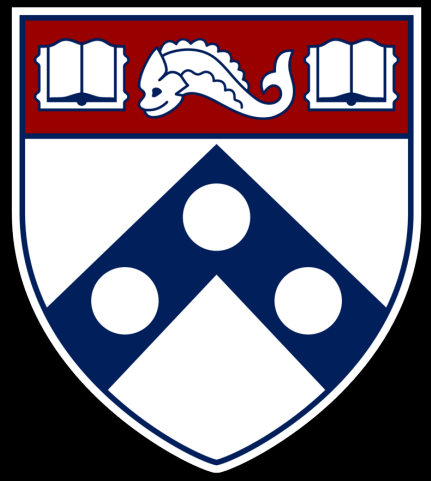
Empirical Security & Privacy, for Humans

UPenn CIS 7000-010

10/23/2025



The Economics of Information Security Investment

Reading

The Economics of Information Security Investment

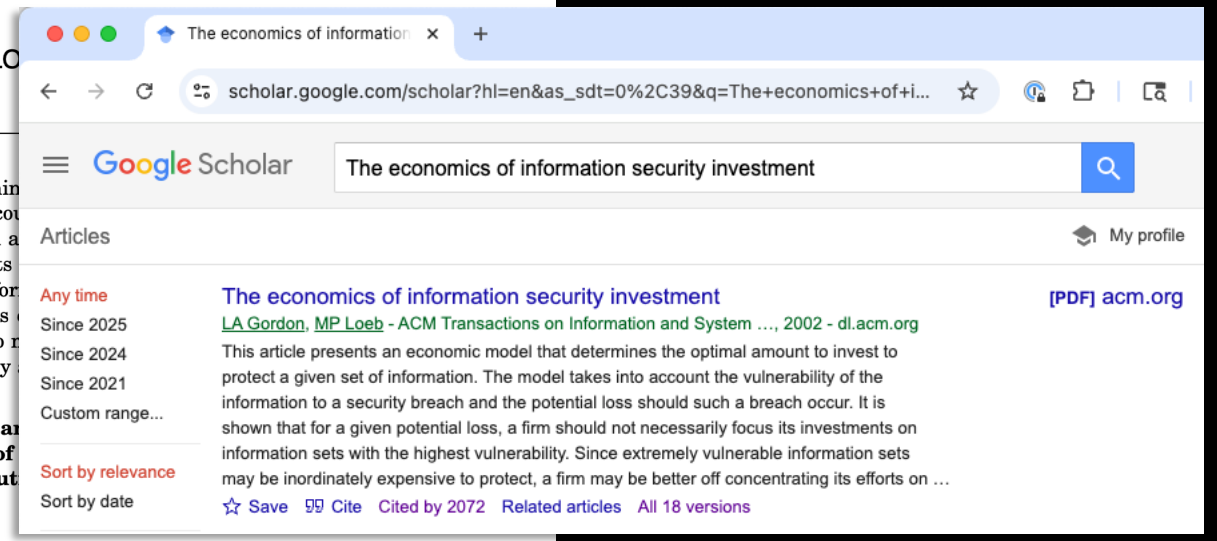
LAWRENCE A. GORDON and MARTIN P. LO
University of Maryland

This article presents an economic model that determin
a given set of information. The model takes into accou
a security breach and the potential loss should such a
potential loss, a firm should not necessarily focus its
highest vulnerability. Since extremely vulnerable infor
to protect, a firm may be better off concentrating its
vulnerabilities. The analysis further suggests that to
ment to protect information, a firm should spend only
a security breach.

