The Benefits of a Notification Process in Addressing the Worsening Computer Virus Problem

Joan L. Aron

DIMACS Working Group Meeting on Analogies between Computer Viruses and Biological Viruses

June 10-13, 2002

Popular Culture

- Cnet's Top Ten Signs that You're a Computer Virus
  - (#5) You had a DNA test … and it consists of zeroes and ones.
  - (#3) You work only one day a year, and (whaddayaknow?) it's on Michelangelo's birthday.

Scientific Stock Images

- www.rkm.com.au
  - Viruses (HIV, Smallpox, Ebola, etc.)
  - Bacteria (Bacillus anthracis - anthrax, etc.)
  - Parasites (Cryptosporidium, Giardia)
  - Prions (bovine spongiform encephalopathy)
  - Cells
  - Medical
  - Astronomical Illustrations
  - Computer Virus Graphics !!!

Published Article

The Benefits of a Notification Process in Addressing the Worsening Computer Virus Problem: Results of a Survey and a Simulation Model

Computers & Security 21 (2): 142-163 (2002)

Authorship

- Joan L. Aron (Science Communication Studies and JHU Public Health)
- Michael O'Leary (Towson Univ. Math)
- Ronald A. Gove (SAIC, now GWU Computer Science)
- Shiva Azadegan (Towson Univ. Computer Science)
- M. Cristina Schneider (Epidemiological Consultant, now PAHO)

ANALOGY S.S.

Antiviral Software Use Immunization

Immune System Strengths

- The immune system can respond to agents during a first encounter.
  - Evolving threat
- The immune system can operate "in the background" without knowledge or directed action.
  - No environmental or behavioral change
  - Computer users as unreliable component of information system security

Immune System Weaknesses

- Can be evaded
  - HIV replication
  - Pharmaceutical industry existence
- Can fire at the wrong target
  - Autoimmune disease
  - Penicillin anaphylaxis

Digital Immune Response

- BENEFIT of a centralized system to automatically remove recognized and novel computer viruses
- DANGER of "authorizing a centralized system to pull files -- including those that may be misidentified as viruses -- from a client's computer and then deposit unfamiliar code from a remote server onto the client's system"

Computer Virus Control

Disease Control

Disease Control

- Immunization
- Drug Therapy
- Human Behavior
- Host Factors
- Environment

Computer Virus Control

- Antiviral Software
- User Behavior
- Organizational Behavior
- Computing Environment

Antiviral Software Roles

User Awareness

Aware of What ?

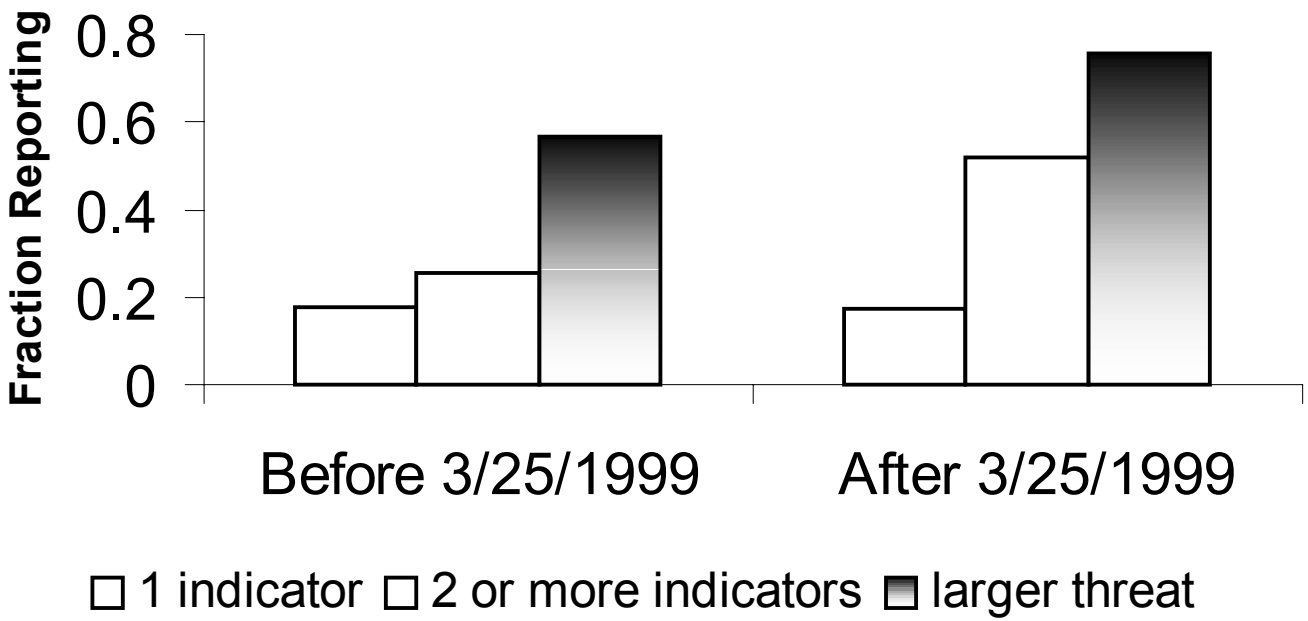
How Aware ?

