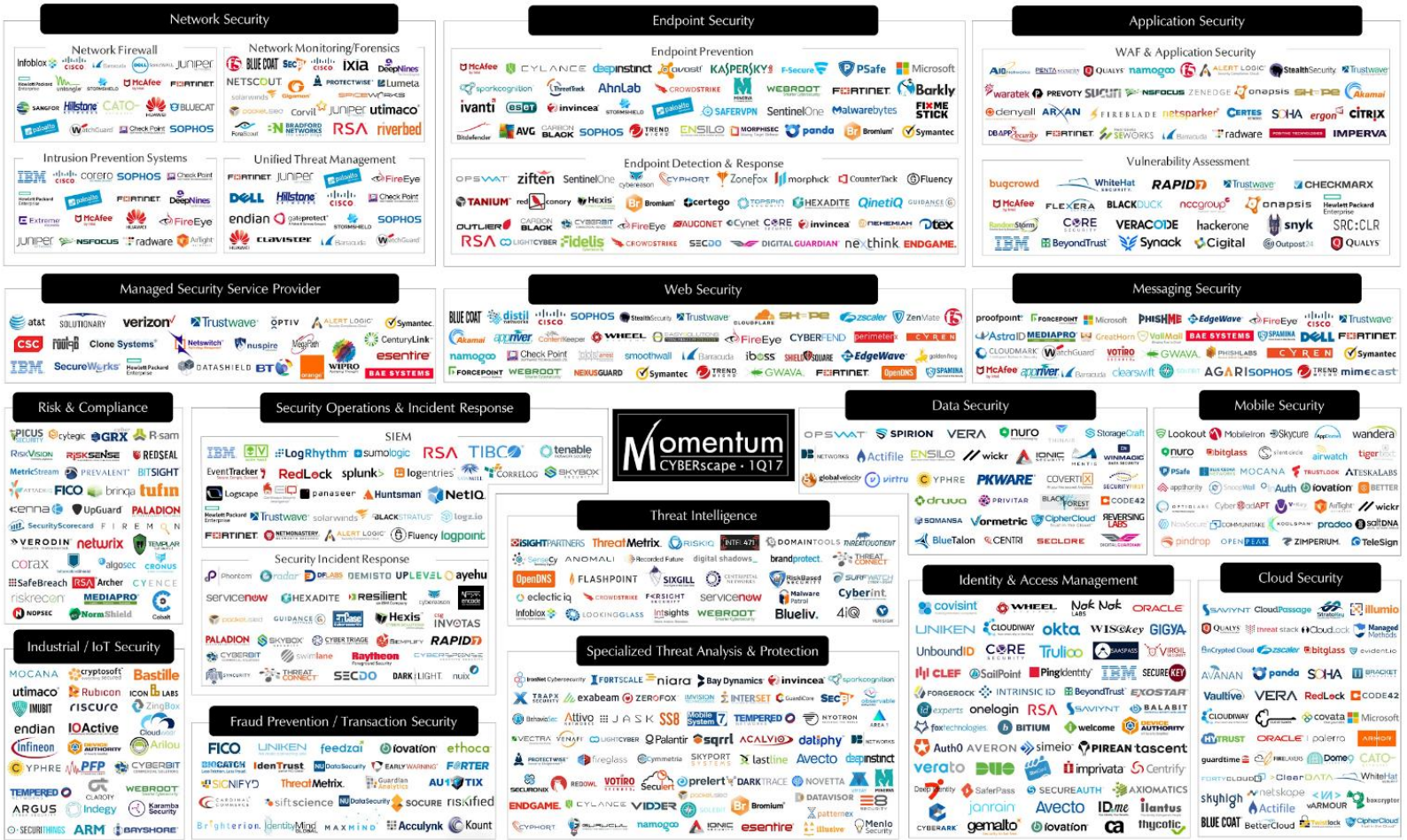
Towards integrating insurance data into information security investment decisions making

Daniel W. Woods & Andrew C. Simpson

CYBERscape: The Cybersecurity Landscape



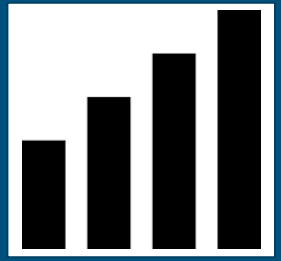
The Cybersecurity Landscape is Vast and Dynamic. We Have Vigilantly Covered The Sector For Over Two Decades.

