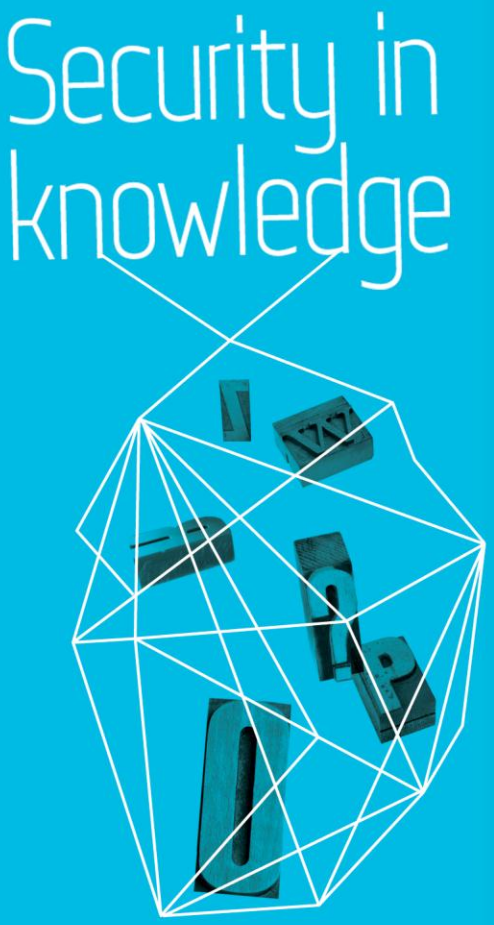
Everything You Wanted to Know About Cyber Insurance But Were Afraid to Ask



Moderator:

Gib Sorebo
SAIC

Panelists:

David Navetta
InfoLaw Group

Nick Economidis
Beazley Group

Scott Kannry
Aon Risk Solutions

Session ID: GRC-R32

Session Classification: General Interest

Background and Current State of Cyber Insurance

- Historical context
  - From general liability to carve outs
  - Data loss not covered
  - Growth in mitigation coverage
  - Growing demand for cyber insurance
- Current state
  - Low limits
  - Focused on identity theft
  - Critical infrastructure "coverage" limited

Losses Covered or Not

- Loss categories
  - Customer data breaches
  - Business interruption (denial of service)
  - Intellectual property loss
  - Data corruption or loss
  - Physical damage to property
  - Personal injury
- Typical policy limits
- Causation
- Minimum standards of care required

What Does This Mean for the Security Professional?

- Relationships with
  - Cyber insurance provider
  - Corporate Risk Management
  - Shared advocacy for security
- Defining need
- Input on defining standards of care
- Obligation to define and share metrics

The Future for Cyber Insurance

- Targeted attacks
  - Is more expected for companies or industries that are targeted?
  - Should insurance cover nation state attacks and cyber terrorism?
- Stuxnet-like attacks causing physical damage and potential personal injuries
- Widespread damage
  - What policy limits are reasonable?
- Better metrics

Key Takeaways

- Security professionals should provide more input on cyber insurance matters to appropriate company officials
- Review policies to ensure that relevant cyber harms are covered
- Work with insurer to understand the risk-based metrics that most influence premiums and cover limits
- Work to customize policies to better fit company needs

Questions?