Negligent Cyber Security: *How* and *When* did we become liable to third parties?

Robert Carolina, Executive Director
Institute for Cyber Security Innovation
Robert.Carolina@rhul.ac.uk; +44 7712 007 095

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Robert Carolina

INSTITUTE FOR CYBER SECURITY INNOVATION

- Royal Holloway University of London
  - Executive Director, Institute for Cyber Security Innovation
  - Law & Regulation module leader, Information Security Group (1999-date)
- Lawyer (US & England)
  - Solicitor, Origin Ltd (London)
  - Law & regulation of ICT; Law & ethics in cyber security
  - BA (University of Dayton); JD (Georgetown); LL.M (London School of Economics)

The Institute for Cyber Security Innovation

- Not-for-profit / market neutral
- Multidisciplinary, drawing from:
  - multiple departments
  - multiple institutions (ours and others)
- Projects to address unmet cyber security needs
  - Directed research
  - Industrial training
  - Cryptographic assessment
  - Investor due diligence
  - Policy development

About this talk

- What is “negligence” liability?
- Who is liable to whom?
- What is “reasonable” conduct?
- How does “reasonableness” change over time?
- (Time permitting) Other basis of liability?

Negligence liability – acting "reasonably"

IF:

- Alice owes a "Duty of Care" to Bob, AND
- Alice fails to act "reasonably" in exercising that duty

THEN:

- Alice has breached her duty of care. Alice is "negligent".

WHAT CAN BOB DO ABOUT IT?

Bob can sue Alice. Bob must prove:

1. Alice owes a duty to Bob
2. Alice breached that duty (by failing to act reasonably)
3. Alice's failure caused legally cognisable harm to Bob

The Target incident (incident as reported by Bloomberg)

- Summer 2013: Target procures monitoring system
- Nov 30, 2013: System reports malware suspicion to Target; Target takes no immediate action
- Dec 2 – 15: Bad guys take card numbers belonging to 1/3 of all American consumers
- Dec 12: US Dept of Justice calls Target
- Dec 15: Target finds and disables malware

- Third party law suit settlements:
  - Consumer class action (pending appeal): $10M + $7M fees to consumers' lawyers
  - Banks (accelerated card replacement costs, underwriting fraud loss, etc): $106M
- As of July 2016:
  - Total costs (1st & 3rd party): $291M
  - Expected insurance payments: $90M

The Reasonable Person

- What does it mean to act "reasonably"?
  - Varies with the expectations & standards of a given community
  - Often measured by reference to standards in ***the victim's community*** (private international law principle)
  - … and standards ***change over time***
- To assess whether a given act is "reasonable", consider standards of the multiple communities in which potential victims reside
- What would knowledgeable people say about Target's failure to respond to the warning?

NOW let's change the facts…

- The relevant behaviour in Target was the "***failure to respond***" to the alarm of a system that was already procured and in operation

BUT

- What if the relevant behaviour had instead been a "***failure to procure***" the monitoring system?

- Old question:
  - Was it "reasonable" to take no action after receiving an alarm of suspected malware in the payment system?

- New question:
  - Would it be "reasonable" to decline to purchase the monitoring system at all?
  - aka the "Ravenous Bugblatter Beast of Traal" defence

Re-thinking "reasonable"

- Famous US case: *TJ Hooper (expanded in Carroll Towing)*
  - Facts of the incident (1928)
    - Tugboat without a radio receiver caught in storm; Cargo lost
    - If a radio had been installed, it would have diverted to a harbour
  - Was the failure to install radio "reasonable"?
    - Most companies also failed to install radios
    - This operator seems to pass the "reasonable person" test

    …or does he?

"common practice" is not the same as "reasonable practice"

-Judge L Hand (1932)

"If B < P * L, then negligence"

-Judge L Hand (1947)

Re-thinking "reasonable"

If B < PL then failure to adopt solution is not "reasonable"

B = cost to implement a solution

P = probability of loss without the solution

L = amount of loss if disaster strikes because we don't have the solution

P: odds of loss w/o radio (0.4%)*

X

L: amount of loss ($100,000)*

B: cost of radio ($75)*

$75 < $400, therefore negligent

* Judge L. Hand used the formula without specific numbers to illustrate his rationale. I have used these hypothetical numbers to further illustrate the point made in the case.