Cyber Science

- “Security cannot be managed better until it can be measured better”
  Ross Anderson and Tyler Moore
- “systems beyond the technical, such as business processes and organisational structures, are included within cyber science and technology”
  UK National Cyber Strategy (2017)
- “Quantified security is thus a weak hypothesis because a lack of validation and comparison between such [operational security] methods against empirical data”
  Vilhelm Verendel

Data sources

Insurance as a quasi-experiment



Security level

Loss estimation

Data standard

Organisation	Organisation Data	Asset Type	Transfer
Revenue **Industry** Breach History, Employee Count Founding Year Mergers/ Acquisitions, BitSight Rating ISO 27001 Indicator Privacy Policy Score	**Data Type** Record Count Cost Per Unit Data Backup Frequency Recovery Cost Health Indicator	**Asset Type** Business Interruption Cost Recovery Cost Location Asset Count Physical Security Measures Anti-Virus Quality Score	**Transfer Type** Access Level Payment Processor DNS Provider Encryption Quality Score Cloud Type

Applying for cyber insurance

ISO Section: Summary of contents	Average Sub-Controls mentioned in the forms
6: Organisational Roles	38%
7: Human resources	35%
8: Asset Management	43%
9: Access Control	28%
10: Cryptography	75%
11: Physical Security	35%
12: Operational security	39%
13: Communications	15%
14: System Management	7%
15: Supplier Relationship	29%
16: Incident Management	17%
17: Business Continuity	50%
18: Compliance	69%

Scenario: A firm considering whether to purchase a phishing awareness scheme

ROSI and ALE

$$ALE = ARO \times SLE$$

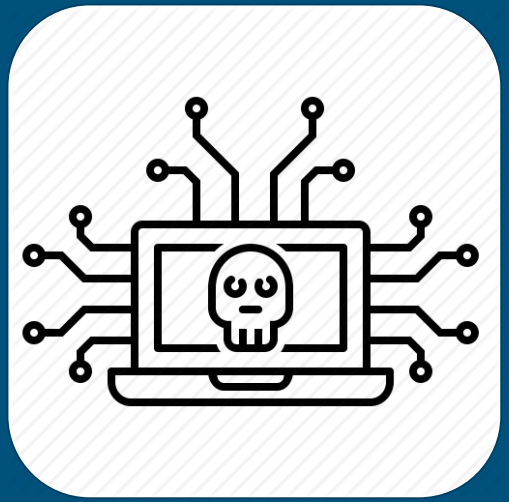
$$ROSI = \frac{\text{Benefits of security - Cost of investment}}{\text{Cost of investment}}$$

Annualised Loss Expectancy (ALE)
(ROSI)
Annual Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)

Return on security investment

Single Loss Expectancy

1. First-Party
2. Data Privacy and Network Security Liability
3. Business Interruption
4. Cyber-Extortion Investigation
5. Public Relations
6. Multimedia Liability Costs
7. Professional Services



Annual Rate of Occurrence

1. Subjective effectiveness
1. External effectiveness
1. Actuarial effectiveness

Improving Data Collection

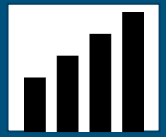
Standardisation

Forensics

Policy wording

Automated

Conclusions



- Linking security level with losses is the holy grail
- Current data falls short
- Insurance data may provide a way in the future
  - Need to actively guide how it is collected