Survey Results

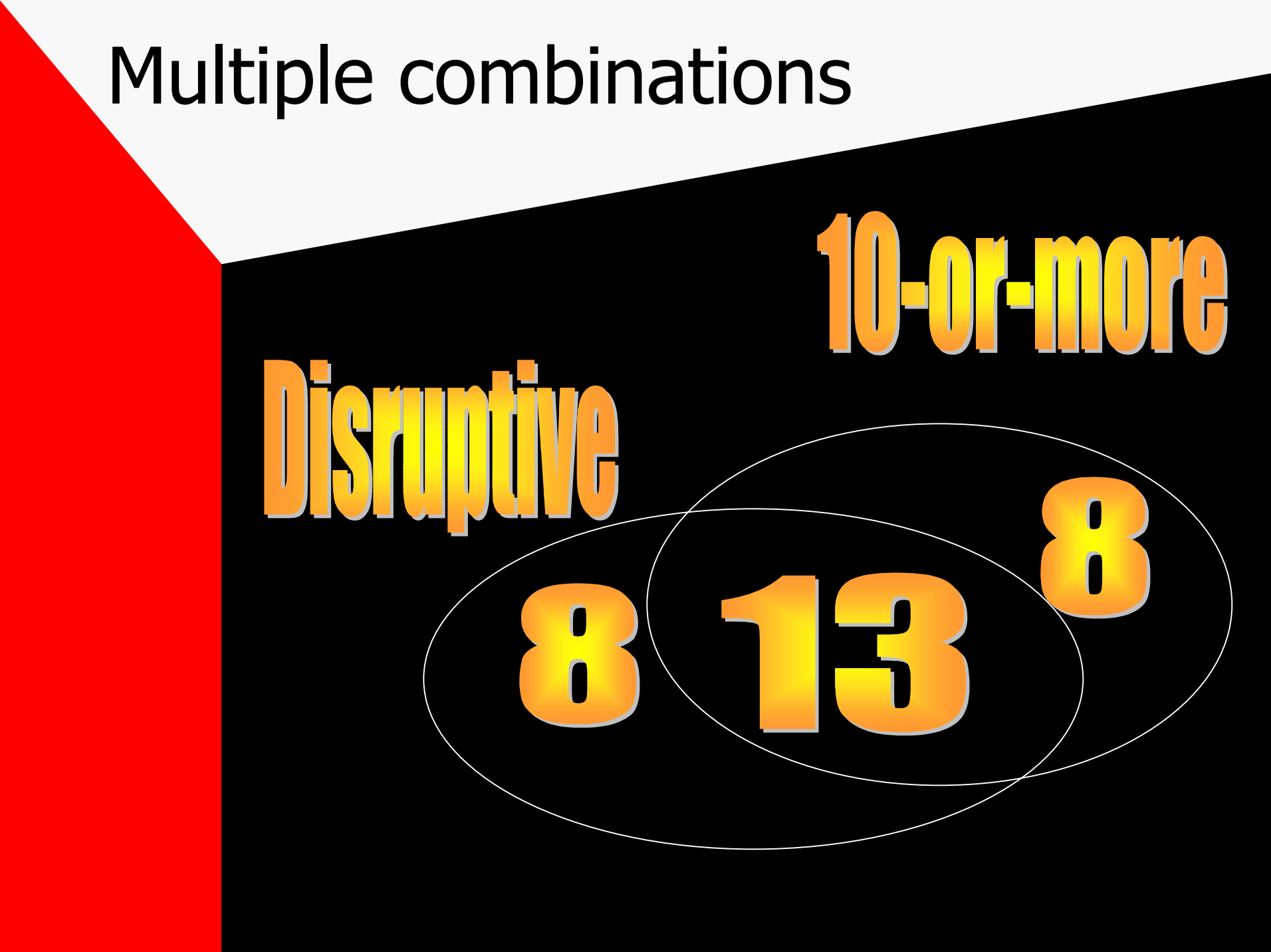
Severity Indicators / Threat

- Computer virus incidents frequent
- Computer virus incidents disruptive
- Infect at least 10 workstations
- Persist for a month or longer
- Recur at least one month after cleanup
- Total disruption or unrecoverable loss
- Threat perceived as getting worse