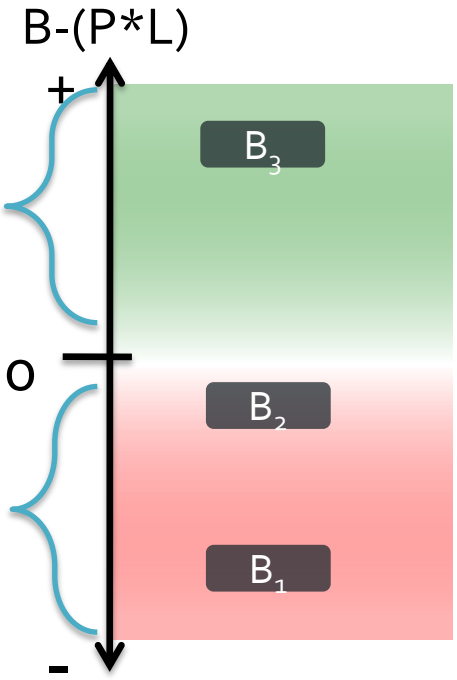
Re-thinking “reasonable”

(1) If B < (P*L), negligence

Reorganise as:

(2) If B-(P*L) < 0, negligence

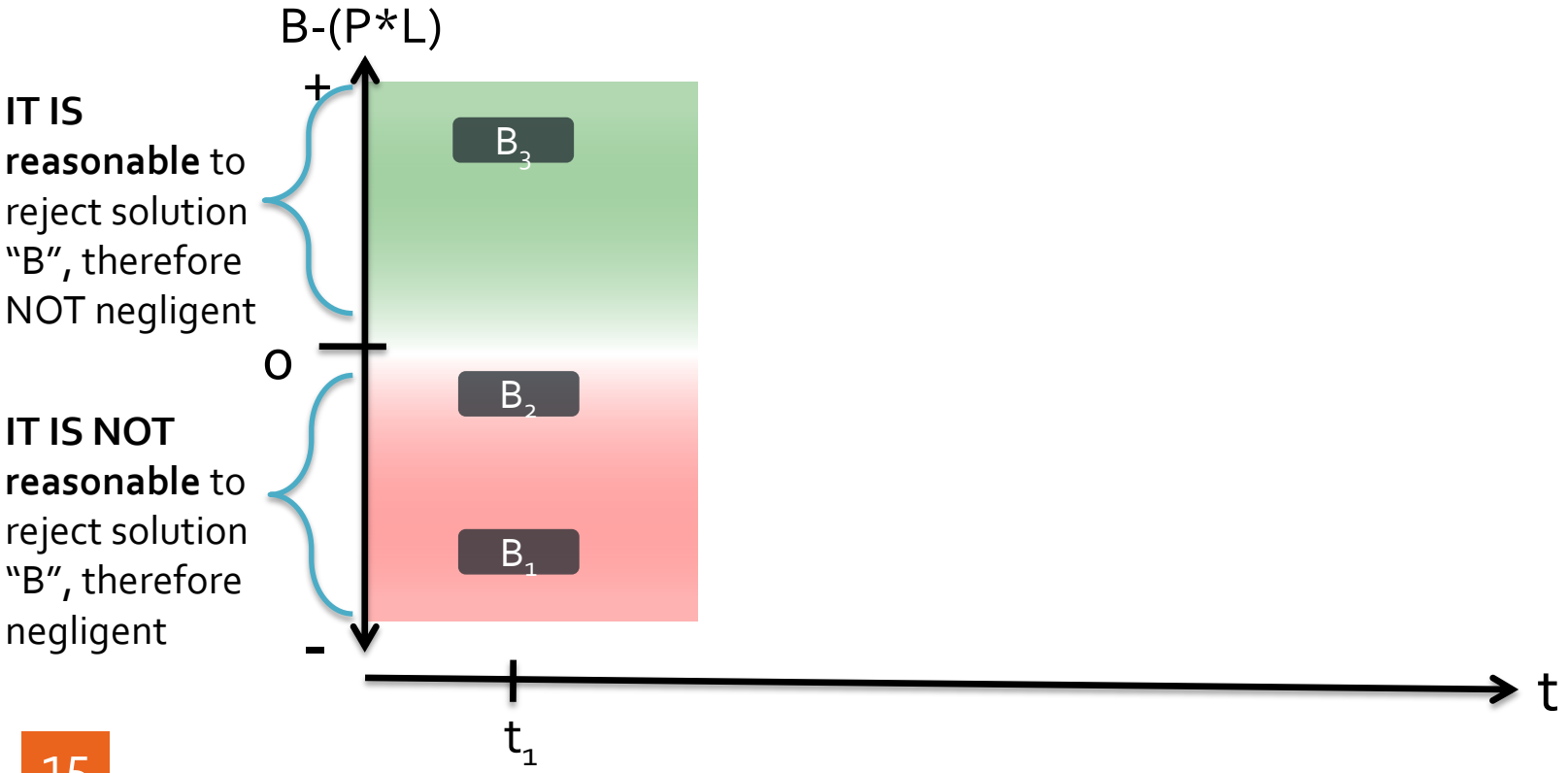
Failure to adopt a solution – negligent?



