Damages and Expenses caused by Viruses

- Direct damages
- Indirect damages
- Virus protection expenses
- Costs caused by the damage
- Case example: Code Red

Direct damages

- Corruption of files
  - Interesting example `W32/Perrun A` corrupts images
- Manipulation of data
- Mass mailing `foobar` information
- Memory consumption (Active and running viruses)
  - Memory resident vs. non memory resident viruses
- BIOS corruption (CIH)
- Even physical hard-disk damage?

Indirect damages

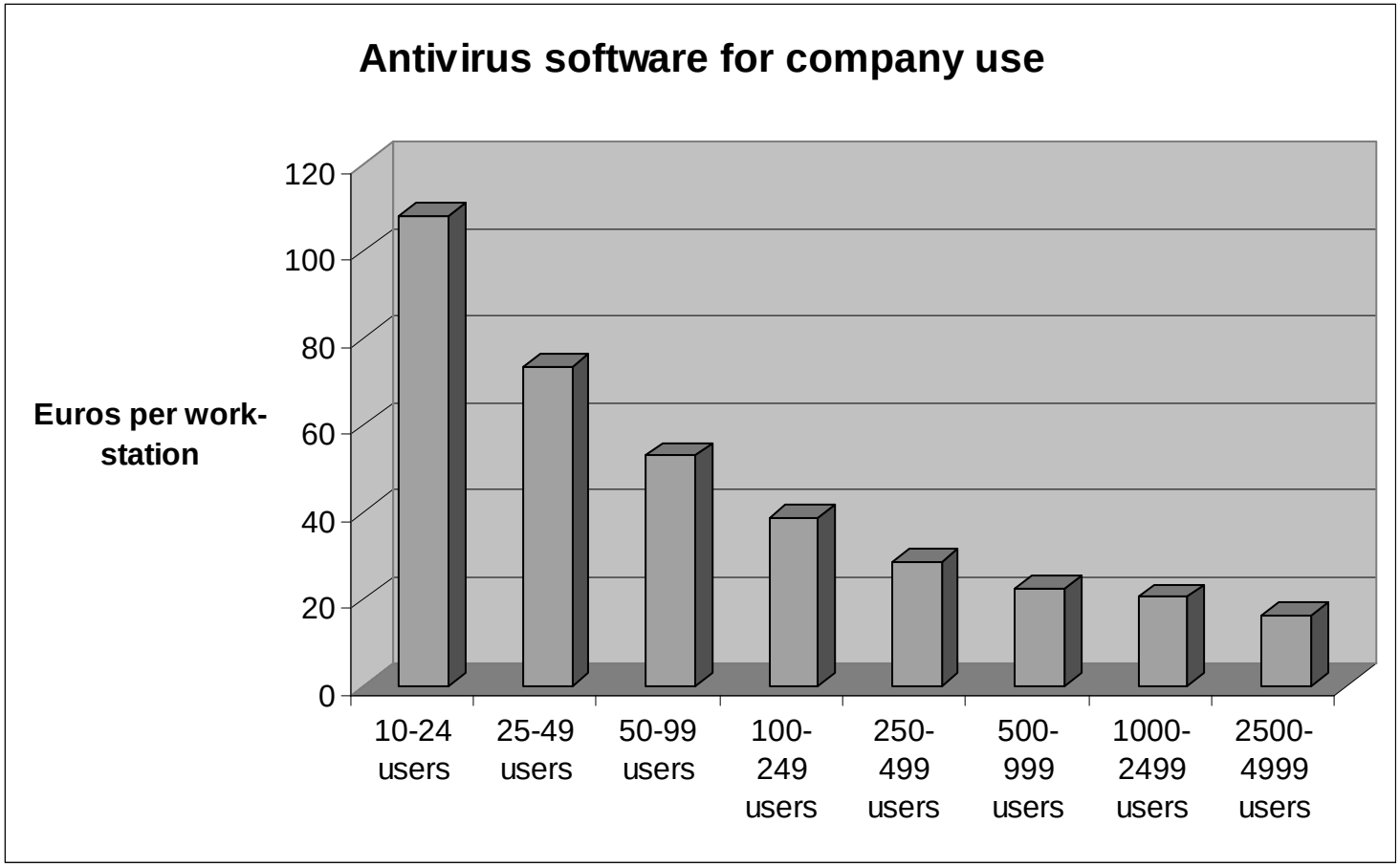
- Bandwidth consumption (scanning, DDoS stream)
- Enable DoS-attack against third party (Code Red var.)
- Enable backdoor to secure network (Code Red variants)
- Disabled services (E-mail, web sites)
- Decreased productivity
- Loss of confidence