Increasing Severity and Perceived Threat



Multiple combinations



Effort to Update Software

- Q3.17 If your workgroup experienced virus problems over the past 12 months, what factors do you consider responsible?
- Antiviral detection software ineffective DESPITE regular updates
- This answer by 15% to 21% of respondents reporting virus problems in workgroups using antiviral software

“New” or “Old” Viruses?

- By implication, the majority (80%) of computer virus problem could be eliminated if systems regularly updated antiviral software. The problem of “old” viruses is largely preventable.
- How much of the problem is actually due to “new” viruses?

“Undetectable”?

- Why did system fail to detect?
  - Improper configuration of software
  - Inability of one antivirus detector to detect at a specific time
  - Inability of all known antivirus detectors to detect at a specific time
  - Need to understand reason for failure in order to improve system
  - Limited empirical data base

Simulation Results

Simulation Assumptions

- Antiviral software can detect viruses
- 200 workstations with randomly-selected communication events
- Exposure to viruses from “outside”
- E-mail, network connection, floppy disk
- Word Macro, Excel Macro, Generic .exe, and Boot Sector virus types
- Clean up viruses from computers

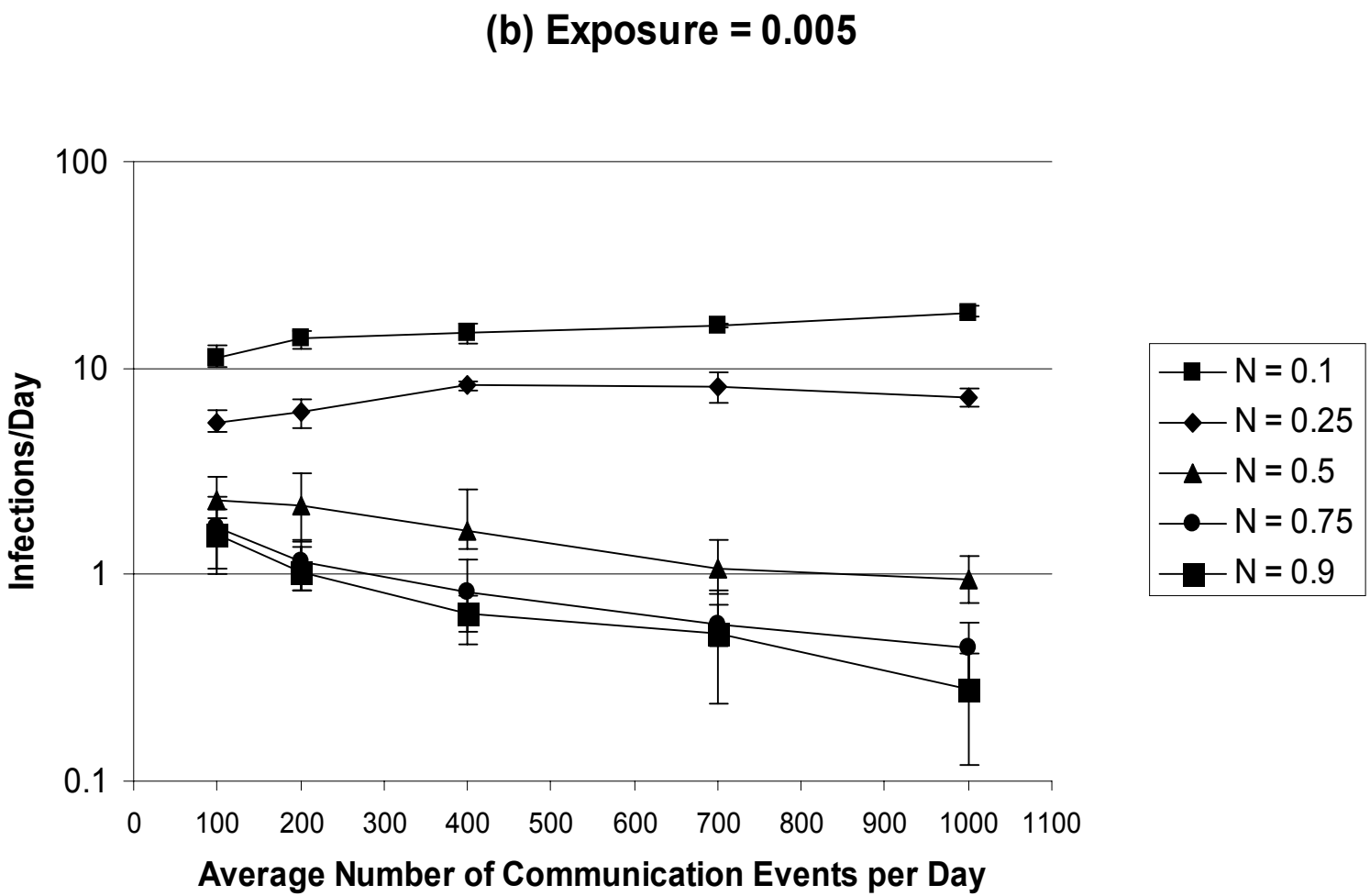
Simulation Parameters

- *Comm* is the mean daily number of communication events that have the potential to transmit computer viruses
- *AV* is the fraction of workstations with effective antiviral software (80%, 95%)
- *Notify* is the probability that a message recipient who has detected receipt of a virus from within the workgroup notifies the sender and system administrator

