Secure Software Development
What is Security?

Objectives

- Define Confidentiality, Integrity, and Availability
- Define authentication, authorization, auditing, and accountability
- Explain the concept of a Risk Management Framework
- Describe the steps taken in a Risk Management Framework
- Explain the relationship between Security expenses and ROI by Phase

The trinity of trouble

- Connectivity

Everything is networked.

- Extensibility

We're building things to change.

- Complexity

⇒ We are building the most complex things EVER

Security is

MSOE

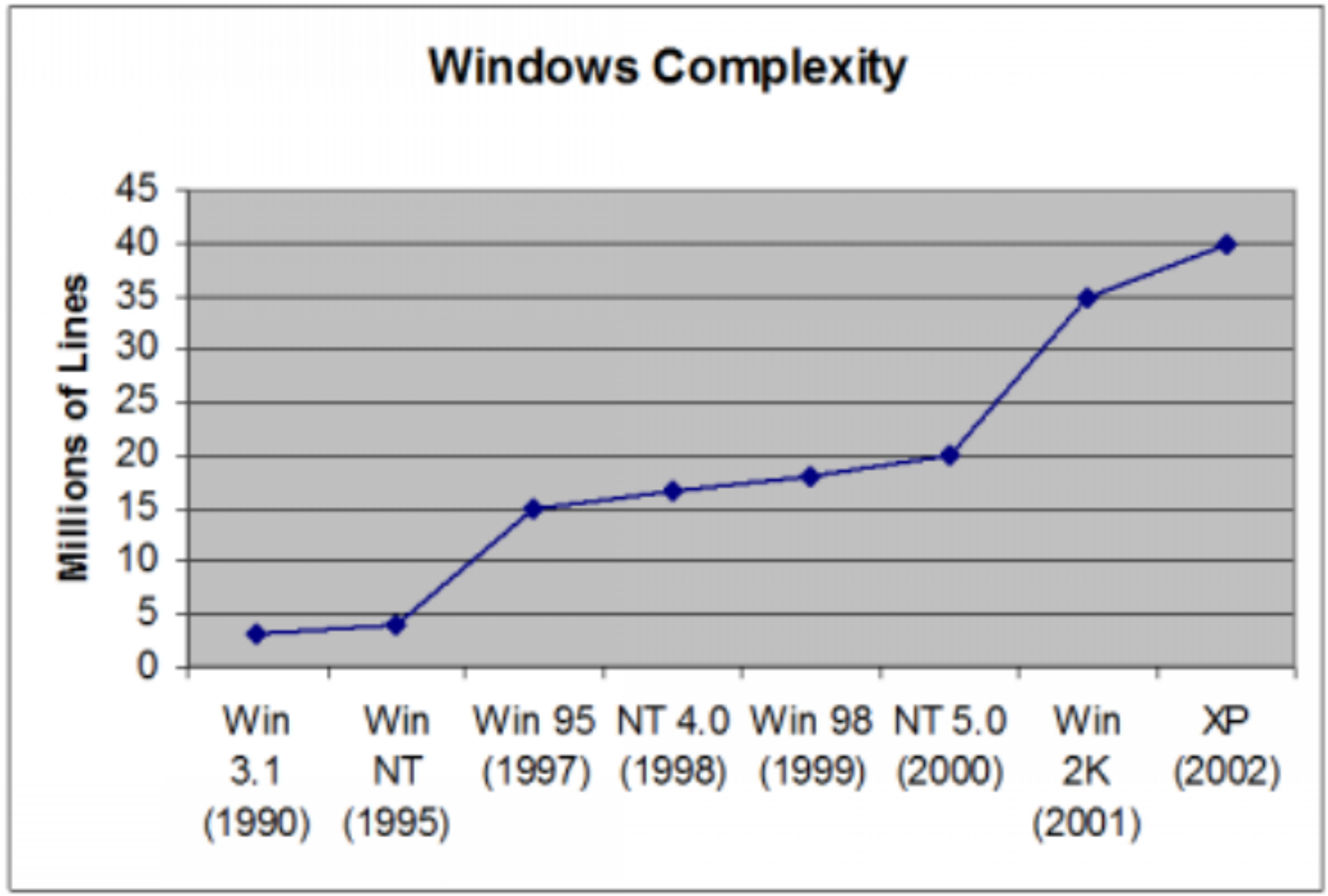
Software Complexity

5-50 bugs per/kloc[8]