Categories and Subject Descriptors: H.1.1 [**Models a**
Theory—*value of information*; K.6.0 [**Management of**
General—*economics*; K.6.5 [**Management of Comput**
and Protection

General Terms: Economics, Security

Additional Key Words and Phrases: Optimal security investment



1. INTRODUCTION

Security of a computer-based information system should, by design, protect the confidentiality, integrity, and availability of the system (e.g., see NIST [1995, p. 5]). Given the information-intense characteristics of a modern economy (e.g., the Internet and World Wide Web), it should be no surprise to learn that information security is a growing spending priority among most companies. This growth in spending is occurring in a variety of areas including software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, automated data backup, and hardware devices [Larsen 1999]. The above notwithstanding, a recent study by the Computer Security Institute, with the participation of the Federal Bureau of Investigation, reported that "Ninety-one

This research was partially supported by The Robert H. Smith School of Business, University of Maryland and the Laboratory for Telecommunications Sciences (within the Department of Defense) through a grant with the University of Maryland Institute for Advanced Computer Studies.
Authors' address: The Robert H. Smith School of Bussiness, University of Maryland, College Park, College Park, MD 20742-1815; email: {lgordon;mloeb}@rhsmith.umd.edu.

Highly influential:
Cited > 2000 times

Model parameters

One-period model: No game theory
Assumes defender is risk-neutral

Core parameters

λ	Monetary loss of a breach
$t \in [0, 1]$	Threat: probability of an attack
$v \in [0, 1]$	Vulnerability: baseline probability an attack is successful

Shorthands, bounds

$vt\lambda$	Expected loss
$L = t\lambda$	Potential loss
$M > \lambda$	Catastrophic loss

Security investments

$z > 0$	Security investment
$S(z, v)$	Security breach prob. function: effective vulnerability starting from v, given an investment z

Security breach prob. function requirements

Security investments

$z > 0$	Security investment
$S(z, v)$	Security breach prob. function: effective vulnerability starting from v, given an investment z

A1: $S(z, 0)=0$ for all z

A2: For all v, $S(0, v) = v$

A3: For all $v \in (0, 1)$, and all z, $S_z(z, v) < 0$ and $S_{zz}(z, v) > 0$

- I.e., as the investment in security increases, the information is made more secure, but at a decreasing rate
- Assume for all $v \in (0, 1)$, *lim* $S(z, v) \rightarrow 0$, as $z \rightarrow \infty$