Virus protection expenses

- Virus protection software costs
- Slight loss of productivity?!
  - Installation and maintenance of antivirus software
- Slight loss of hardware resources?!
  - Processor capacity and memory comsumption

Software expenses

F-Secure Anti-Virus Total Suite 2001

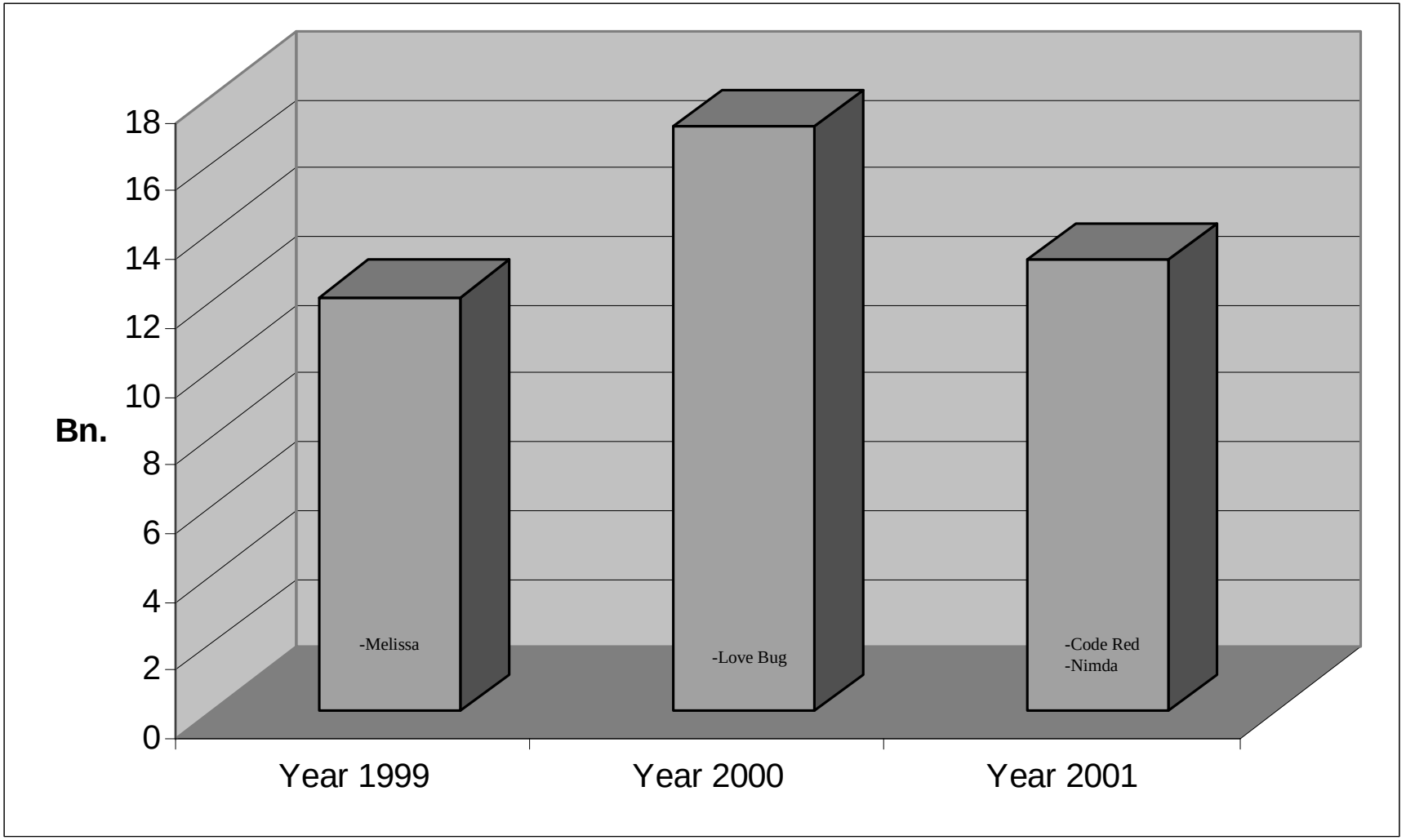


Costs caused by the damage

- Loss of information
- Significant loss of productivity
  - Lost work days
  - Recovery time
- Loss of confidence
  - Might explain why most of the attacks are not reported