IT IS reasonable to reject solution "B", therefore NOT negligent

IT IS NOT reasonable to reject solution "B", therefore negligent

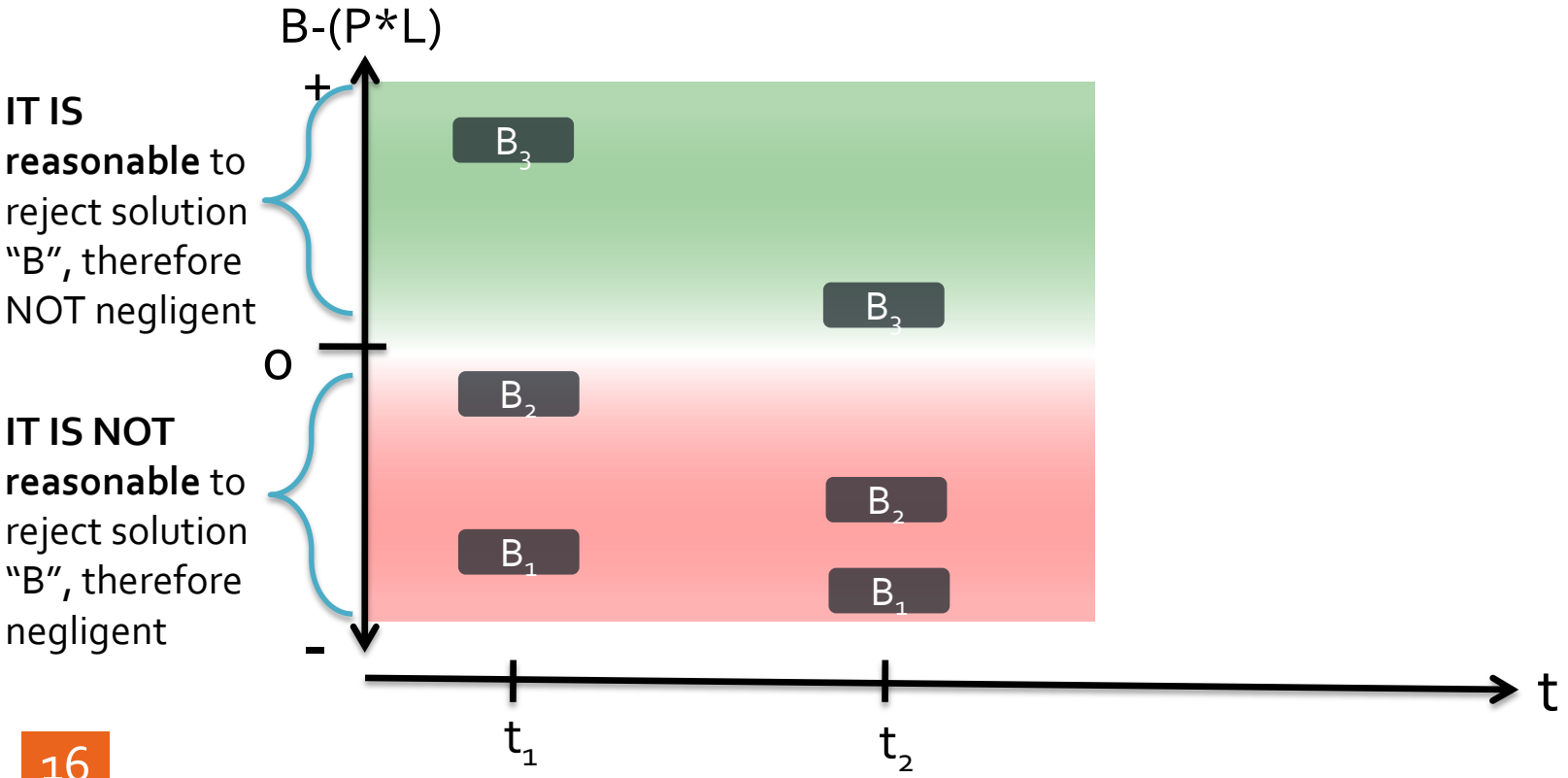
Failure to adopt a solution – negligent?