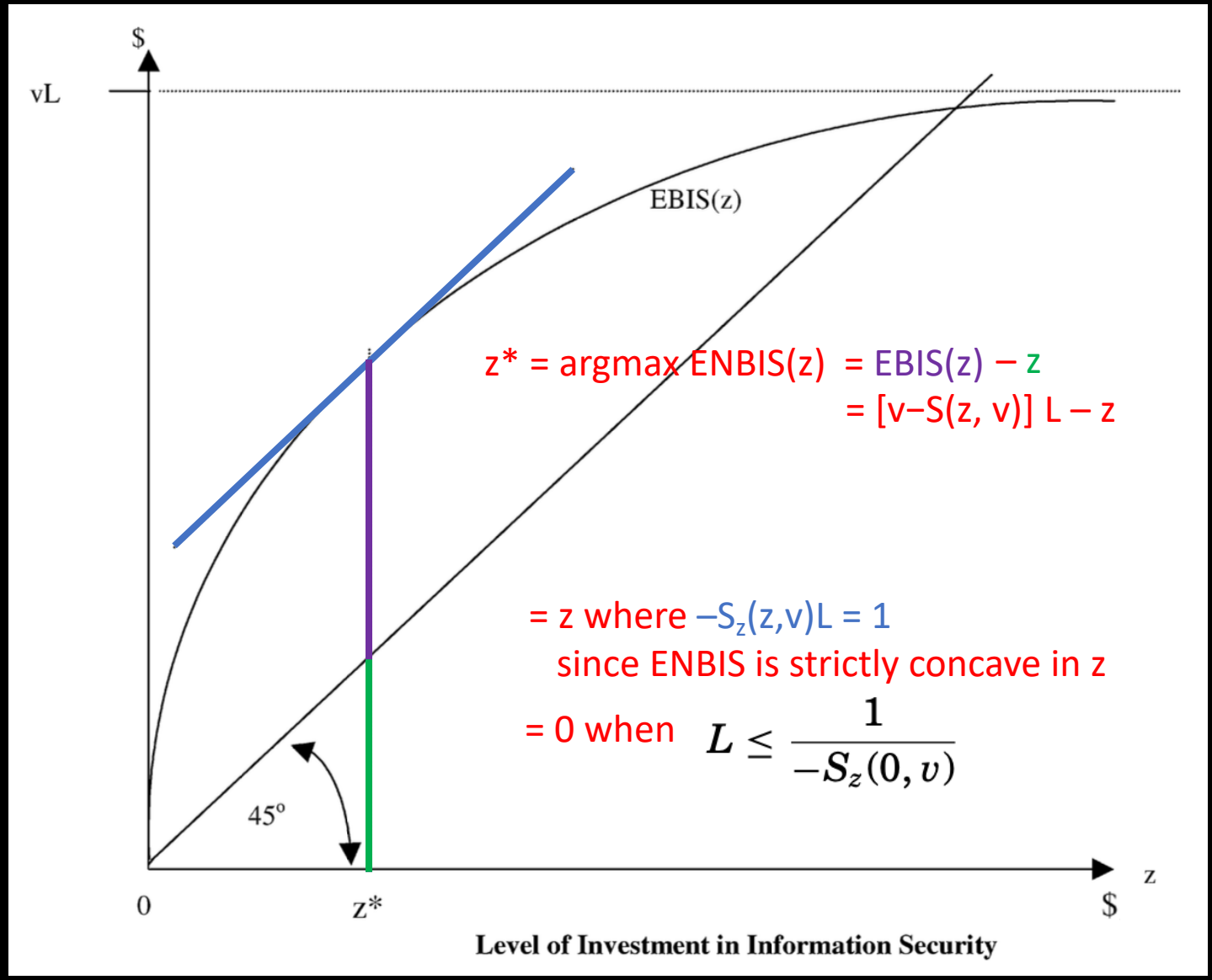
Optimizing investment

Security investments

$z > 0$	Security investment
$S(z, v)$	Security breach prob. function: effective vulnerability starting from v, given an investment z

$EBIS(z) = [v - S(z, v)] L$	Expected benefits of an investment
$ENBIS(z) = EBIS(z) - z$	Expected *net* benefits of an investment
$z^* = \text{argmax } ENBIS(z)$	Optimal investment

Benefits vs. cost of investment



Modeling scenarios

Who
- Cloud provider
- Hospital
- Bank
- Local government
- Retailer
- University
- …

Resource
- Computing / storage
- Company's sensitive data
- Customers' sensitive data

Security investment
- MFA, passkeys
- IDS or A/V
- Pen testing
- …

When might we have different vulnerability, and a different form of investment, for different resources?

Possible investments: BSIMM8

Table 1. Vulnerability prevention practices.

Problem	Practice	Usage (%)
Bugs (2)	Use a top-*N* bugs list (real data preferred).	21
	Use secure coding standards.	14
	Average (bugs)	18
Flaws (28)	Build and publish security features.	78
	Translate compliance constraints to requirements.	65
	Engage a software security group (SSG) with architecture.	64
	Create a data classification scheme and inventory.	62
	Unify regulatory pressures.	61
	Create security standards.	61
	Create (security) policy.	51
	Gather and use attack intelligence.	46
	Create an SSG capability to solve difficult design problems.	38
	Identify potential attackers.	33
	Implement and track controls for compliance.	32
	Use application containers.	27
	Identify a personally-identifiable-information data inventory.	25
	Create standards for technology stacks.	23
	Identify open source in apps.	23
	Define and use an architectural-analysis process.	13
	Build and maintain a top-*N* possible attacks list.	13
	Standardize architectural descriptions (including dataflow).	11
	Require use of approved security features and frameworks.	10
	Build attack patterns and abuse cases tied to potential attackers.	8
	Create technology-specific attack patterns.	7
	Build a capacity for eradicating specific bugs from the entire code base.	5
	Form a review board to approve and maintain secure design patterns.	5
	Have a science team that develops new attack methods.	4
	Make the SSG available as an architectural-analysis resource or mentor.	2
	Have software architects lead design review efforts.	2
	Find and publish mature design patterns from the organization.	2
	Drive analysis results into standard architecture patterns.	0
	Average (flaws)	28
	Average usage of all 30 practices	27

