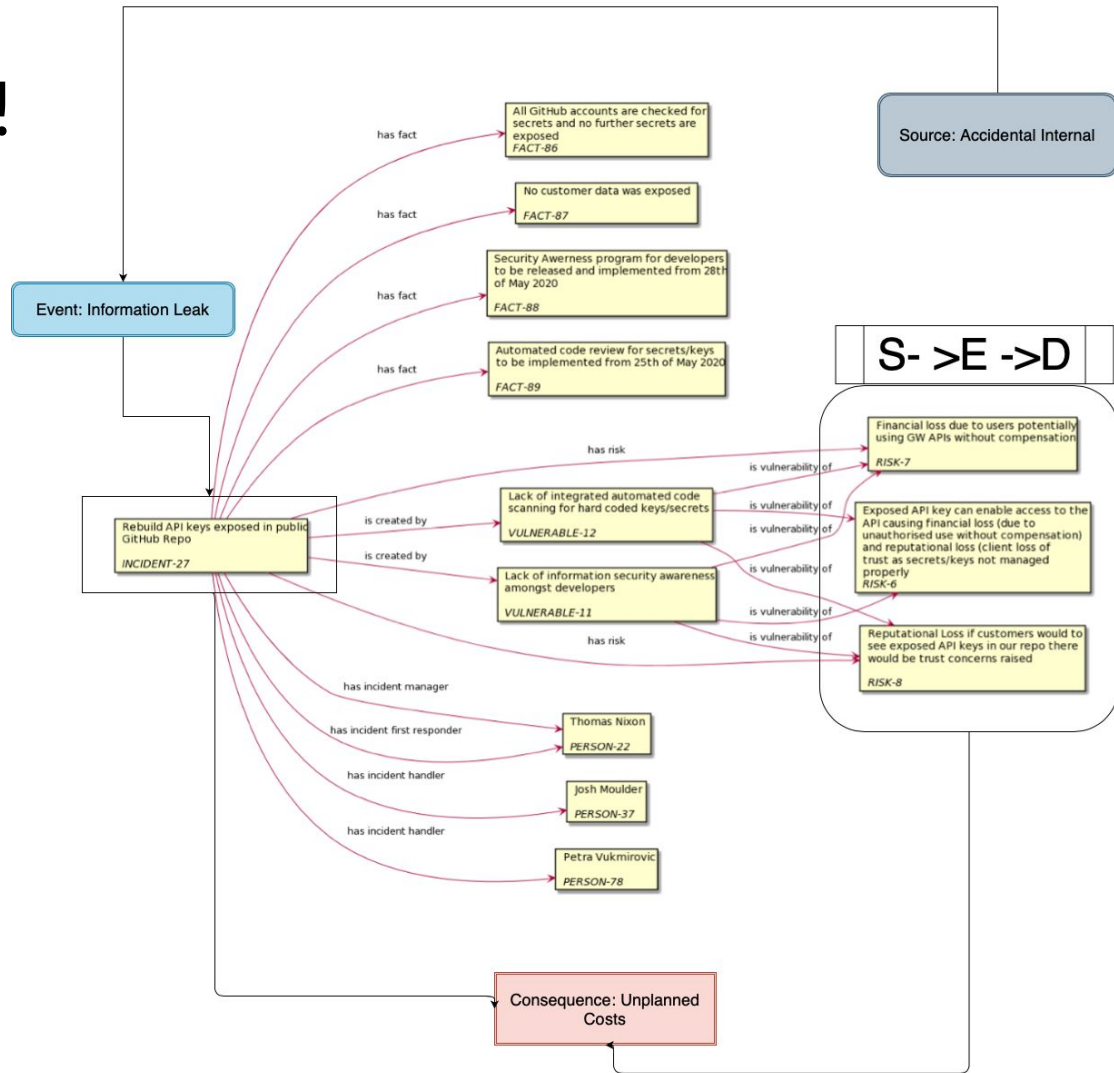
CON.Q

EVENT

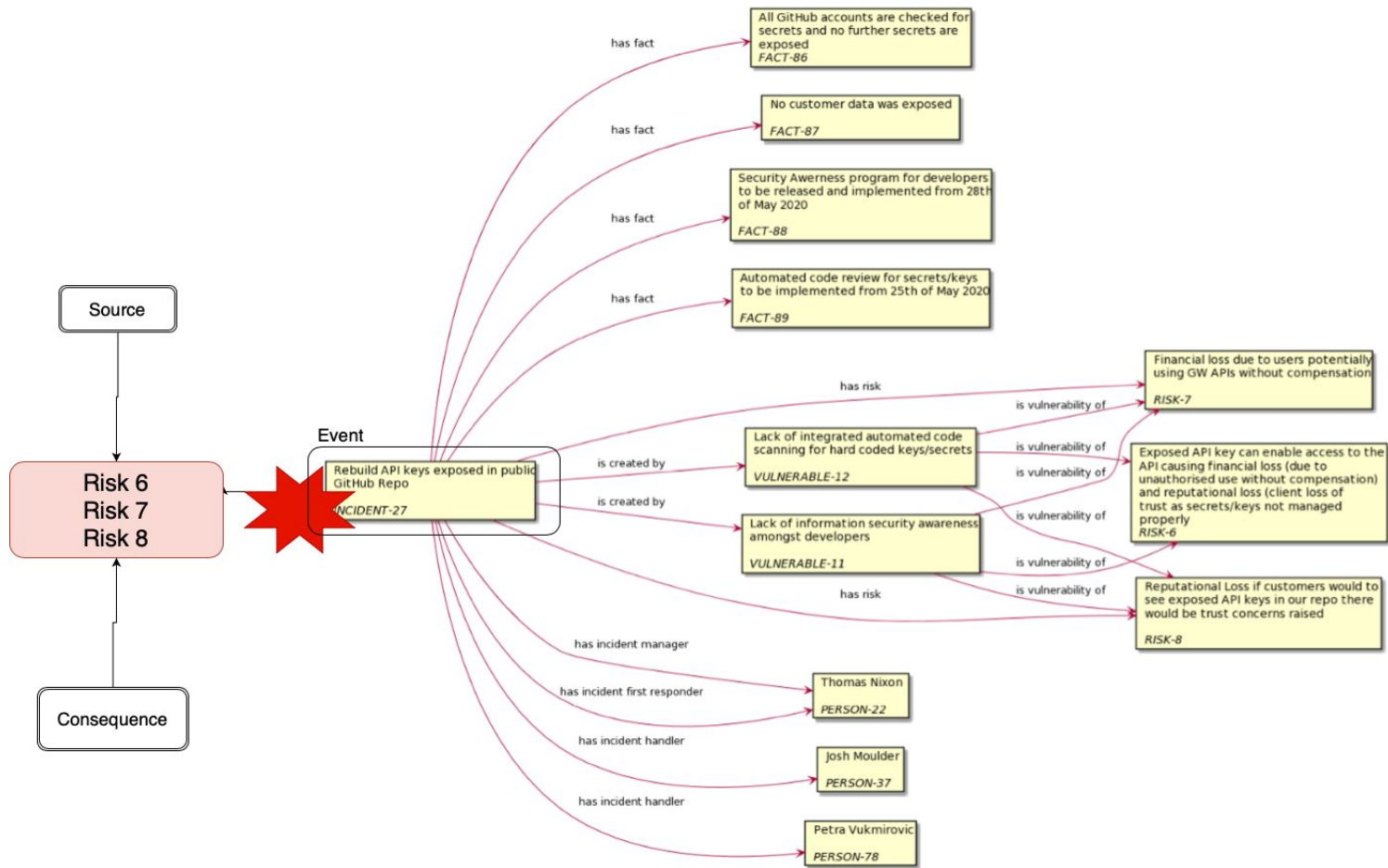
draw.io-13.2.2-win...exe
Failed - Download error

Show all

Graphs! All the graphs!



Graphs!



Questions & feedback, please!

- Does it make sense?
- Do you think anything is missing?
- How did you find putting it in to practice?
- What (other) use cases excite you most?





Thank You

Robin & Phil & Petra

Links

Open Information Security Risk Universe

- <https://oisru.org>
- <https://github.com/oracuk/oisru>

Bow tie diagrams:

- <https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/About-Bowtie/Introduction-to-bowtie/>

Photos 📷

- Unknown CC0 author, <https://pxhere.com/en/photo/140573>
- NASA, <https://commons.wikimedia.org/wiki/File:Astronaut-in-space.jpg>
- Casey Horner, <https://unsplash.com/photos/mPnxwQBtUZE>
- NASA, ESA, and the Hubble Heritage Team (STScI/AURA)-ESA/Hubble Collaboration, https://commons.wikimedia.org/wiki/File:LH_95.jpg
- “Pale Blue Dot” NASA, <https://www.jpl.nasa.gov/spaceimages/details.php?id=PIA23645>