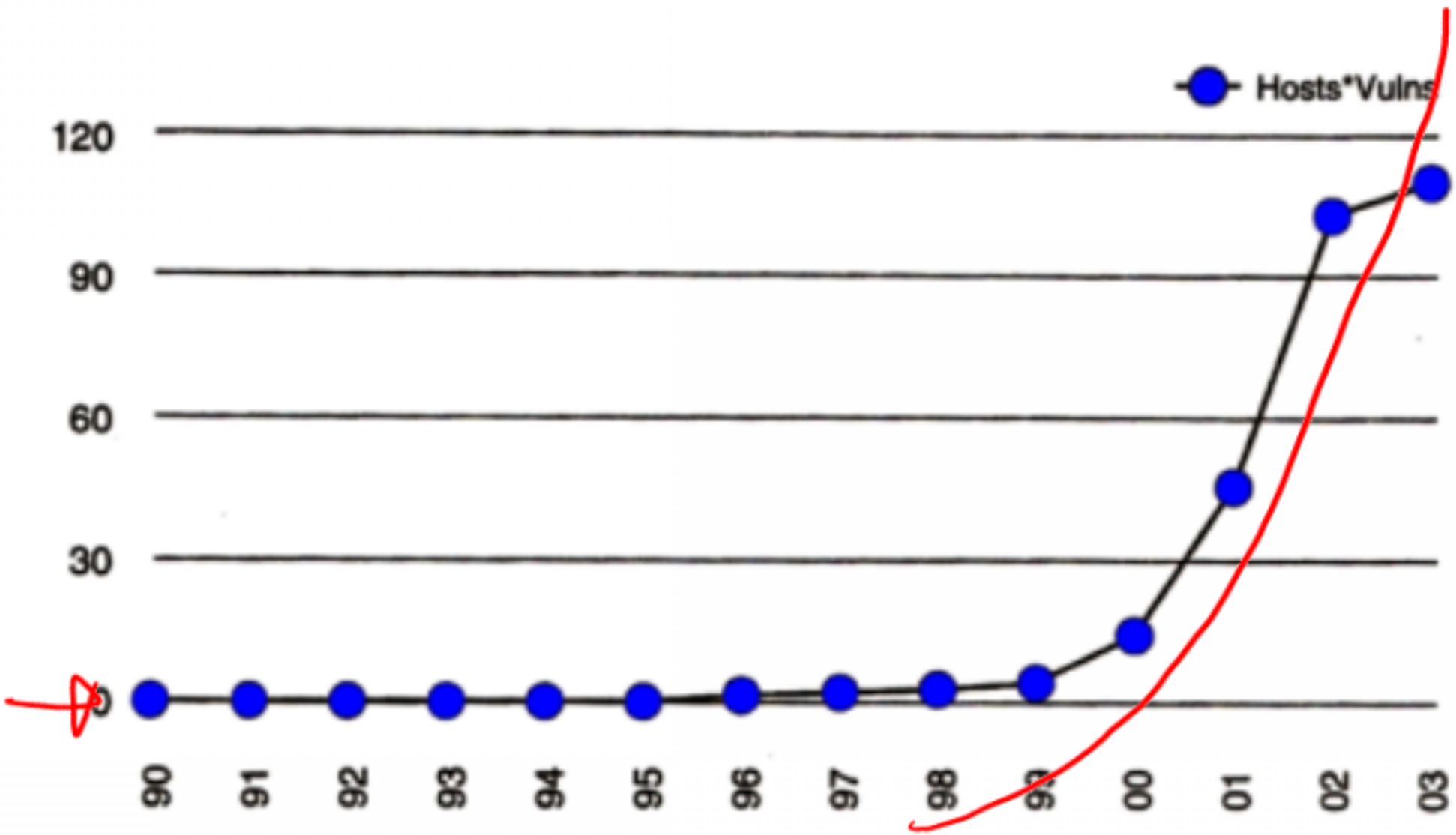
- 5/kloc: rigorous quality assurance testing (QA)
- 50/kloc: typical feature testing

System	Lines of Code
MS Word 95	2 million
MS Windows 3.1	3 million
Boeing 777	7 million
Space Shuttle	10 million
Netscape	17 million
MS Windows XP	40 million
Vista	50 million
Red Hat Fedora	6.7 million (Core) 204.5 million (Entire Distro)