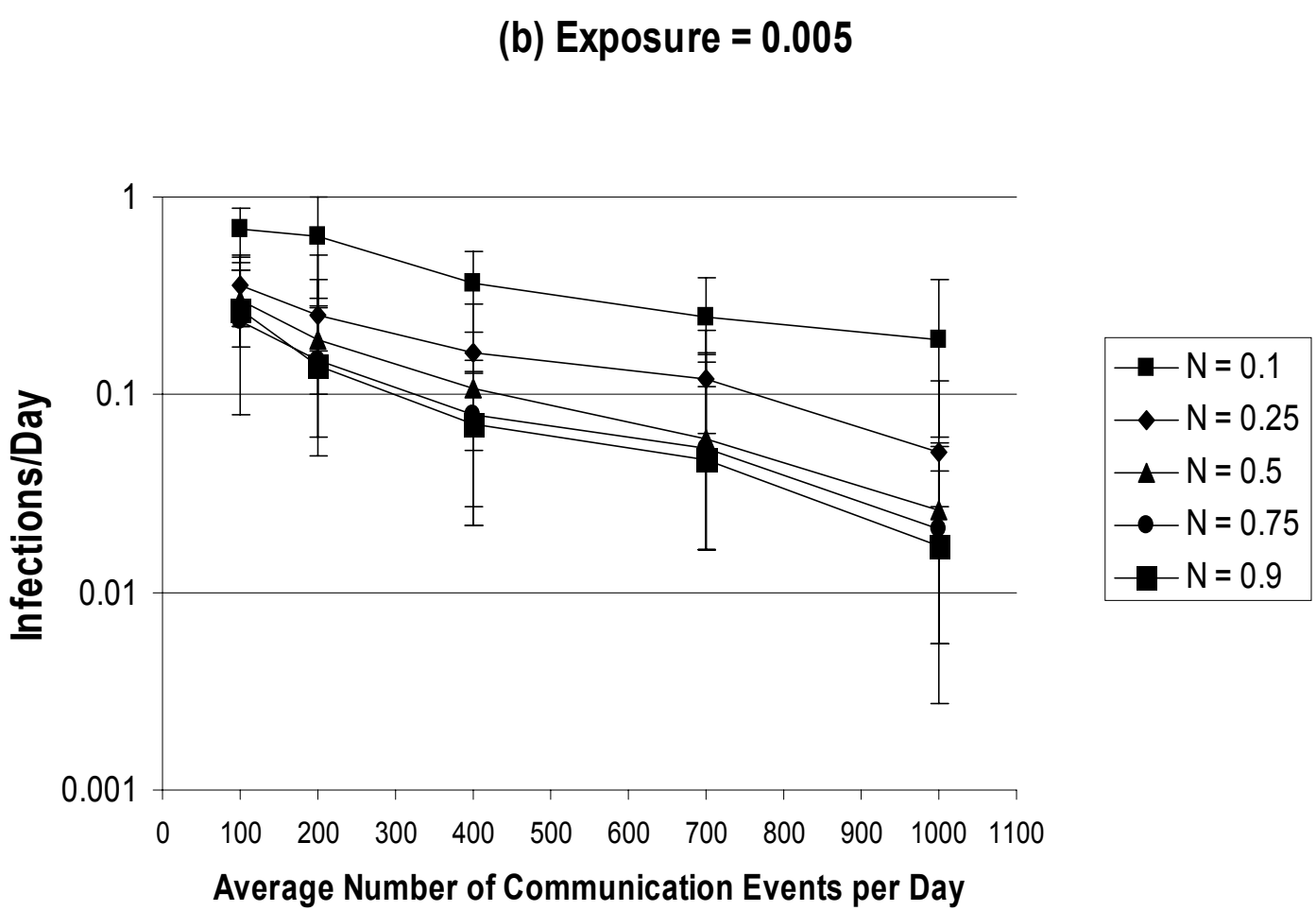
Simulation Runs

- Run 365 simulated days
- Average daily number of infected workstations
- Run simulation with five different sets of seeds for random number generators, with range of results shown as “error bars”

AV = 80%


(b) Exposure = 0.005
100
10
1
0.1
Infections/Day
0
100
200
300
400
500
600
700
800
900
1000
1100
Average Number of Communication Events per Day
N = 0.1
N = 0.25
N = 0.5
N = 0.75
N = 0.9

AV = 80%


(b) Exposure = 0.005
Infections/Day
1
0.1
0.01
0.001
0
100
200
300
400