IT IS reasonable to reject solution "B", therefore NOT negligent

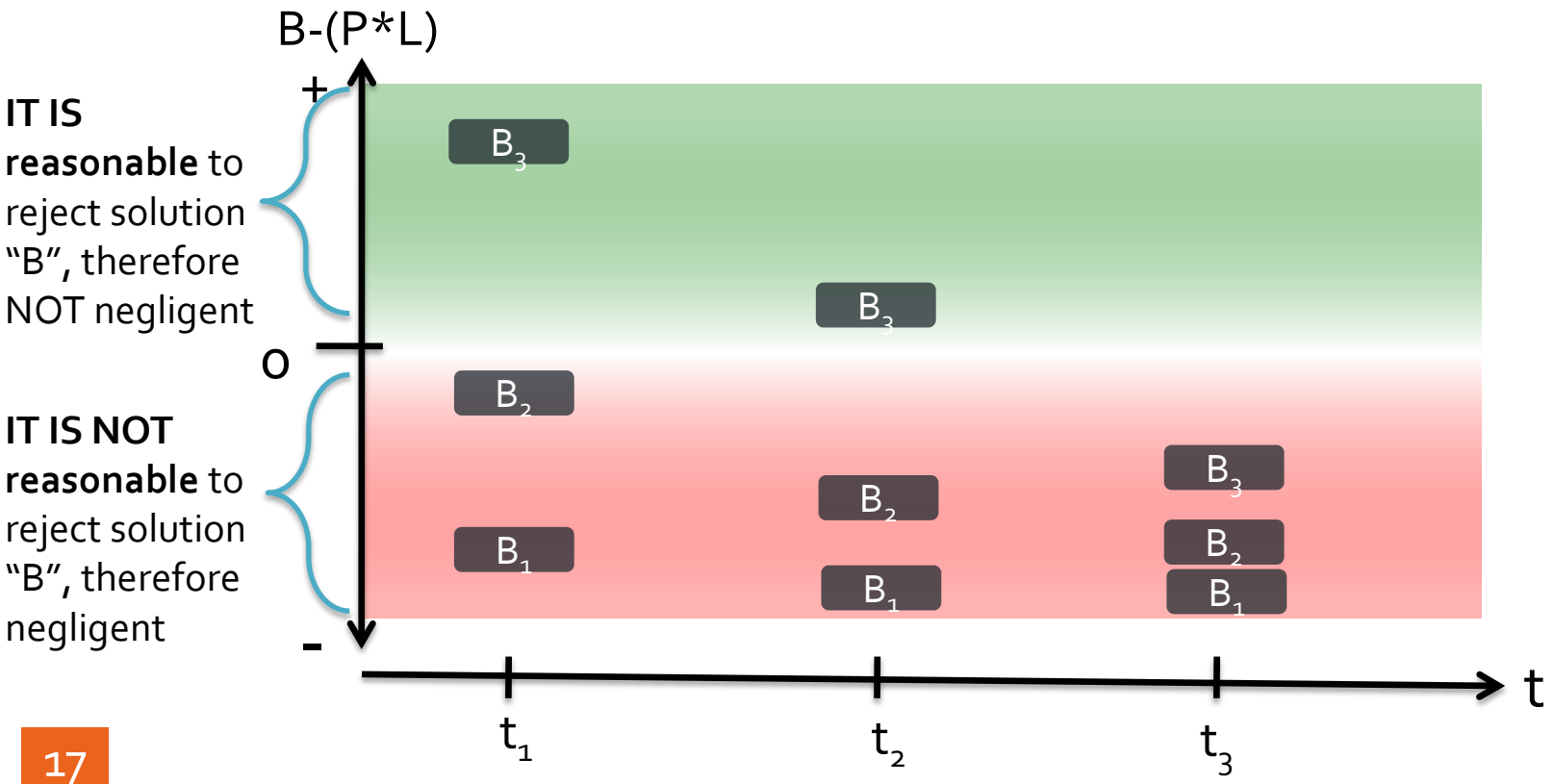
IT IS NOT reasonable to reject solution "B", therefore negligent

Failure to adopt a solution – negligent?



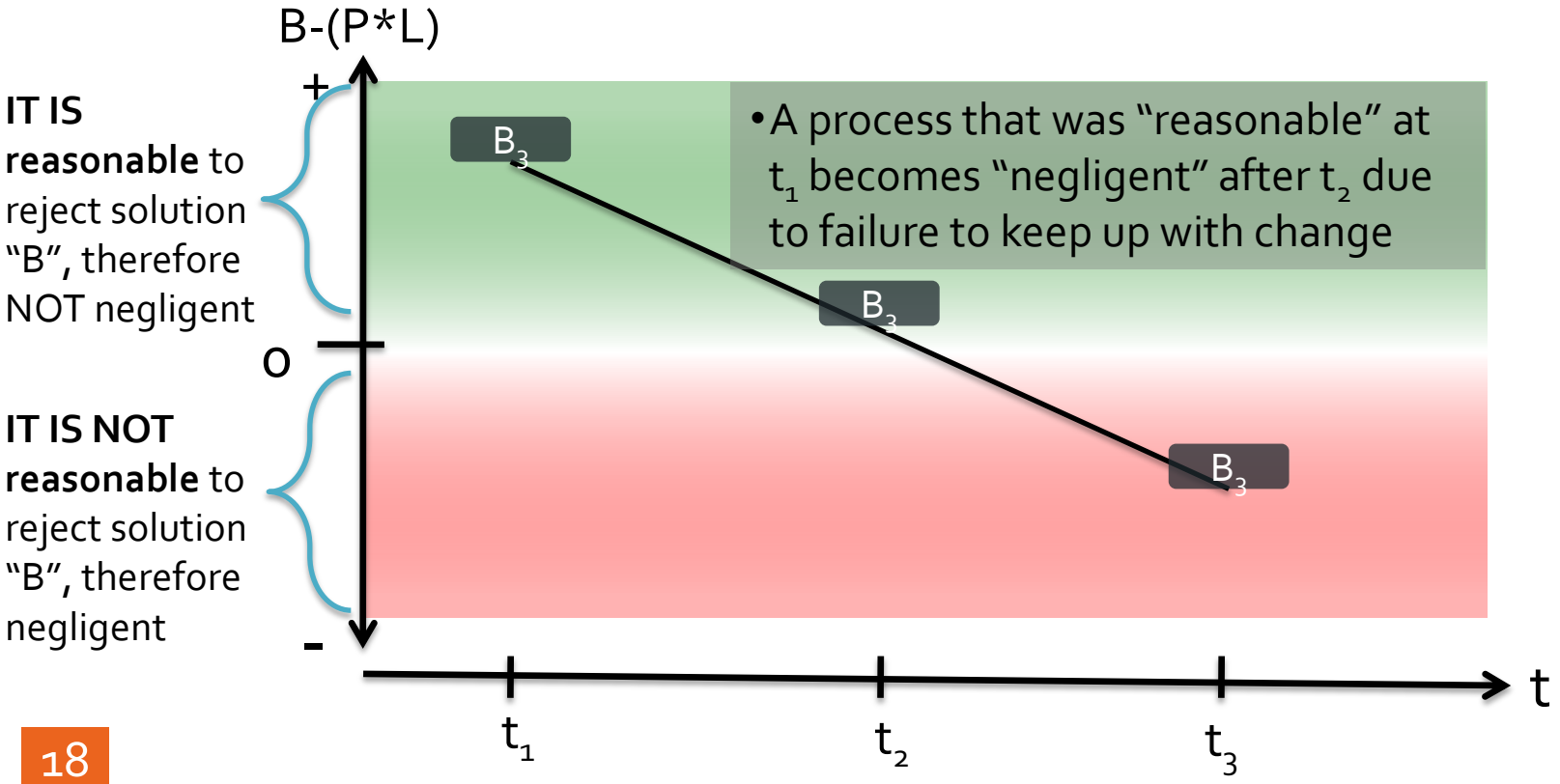
Failure to adopt a solution – negligent?