Software Complexity: Windows

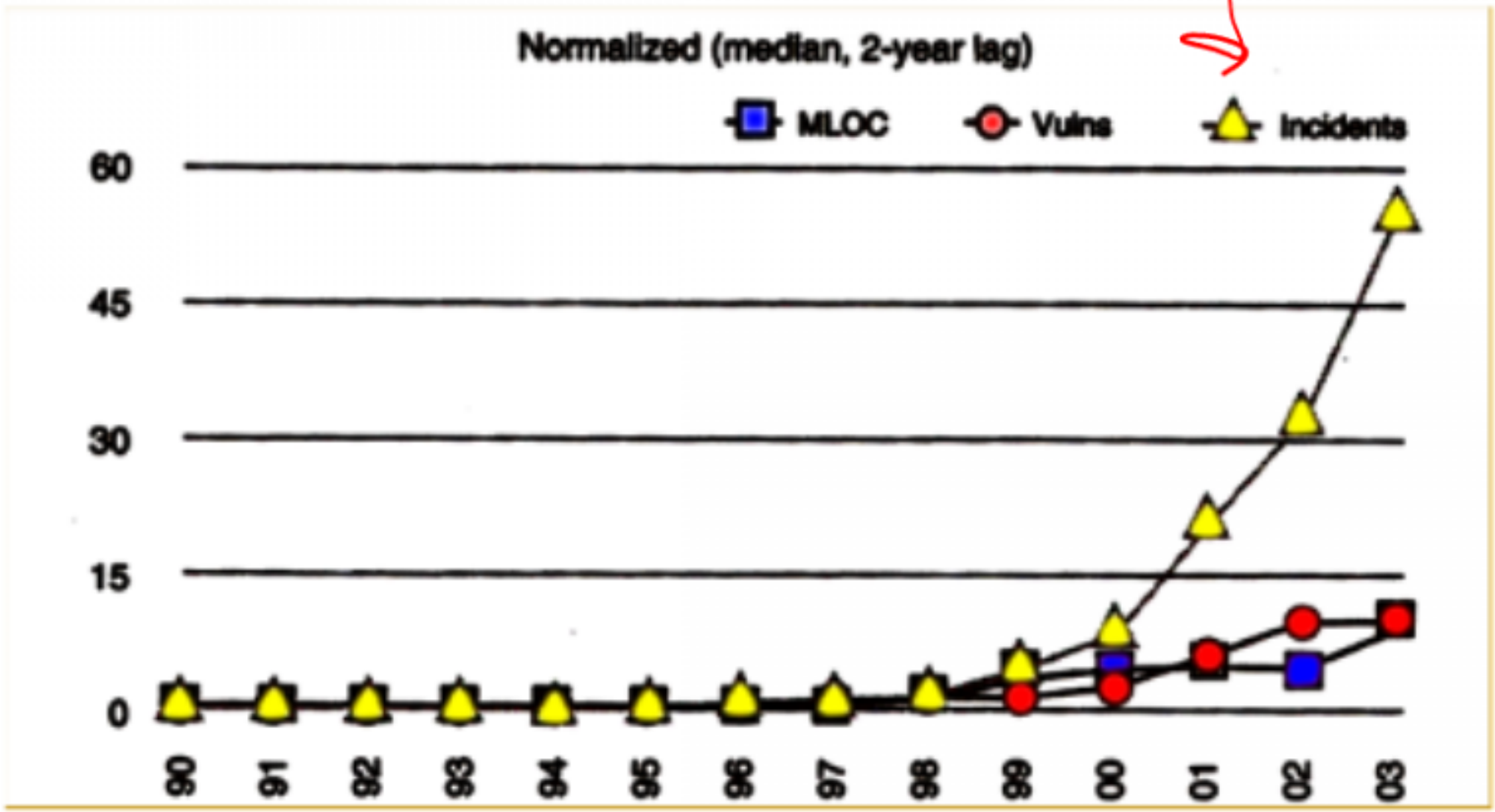


Normalized Number of security vulnerabilities

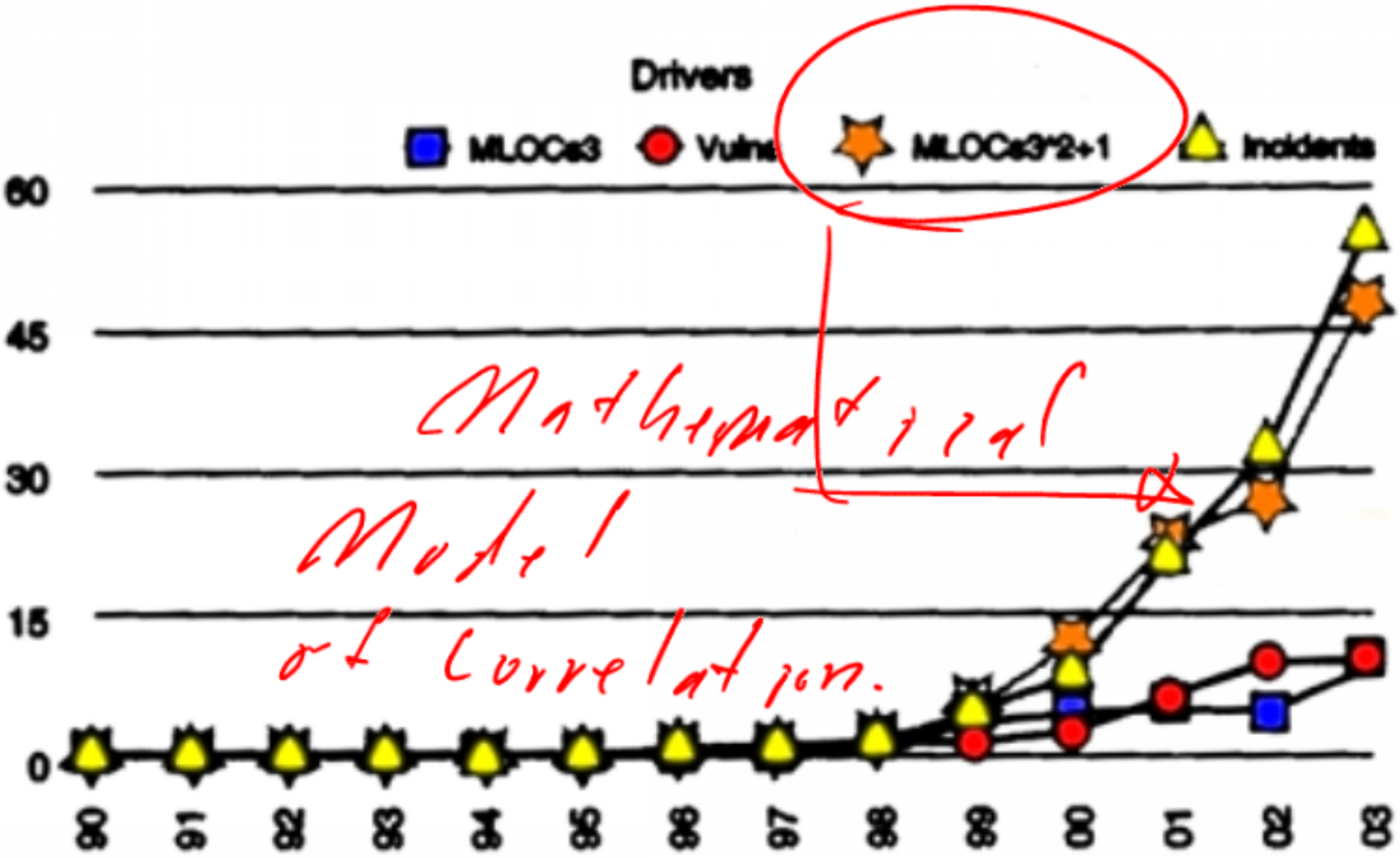


Attacks

Normalized MLOC, Vulnerabilities, and incidents



Don't believe me?



Bugs versus flaws again

Bugs	Flaws
Buffer overflow: stack smashing	Method over-riding problems (subclass issues)
Buffer overflow: one-stage attacks	Compartmentalization problems in design
Buffer overflow: string format attacks	Privileged block protection failure (DoPrivilege())
Race conditions: TOCTOU	Error-handling problems (fails open)
Unsafe environment variables	Type safety confusion error
Unsafe system calls (fork(), exec(), system())	Insecure audit log design
Incorrect input validation (black list vs. white list)	Broken or illogical access control (role-based access control [RBAC] over tiers)
	Signing too much code

Question #1

- The testing or reconciliation of evidence of a user's identity is
  a) Authorization
  b) Accountability
  c) Auditing
  d) Authentication — 1/1

A user is who they claim to be.