500
600
700
800
900
1000
1100
Average Number of Communication Events per Day
N = 0.1
N = 0.25
N = 0.5
N = 0.75
N = 0.9

AV = 95%

Analytical Approximation

Prevalence of infection

Consider workstations without effective antiviral software.

y is fraction with infection

Increase prevalence by 1) infection from outside workgroup and 2) infection from inside workgroup.

Decrease prevalence by cleanup.

Prevalence of infection

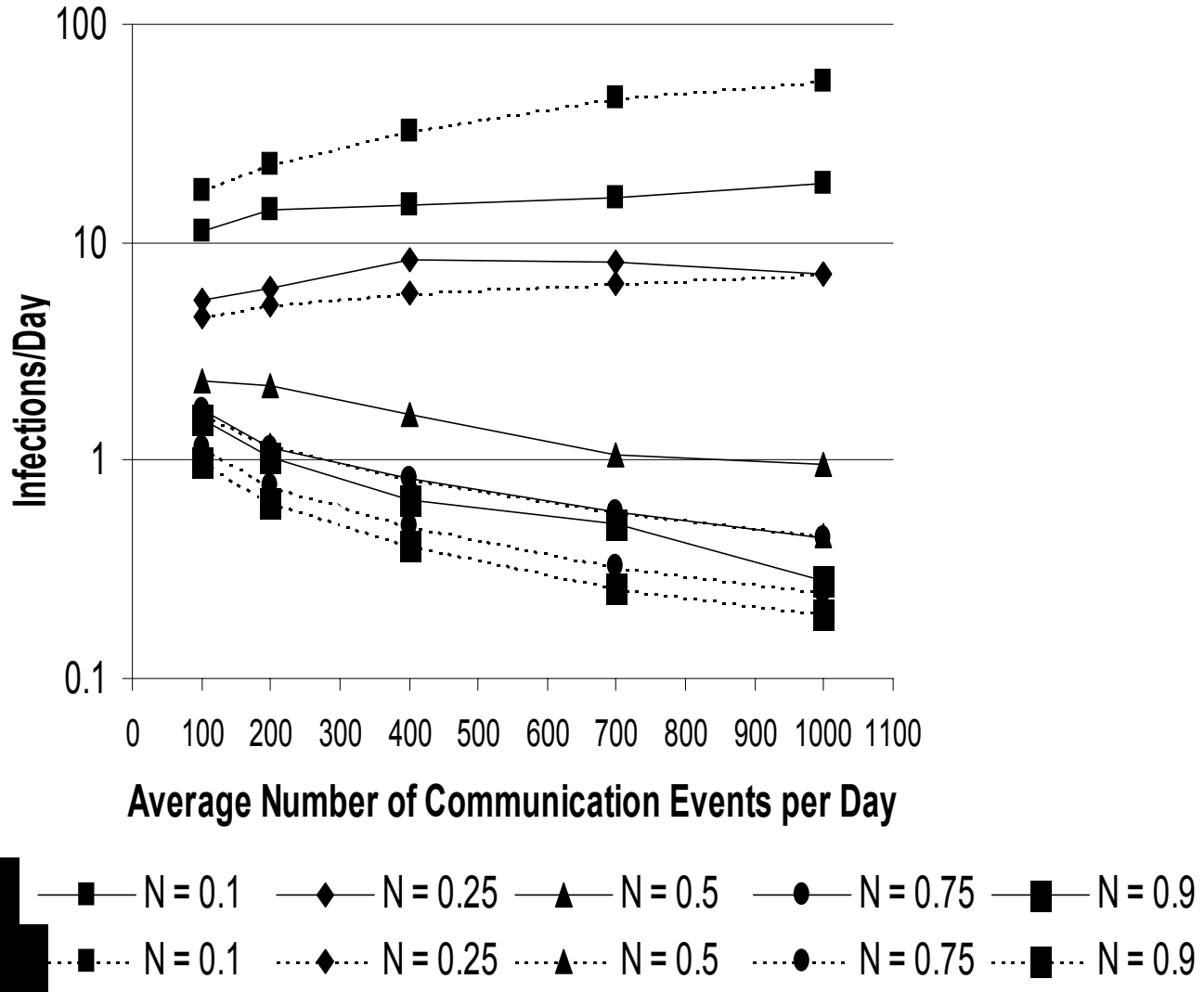
$$dy/dt = c_v (1 - \alpha) x y - \gamma_v y + \lambda G_V x$$

