Expanding the evidence base in cyber insurance

Benjamin Dean

President
Iconoclast Tech LLC

Today's presentation

1. Cyber insurance evidence deficiencies
2. Opportunities
3. Recommendations

Cybersecurity's evidence problem

- Economic issues:
  - Impossible to reach 100% security
  - Limited resources to invest in security measures
  - Each € spent has diminishing marginal (security) benefits
- Technical and organisational issues:
  - Cybersecurity is an area where the outcomes are rarely measured (Florencio & Herley, 2014)
  - Iatrogenics – Some measures make the problem(s) worse
    - Strong passwords (Zhang et al, 2010; Chiasson & van Oorschot, 2015)
    - High-jacking of patching supply chain (e.g. Ccleaner)
    - Phishing breach notification letters (e.g. Equifax)

3 gaps in the evidence base:

1

Incident probability

2

Incident impact

3

Effectiveness of security measures

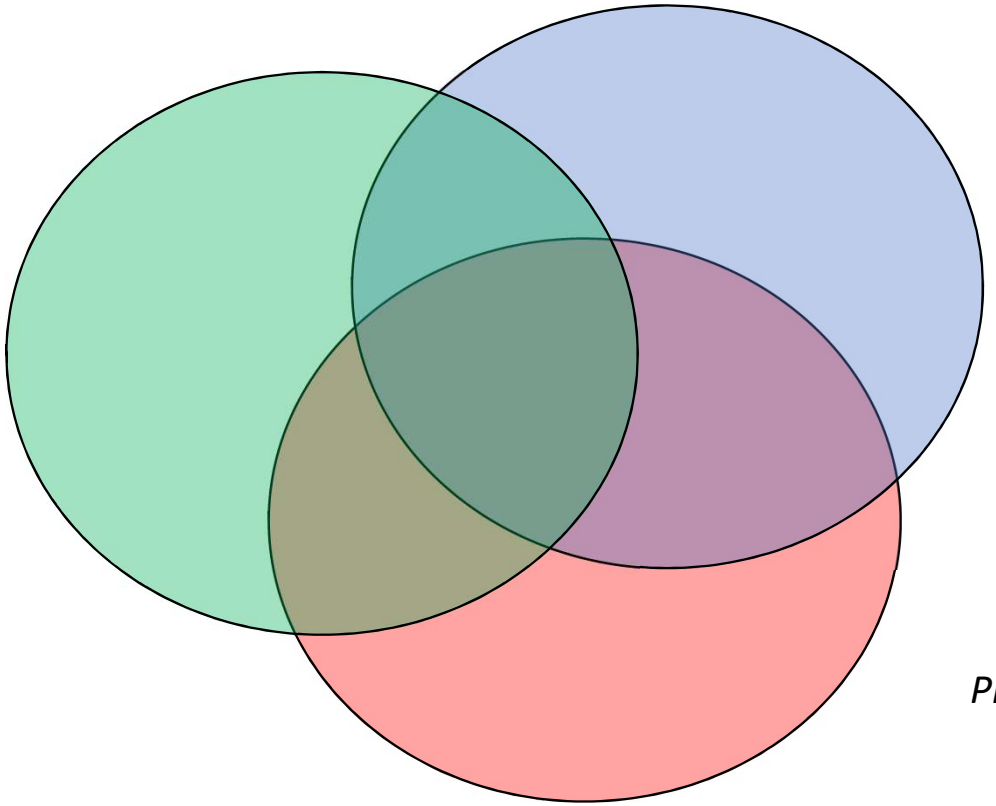
Better evidence helps you answer the following questions:

	Insurers	Businesses	Government
Incident probability	• What coverage do customers want?	• Which incidents could my business face? • Which are most likely?	• What's the best allocation of law enforcement and cybersecurity budget?
Incident impact	• At what price should I cover the perils?	• What would be the impact of those incidents on my business?	• What incidents should CSIRTs prioritise?
Effectiveness of security measures	• How might I assess the insured's risk profile? • What measures do I need to monitor?	• Which measures to implement to reduce risk? • Which risks should I transfer through insurance?	• How to develop effective awareness campaigns? • Which security measures should public authorities use?