Question #2

- Iam Gone is a former MSOE Software Engineering student. He really wanted to graduate, but was unable to HCI. Thus, to graduate, he broke into the MSOE systems and changed his F to a grade of A for HCI, thus allowing him to graduate. This action is a violation of the systems
  a) Confidentiality
  b) Integrity — 1
  c) Availability
  d) Backup strategy

Question #3

- Iam Caught wanted to prevent a bad grade from appearing on his transcript. Thus, to prevent the bad grade from appearing, he launched a denial of service attack against my.msoe.edu. Thought unsuccessful, his attempt was an attack against system

a. Authentication
b. Confidentiality
c. Integrity
d. Availability

Confidentiality

- Refers to the prevention of intentional or unintentional disclosure of information
- The security concept dealing with protection against unauthorized information disclosure

- The measure of software resiliency
- Requires 3 principles be met
  - Modifications are not made by unauthorized personnel or process
  - Unauthorized modifications are not made to data by authorized personnel or processes
  - The data is internally and externally consistant

Integrity

How well does the system keep up.

Do not change things w/ out proper process/procedure

MSOE

Availability

- Ensures that reliable and timely access to data or computing resources can be made by the appropriate personnel

- Data must not be available to the wrong people at the wrong time

- Security is Risk Management

What is security?

Mitigate the most serious risks to the system

Risk Management Framework

- Deals with
  - Identifying => Figuring out what risks we face.
  - Tracking => Always know our vulnerabilities
  - Mitigating => Put something in place to lessen the risk.
- Requires us to also keep in mind the concept of impact

Risk Management Framework

"Brainstorming"

Figuring out what risks we face.

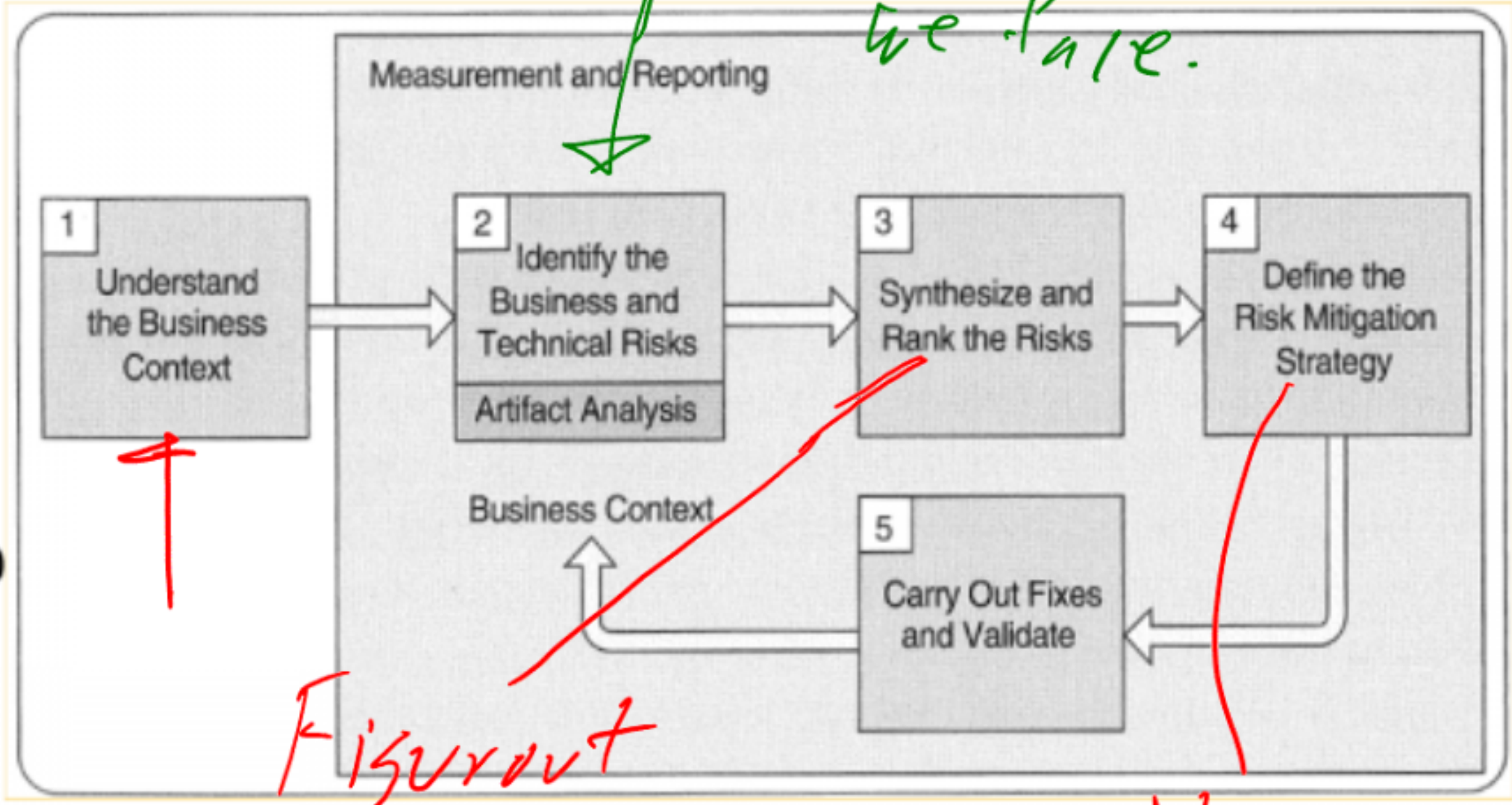
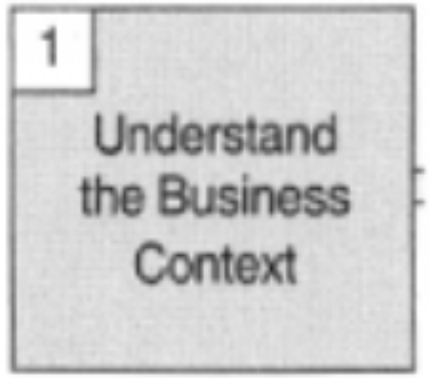