INSTITUTE FOR CYBER SECURITY INNOVATION

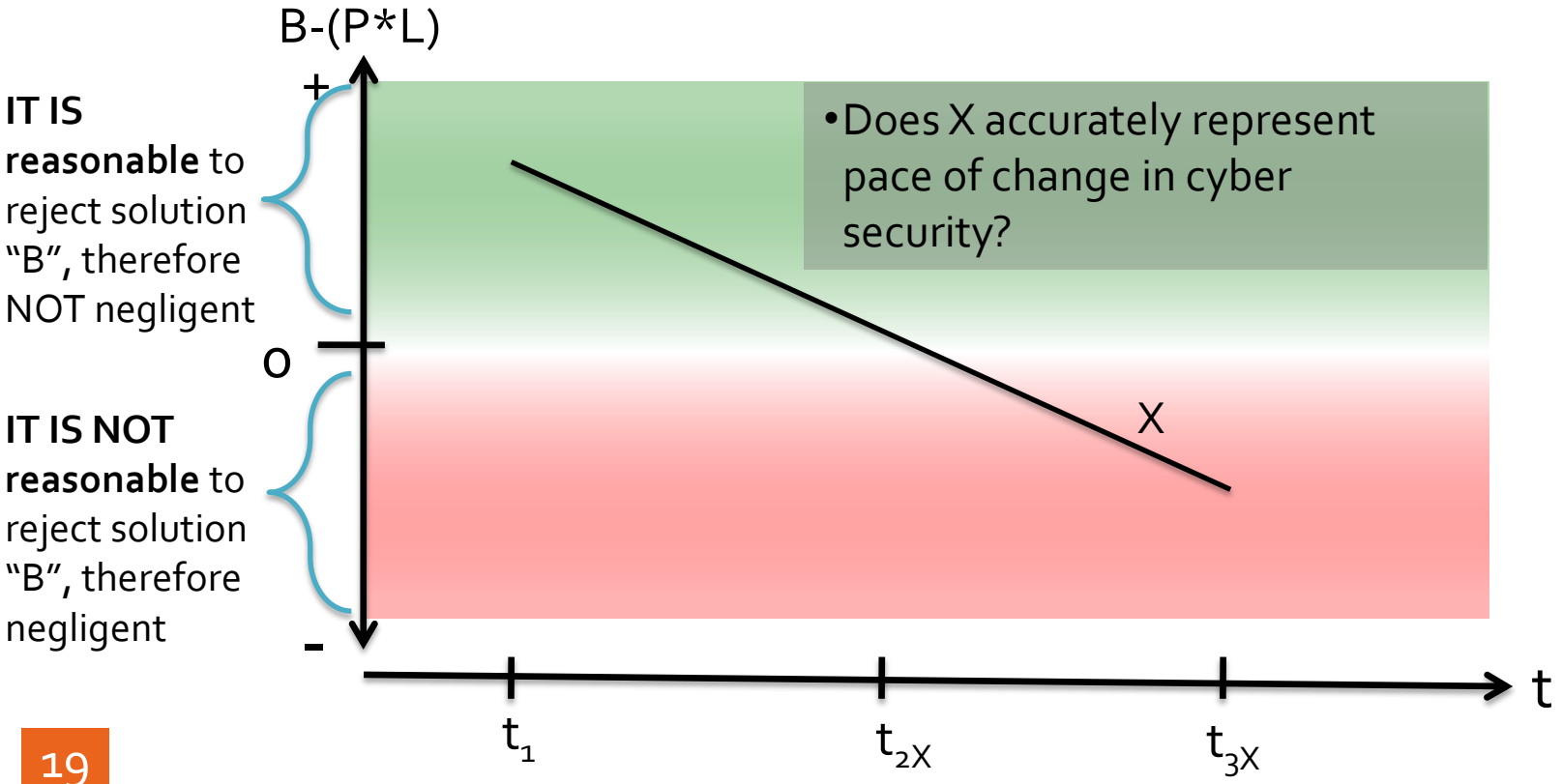


Failure to adopt a solution – negligent?

INSTITUTE FOR CYBER SECURITY INNOVATION



Failure to adopt a solution – negligent?

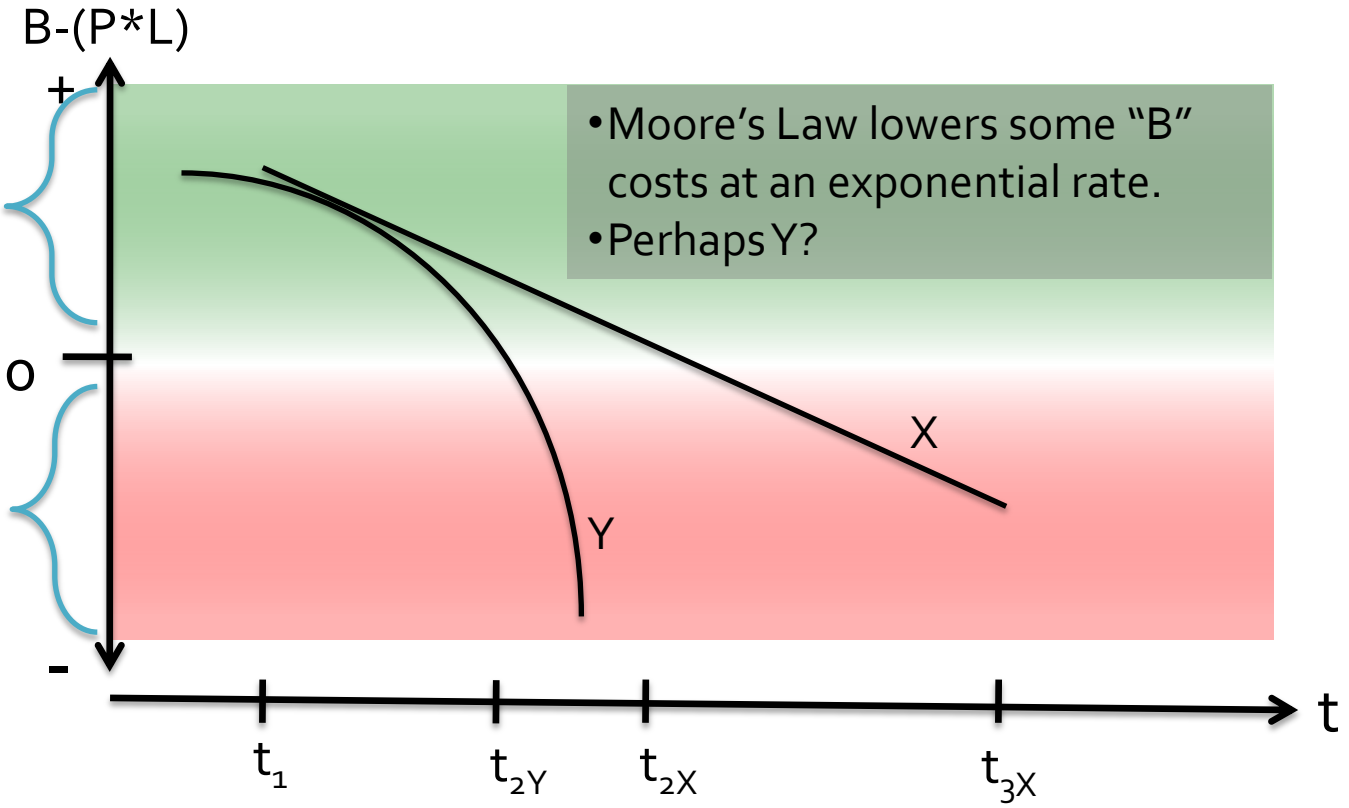


Failure to adopt a solution – negligent?