Common interests

Businesses

Reduce risk exposure



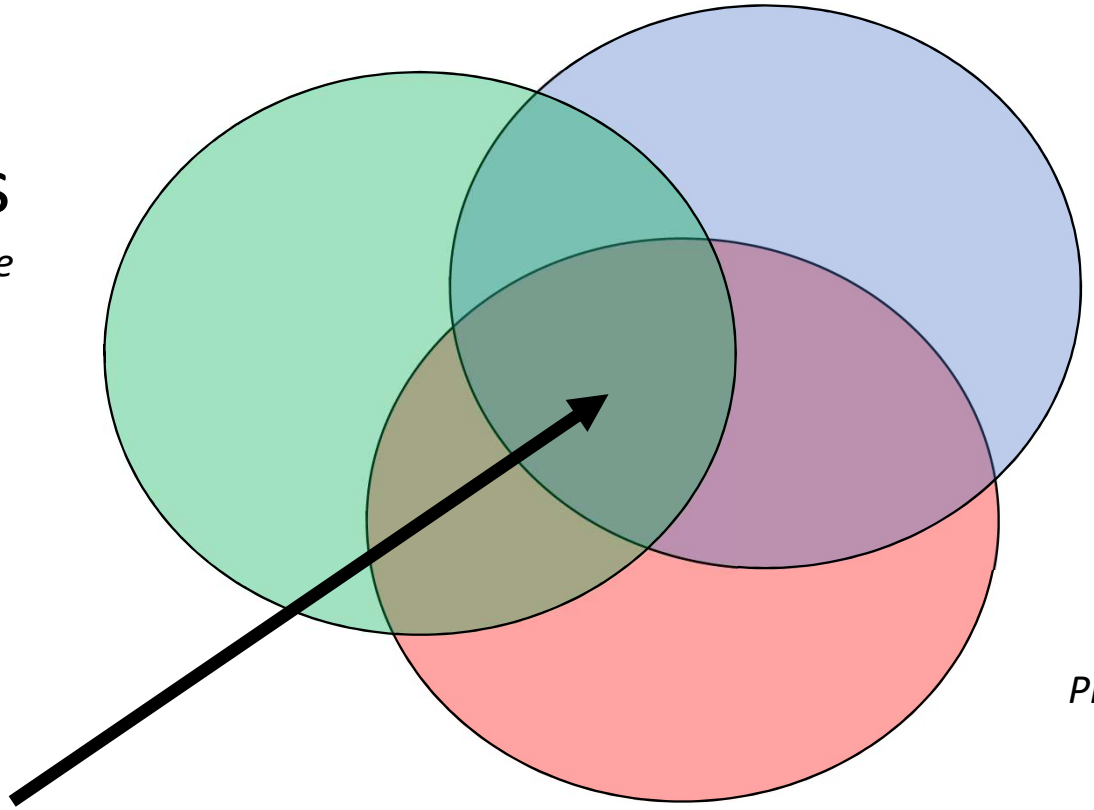
Insurers

Generate long-term value and profit

Government

Protect the wellbeing and safety of citizens

Common interests



Businesses

Reduce risk exposure

Insurers

Generate long-term value for shareholders

Government

Protect the wellbeing and safety of citizens

How to spend our limited resources to achieve these goals?

NIS Directive and GDPR are an opportunity

NIS and GDPR address:

1. Incident Notification

2. 'Appropriate security measures'

Which potentially provide evidence for:

Incident probability

Incident impact

Effectiveness of security measures

1. Notification requirements

GDPR

- Breach nature
- Category of & no. of people affected
- Likely consequences
- Proposed mitigation measures