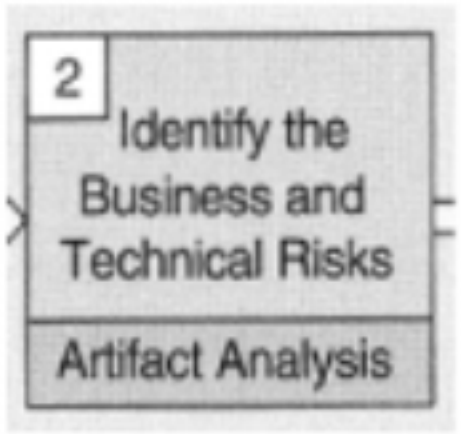
Figure out which to fix first.

How to patch the problem

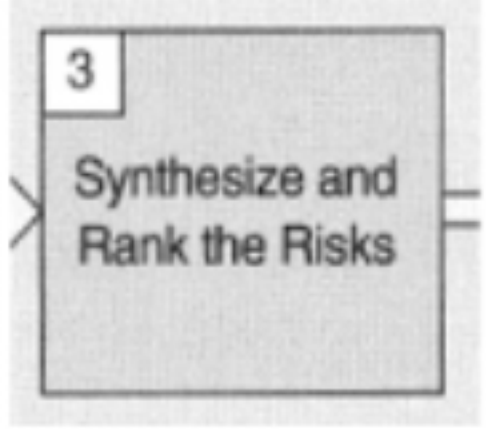
Understand the business context



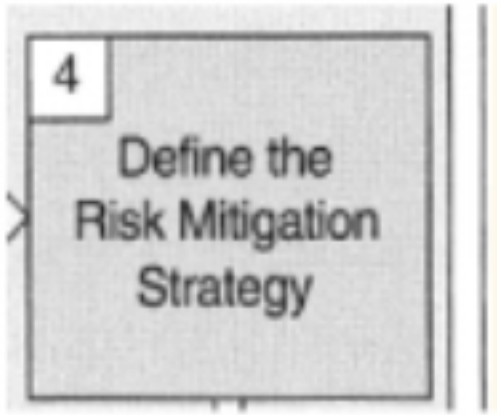
Identify the Business and Technical Risks



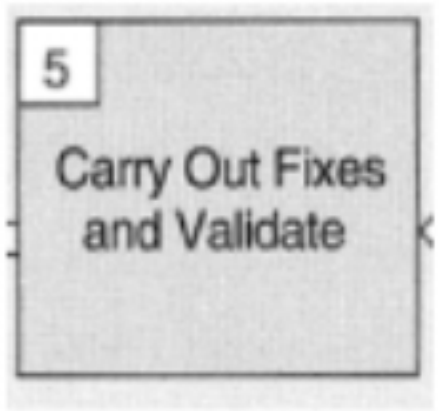
Synthesize and Rank



Define the Risk Mitigation Strategy



Cary out Fixes and Validate



Business Case Example

- Mayo Clinic

Larger, more patients

More points of attack.

More reasons for one's records to be accessed.

- Corner Hospital

One Location

Smaller IT staff