

# Ten Years After The Snowden Revelations (and other ISEities)



Eliot Lear  
Independent Submissions Editor

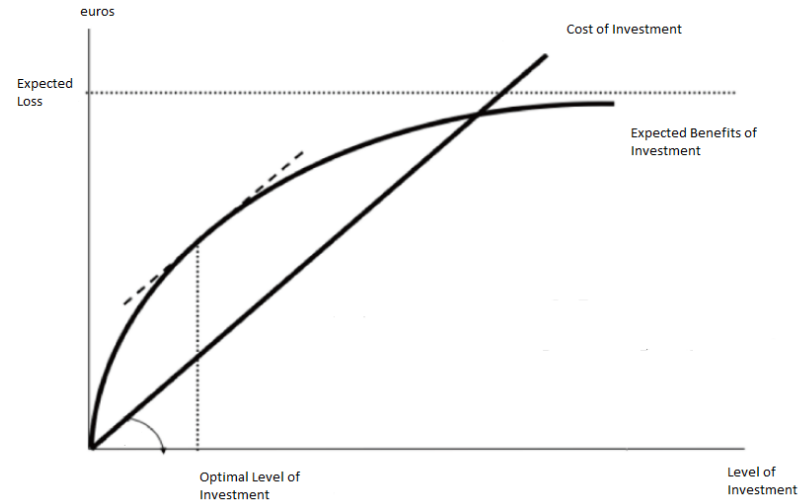
# Before 2013



- We accepted that people could observe certain activities

$$s = \text{expected loss} / e$$

- We assumed that such observations were limited by locality
- There was some positive network management benefit to such an observation
- It was still subject to abuse by certain parties



Gorden-Loeb model (2002)



But what if the attacker has (near) infinite resources?

And what if you can't quantify the losses?

# November, 2013 in Vancouver: We were not amused.



Courtesy: Tim Bray

# RFC 9446: Reflections on Ten Years Past the Snowden Revelations



## Four Essays:

- Bruce Schneier
  - What it was like to report the event
- Stephen Farrell
  - Our response and advances since
- Farzaneh Badii
  - Human rights implications
- Steve Bellovin
  - Putting the revelations into historical perspective

# Why Is This Document Important?



- This event was a big deal in our history!
  - Did we react well?
  - What accomplishments did we achieve?
  - What is left to be done (by us and by others)?
  - How has the threat environment evolved since then?

Retrospectives are **useless** unless they help us learn.  
Hopefully this one will help us learn.

*(Hint: the ISE asks the above question each time a draft is submitted for consideration)*

# A few additional observations



- Development of new capabilities (cf H2/TLS1.3,...) took time, commitment, consensus, and code.
- Economics **were** and **are** in play
  - Much of the data is still there, but it may be held by different players
- The threat environment **has** changed
  - Centralization makes pervasive surveillance easier
  - Infrastructure attacks are serious



By Martin Grandjean - Grandjean, Martin (2014).  
"La connaissance est un réseau". Les  
Cahiers du Numérique 10 (3): 37-54.  
DOI:10.3166/LCN.10.3.37-54., CC BY-SA 3.0,  
[https://commons.wikimedia.org/w/index.php?  
curid=29364647](https://commons.wikimedia.org/w/index.php?curid=29364647)

Do you have an protocol or a view you'd like to share?



- Independent submissions can help with...
  - Interoperability
  - Continuous Improvement
  - Levity
- Caveats: Won't be a standard, will not have community consensus (and cannot pretend to be either)



Thank you!

[rfc-ise@rfc-editor.org](mailto:rfc-ise@rfc-editor.org)