NIS

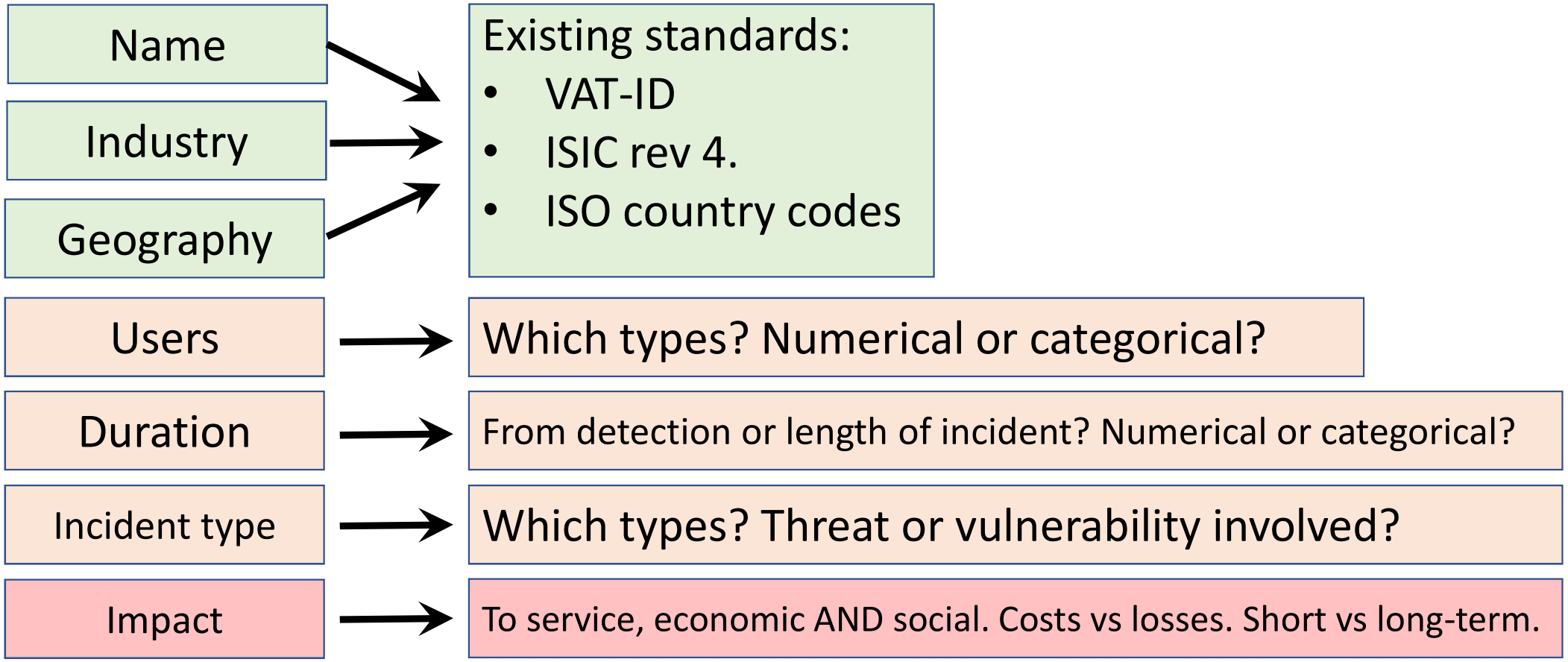
Operators of essential services

- No. of users affected
- Duration
- Geographic spread

Digital service providers

- No. of users affected
- Duration
- Geographic spread
- Extent of disruption on service
- Extent of impact on economic and societal activities

To be useful, all require taxonomies + definitions



2. 'Appropriate security measures'

GDPR

- Pseudonymisation
- Encryption
- Confidentiality, integrity, availability and resilience
- Restore… in a timely manner
- Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

NIS

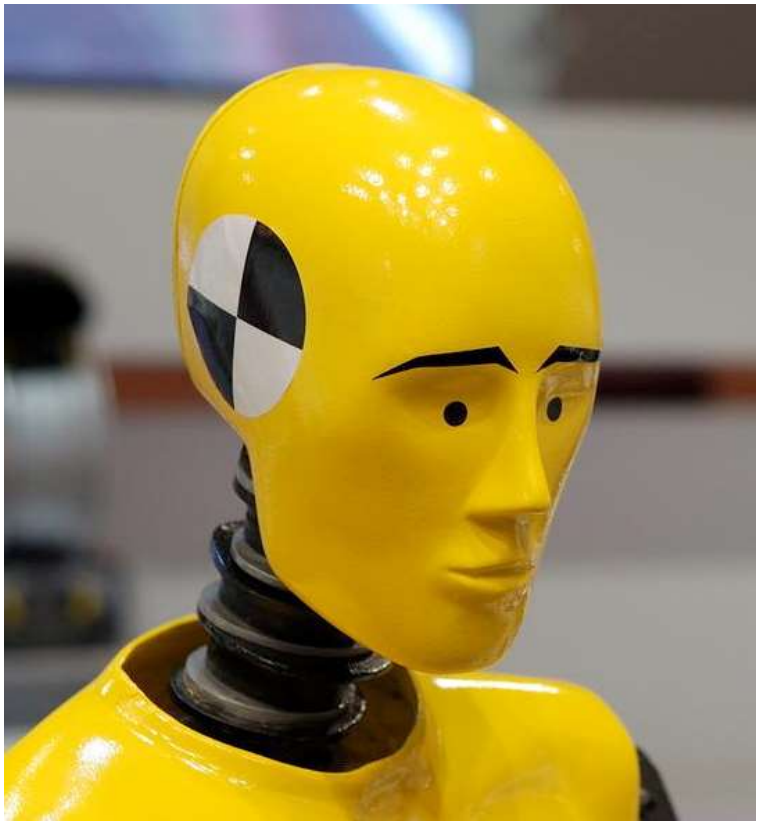
Operators of essential services

- "State of the art" network and information security systems appropriate to each organization's risks

Digital service providers

- Consider the security of systems and facilities, incident management, business continuity, monitoring, auditing and testing, and compliance with international standards

How to measure ‘appropriate’ or effective?



We do it in the auto industry

e.g. Automotive Crash Injury Research Center (1952)

We don’t do it in cyber security

Some suggestions:

- Quasi-natural experiments*
- Simulations
- Incident investigation

*See: Dean, Quasi-natural experiments to evaluate cyber Security policies, Journal of International Affairs, Winter 2017.

Summary

1. Growth of cyber insurance has not kept pace
2. Deficient evidence base
3. GDPR and NIS Directive present opportunities
4. Need to develop standard definitions and taxonomies

Expanding the evidence base in cyber insurance

Benjamin Dean

Iconoclast Tech LLC

ben@iconoclast.tech