Table 2. Vulnerability detection practices.*

Problem	Practice	Usage (%)
Bugs (10)	*Use external penetration testers to find problems.*	87
	Ensure that quality assurance (QA) supports edge or boundary value condition testing.	80
	Have the SSG perform an ad hoc review.	63
	Use penetration testing tools internally.	62
	Use automated tools along with a manual review.	60
	Make code review mandatory for all projects.	31
	Integrate black-box security tools into the QA process.	23
	Perform fuzz testing customized to application APIs.	9
	Include security tests in QA automation.	8
	Create and use automation to do what attackers will do.	1
	Average for bugs	42
Flaws (11)	*Use external penetration testers to find problems.*	87
	Perform a security feature review.	83
	Use penetration testing tools internally.	62
	Perform a design review for high-risk applications.	28
	Integrate black-box security tools into the QA process.	23
	Have the SSG lead design review efforts.	22
	Use automated tools with tailored rules.	15
	Include security tests in QA automation.	8
	Build a factory. (Multiple analysis techniques feed into one reporting or remediation process.)	3
	Automate malicious-code detection.	3
	Create and use automation to do what attackers will do.	1
	Average for flaws	30
	Average use of all 16 practices (duplicate practices removed)	36

* Italics indicate practices that appear for both bugs and flaws.

Table 3. Vulnerability response practices.

Practice	Usage (%)
Create or interface with incident response.	84
Track software bugs found in operations through the fix process.	76
Have an emergency code base response.	72
Use application input monitoring.	45
Use application behavior monitoring and diagnostics.	4
Fix all occurrences of software bugs found in operations.	4
Average	48

- 7 prevention practices are used by more than half the firms; more motivated by compliance than impact? Could firms better use their SSG for for prevention?
- Pen testing, external and internal, extremely popular
- In general, more activities followed for detection rather than prevention – implies reactive rather than proactive security?
- For response, few firms use app behavior monitoring – missed opportunity?

Function S(z,v): how to interpret it?