where $x + y = 1$

(Refer to publication.)

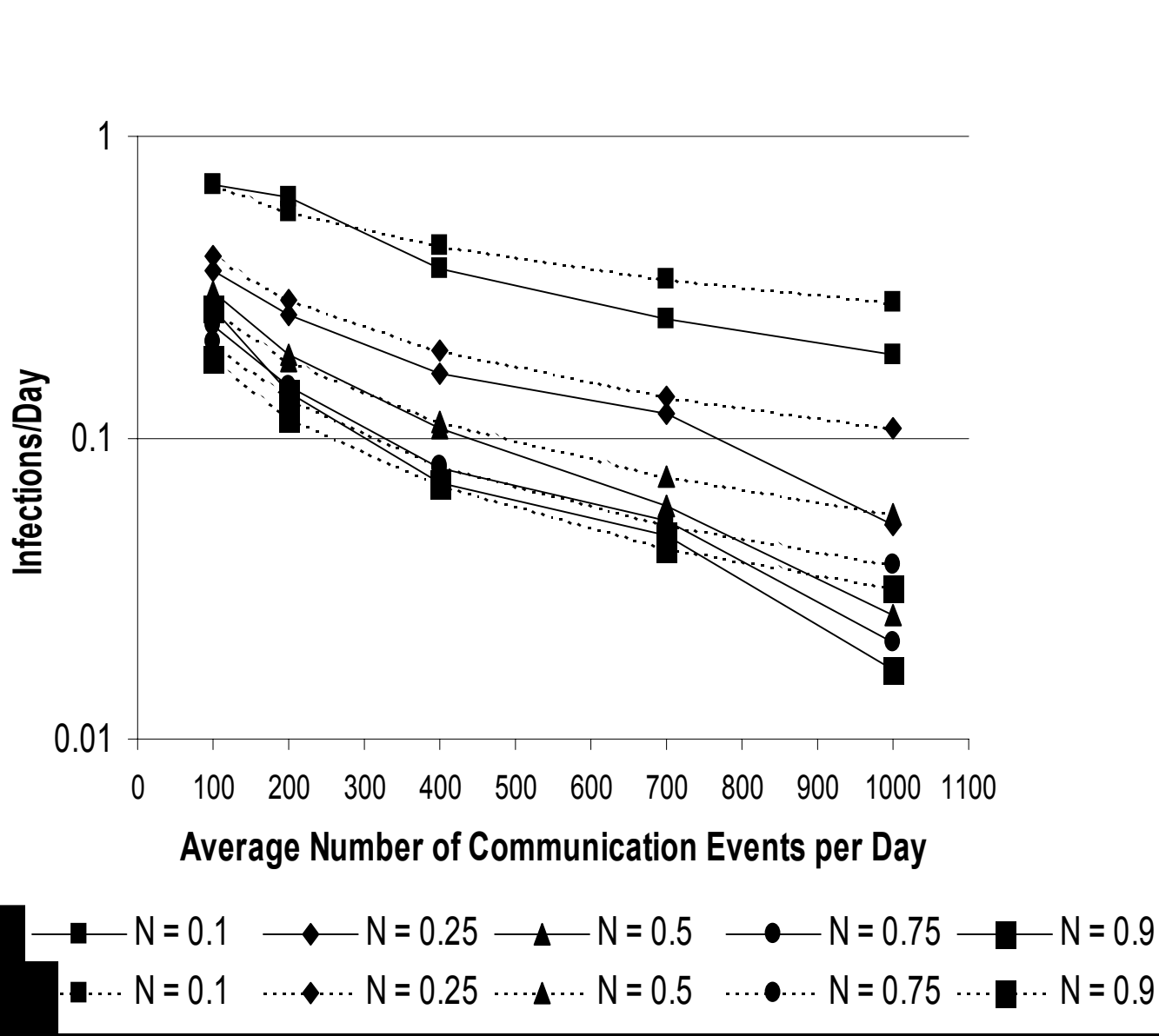
Calculate equilibrium prevalence for each of four virus types and add them up.