INSTITUTE FOR CYBER SECURITY INNOVATION

IT IS reasonable to reject solution "B", therefore NOT negligent

IT IS NOT reasonable to reject solution "B", therefore negligent

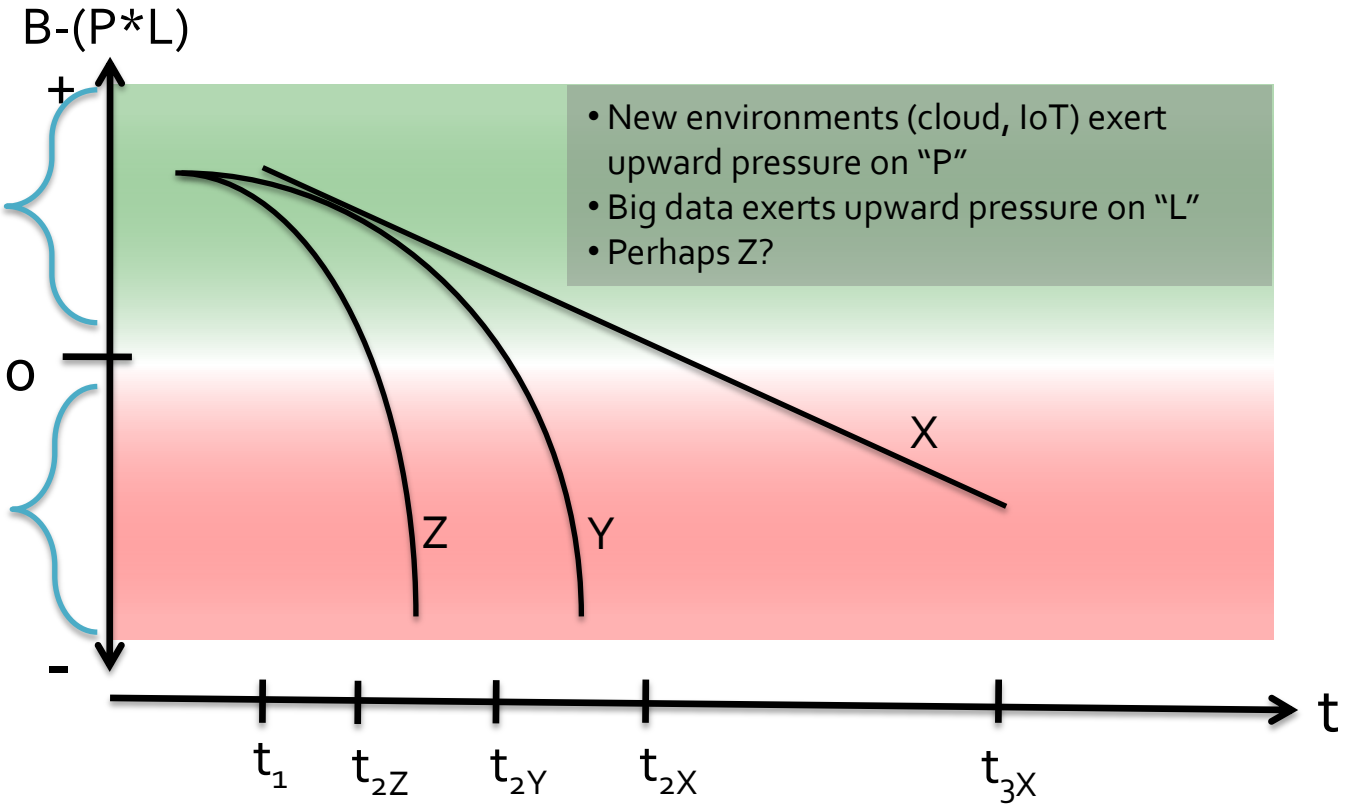


Failure to adopt a solution – negligent?