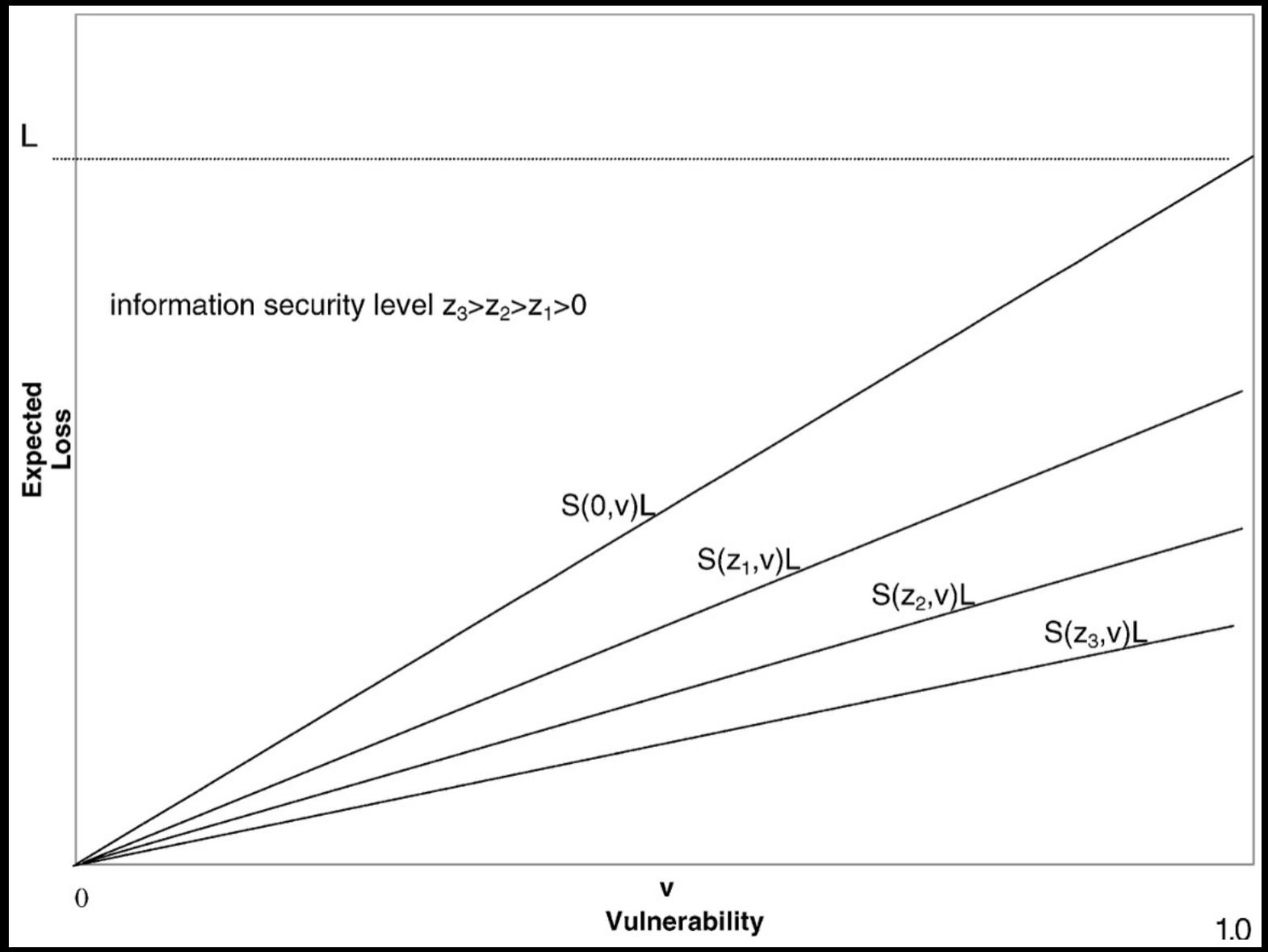
A3: For all $v \in (0, 1)$, and all z, $S_z(z, v) < 0$ and $S_{zz}(z, v) > 0$

- I.e., as the investment in security increases, the information is made more secure, but at a decreasing rate
- Assume for all $v \in (0, 1)$, *lim* $S(z, v) \rightarrow 0$, as $z \rightarrow \infty$

- Consider scenarios outlined above; which of them look like this?
  - Fixed investment cost (no incremental fixed costs)
  - Continuous reduction in vulnerability with investment cost increase
  - Can you imagine a “lumpy” cost function instead? What other shapes?