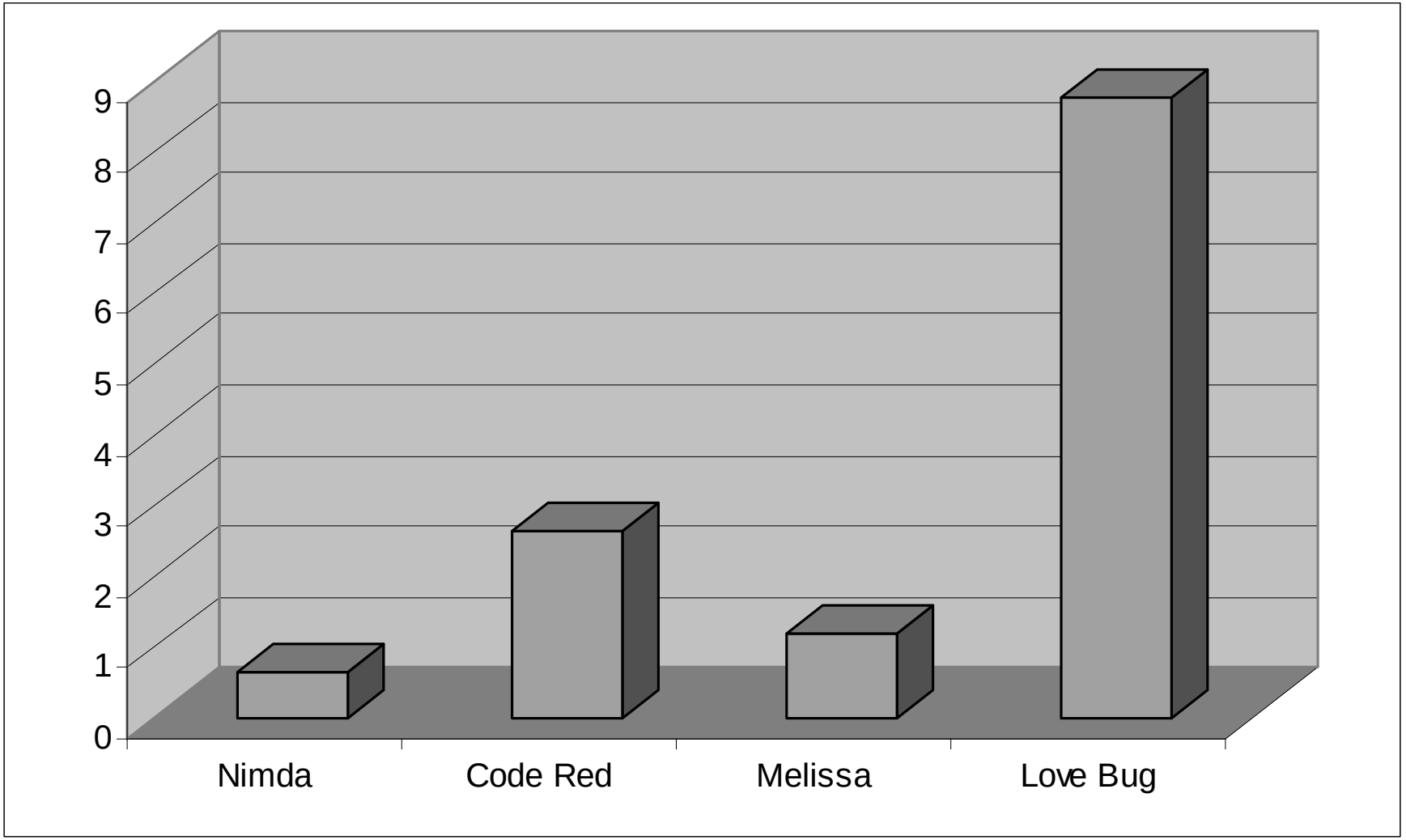
`Guesstimated` costs for viruses 1999 - 2001