INSTITUTE FOR CYBER SECURITY INNOVATION

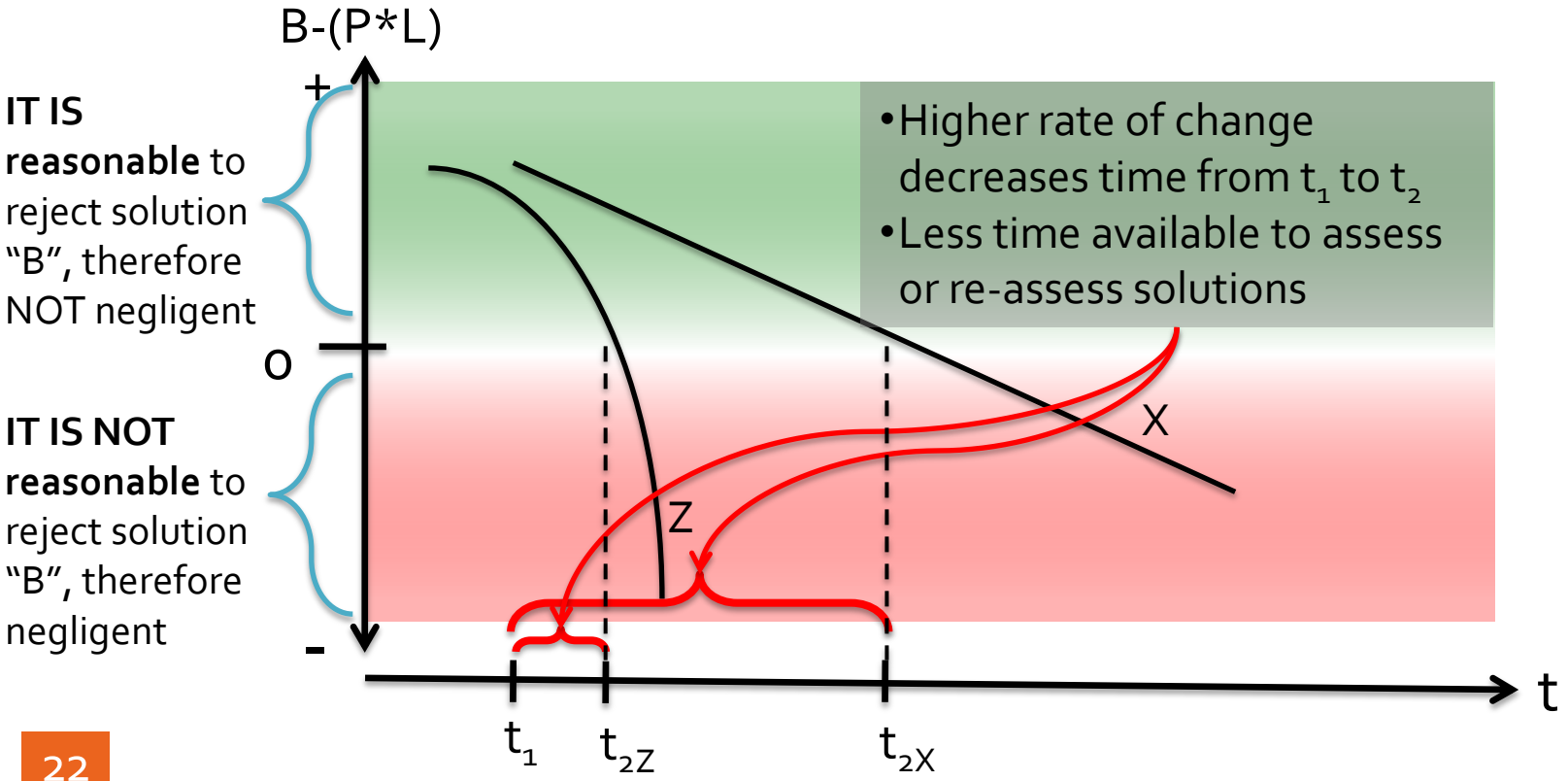
IT IS reasonable to reject solution "B", therefore NOT negligent

IT IS NOT reasonable to reject solution "B", therefore negligent



Failure to adopt a solution – negligent?

INSTITUTE FOR CYBER SECURITY INNOVATION



Pace of Change in Liability Profile – Impact on Cyber Security

- Strong business case for:
  - continuous assessment of Cyber Security risks & solutions
  - continuous re-examination of cost-benefit decisions
  - duty to re-examine decisions that reject or delay new security methods because they were too expensive compared to risk
- Consider defence through the lens of "manoeuvre warfare" theory
  - OODA Loop, etc, originally developed by the late Col John Boyd, USAF
  - responding to the challenge of ever-shortening innovation curves (cf Freddie Hult)

Other methods for Bob to prove that Alice was negligent?

Negligence "*per se*"

- Basic Concept:
  - If there is a law, or regulation, or widely adopted industry standard, that defines "reasonable conduct", then a failure to meet this law or standard should be regarded by the courts as "unreasonable" conduct
  - Some courts treat this as a rule of evidence: violating the standard can be used to infer negligent conduct
  - Others courts prepared to treat it as "proof" of negligence
- Consider
  - What happens when cyber security experts decide to adopt what they describe as a standard of practice?
  - What happens when the payment card industry decides to adopt PCI-DSS?
- Caution:
  - Meeting or exceeding a published standard is not necessarily proof (on its own) that Alice's actions were "reasonable"

Res ipsa loquitur

- "The thing speaks for itself"
  - Some things are "obviously" the result of negligence by Alice; no need for Bob to prove it, but Alice may be allowed to prove the negative
  - Leading case: barrel falls from upper floor storage room onto a person below at ground level.
- Doctrine normally applies only when the accused (Alice) had "control" over the thing that has now gone out of control
- Modern examples:

  Engine pylon assembly separates from wing at take-off (DC-10 Chicago, 1979)

  "Hey Doctor, why is one of your operating instruments still inside the patient?"

Negligent Cyber Security: *How* and *When* did we become liable to third parties?

Robert Carolina, Executive Director
Institute for Cyber Security Innovation
Robert.Carolina@rhul.ac.uk; +44 7712 007 095

ROYAL HOLLOWAY UNIVERSITY OF LONDON