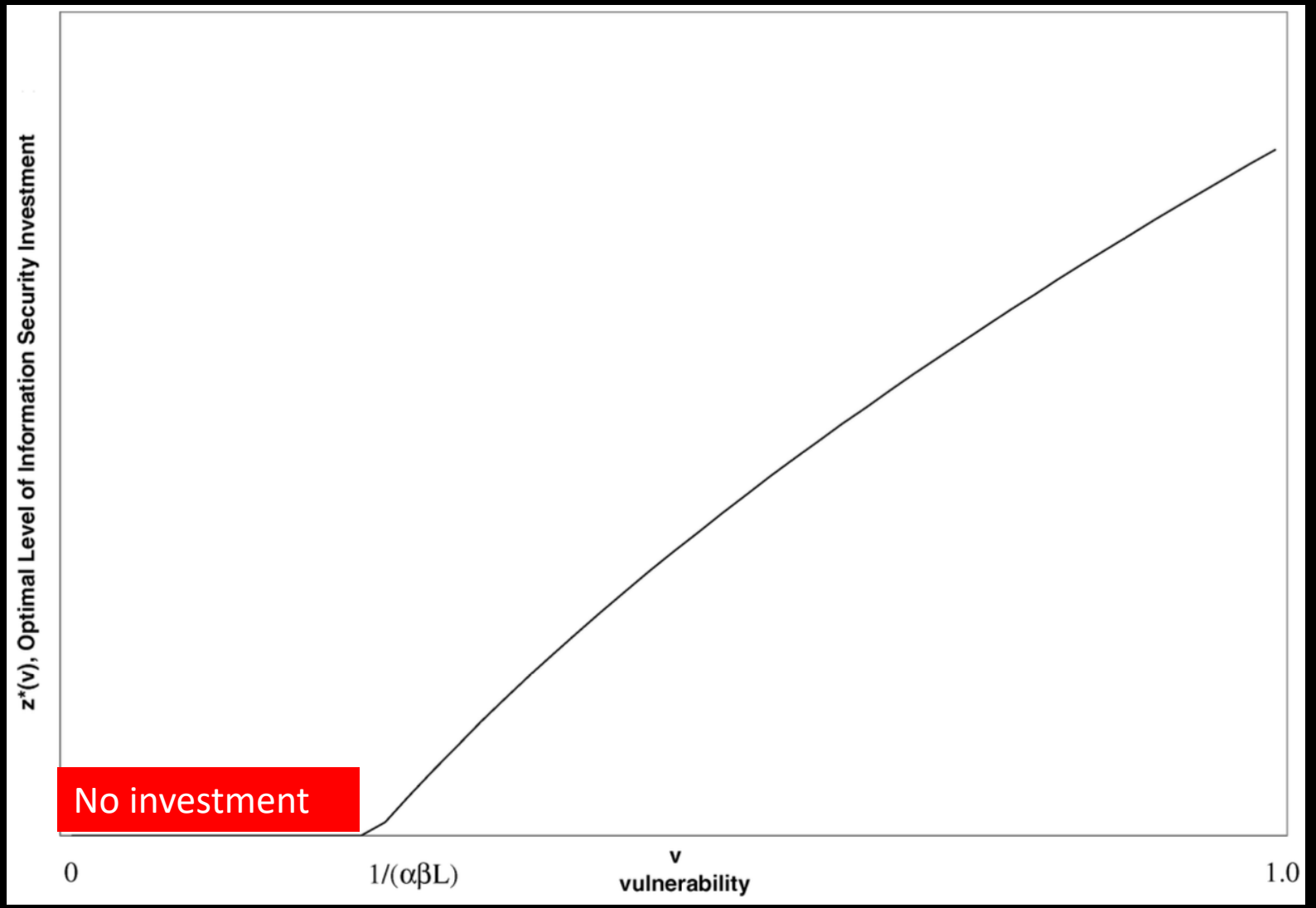
S: class I

$$S^I(z,v) = \frac{v}{(\alpha z + 1)^\beta}$$



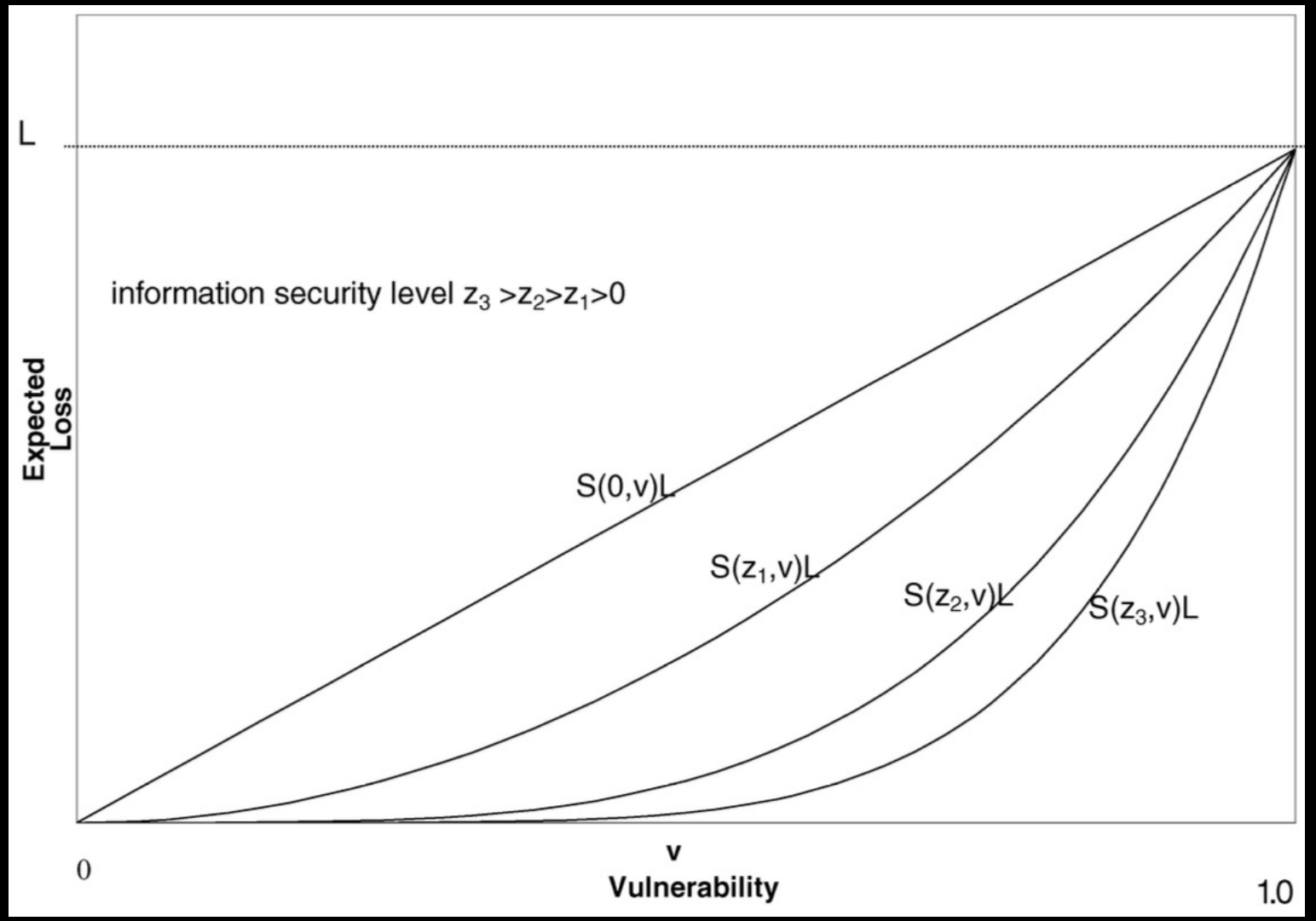
Optimal value of investment, class I

$$z^{I*}(v) = \frac{(v\beta\alpha L)^{1/(\beta+1)} - 1}{\alpha}$$



S: class II

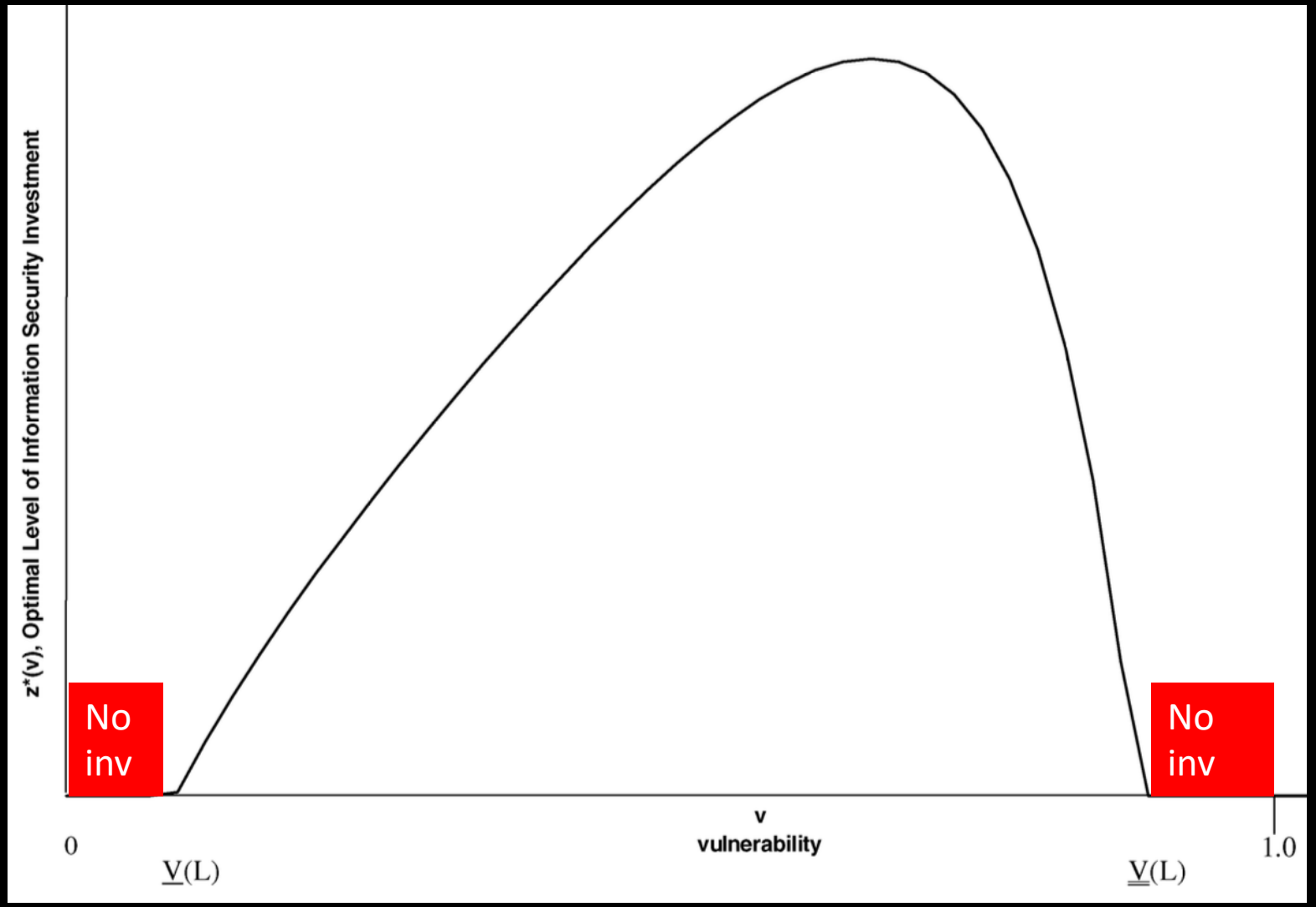
$$S^{II}(z, v) = v^{\alpha z + 1}$$



Optimal value of investment, class II

$$z^{II*}(v) = \frac{\ln(1/-\alpha v L(\ln v))}{\alpha \ln v}$$

Optimal level of investment does not weakly increase as vulnerability increases



Some takeaways

- The key in analyzing information security decisions is **not the vulnerability** v (or the **expected loss without the investment** vL), but the **reduction in expected loss** [v-S(z,v)]L **with the investment** z
- The **optimal investment amount** z* could be **well below** the **expected loss** vL
  - Theorem: If the breach probability function S(z,v) is either of class I or class II, then $z* < (1/e)\,vL = .3679vL$
  - For class I, there are scenarios where $z^* < .25vL$
- What does this mean for our modeled scenarios?

Discussion

- Do you think CISOs use the 37% rule in practice?
- Beyond what we've already discussed, what are limitations of this model?
  - What about one company's security affecting another (hello, AWS outage on Monday …)?
- What improvements might you want to make to the model, to get to the point that you could use it for decisionmaking?
  - How does it relate to the Simpson uncertainty paper?
  - How might the results change if the model considered time, e.g., ongoing attacks over time, instead of just one period?