Computer Economics 2001

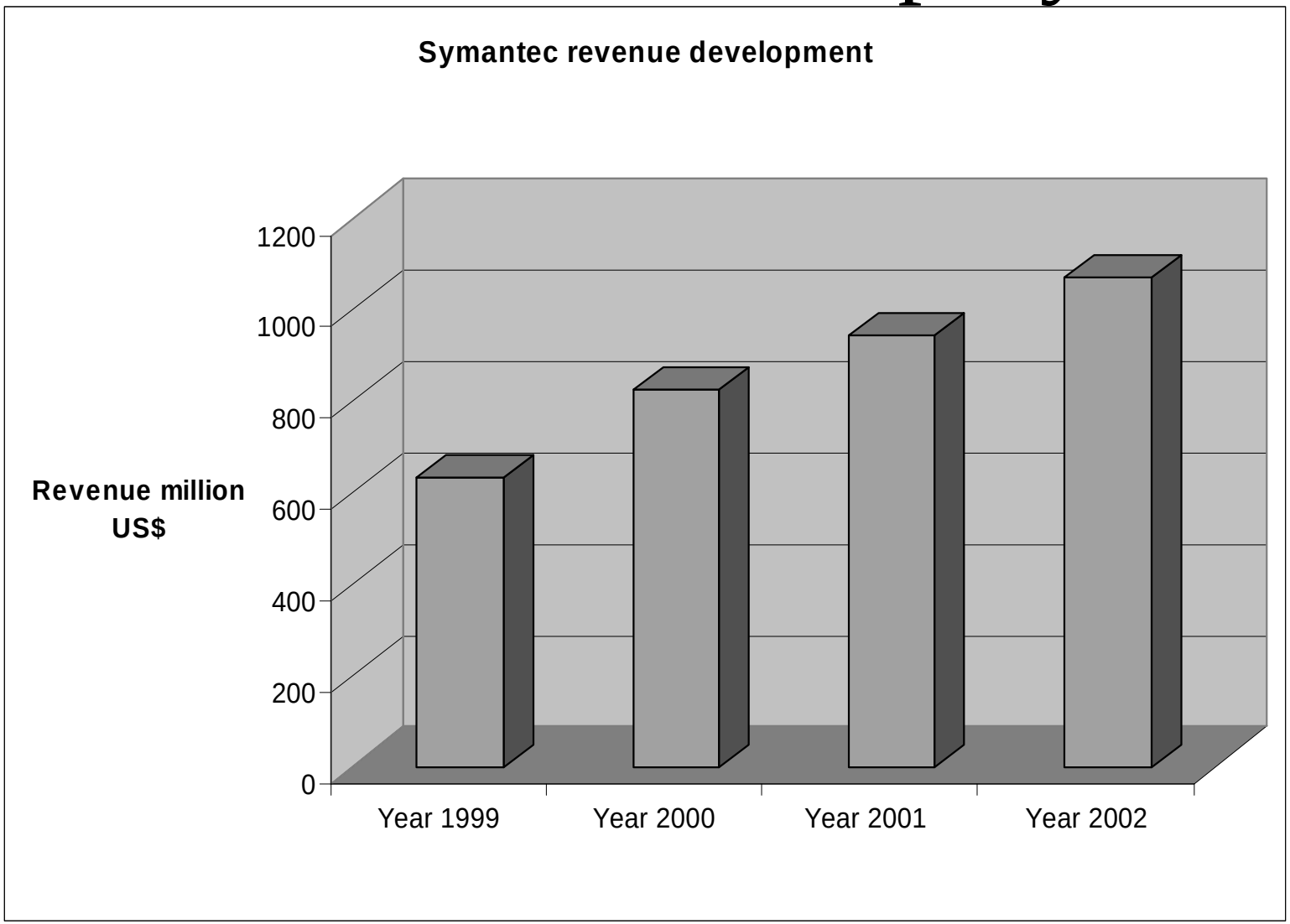


`Guesstimated` costs per virus

Computer Economics 2001



Revenue development of an antivirus company



Estimated costs of virus attack in an average company

Statistics: ICSA 2000

- 84 percent of virus infected companies end up to:
  - More than 20 lost work days
  - more than 50 hours for recovery
  - average costs `guesstimate` exceed 10,000 $
  - Reported losses of productivity up to 70% during the attack
  - Lost information (of infected files) up to 40%

- In comparison: Annual expenses for antivirus software in a mid size company with 300 workstations `guesstimate` 7500 $

Case Example: CODE RED

- Virus infected Microsoft Windows 2000, Windows NT or versions 4.0 or 5.0 IIS servers using a code bug in the Microsoft OS
- Virus was worm type: no human intervention needed to spread
- Infected servers scanned local IP-networks for other vulnerable workstations (causing network traffic)
- Initialised a DDoS-attack against certain websites using (or trying to use) 250.000 infected servers / workstations
- Did not actually damage the infected workstations
- Data flood slowed some links `in the Internet` by 40%
- Protection / recovery required installing an update patch and booting the infected workstation
- Estimated costs worldwide 2.62 billion $

Damages and costs conclusions

- Damages have explicit nature
- Prevention and antivirus software expenses can be measured as well
- Costs of virus damages are hard to measure
  - "users are unable to estimate the damage a virus outbreak might cause their own company ... so how does a third party get a figure?” Alex Shipp, MessageLabs
  - "As well as lost productivity, viruses can also cost money through damaged credibility, effects on customer relations and attacks on confidentiality which is hard to estimate.” Alex Shipp, MessageLabs
- Preventing virus attacks in advance is most likely a good investment