(b) Exposure = 0.005



Sim

Analytical


(b) Exposure = 0.005
1
0.1
0.01
Infections/Day
0
100
200
300
400
500
600
700
800
900
1000
1100
Average Number of Communication Events per Day
N = 0.1
N = 0.25
N = 0.5
N = 0.75
N = 0.9
Sim
Analytical

Basic Reproduction Ratio

For each type of computer virus:

$R_v = c_v (1 - \alpha) / \gamma_v$

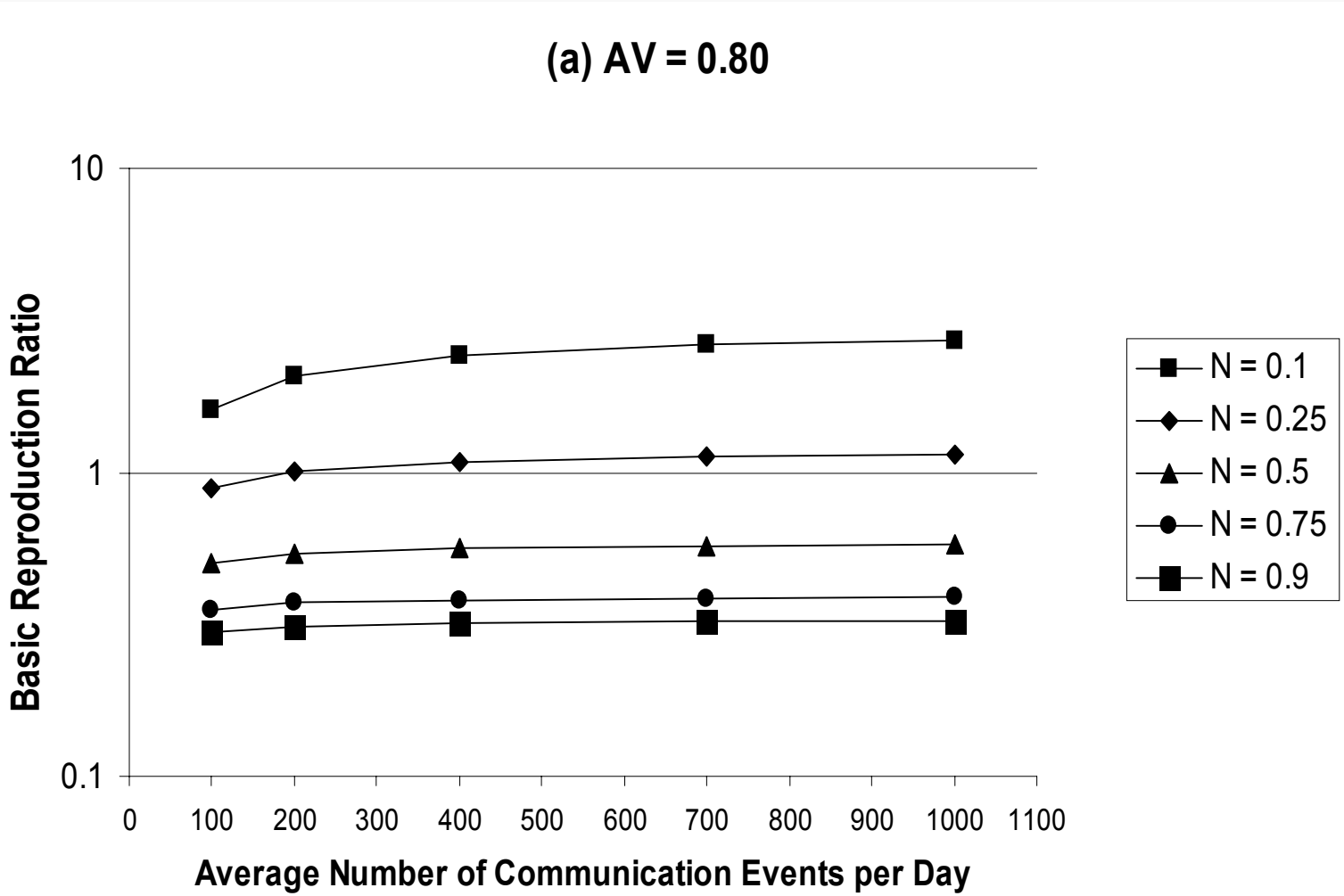
$W_v = \lambda G_v / \gamma_v$

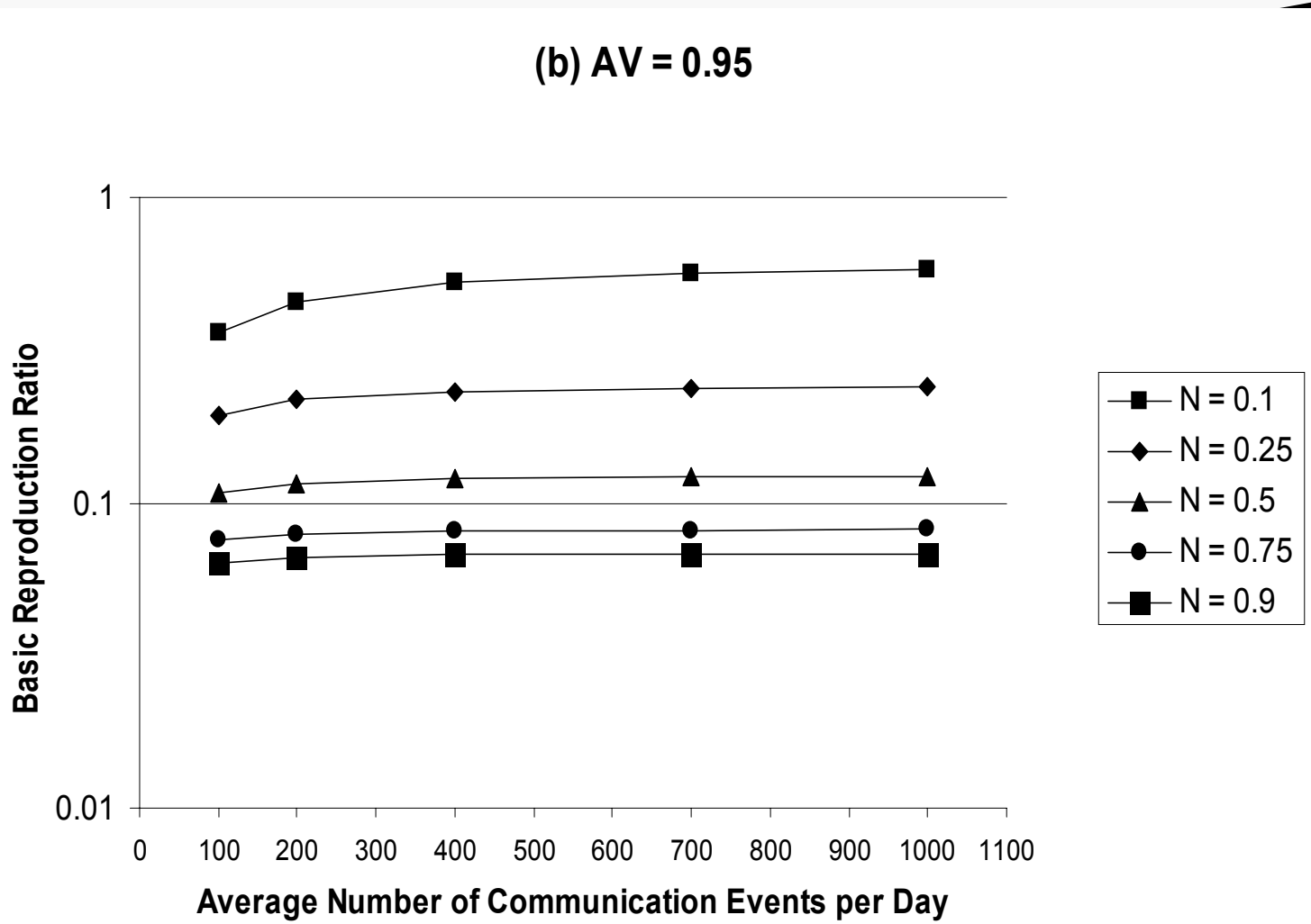
R_v is basic reproduction ratio for propagation within network.

W_v is propagation due to external exposures.

Basic Reproduction Ratio

- Basic reproduction ratio for macro viruses (most common) accounts for qualitative behavior of the effect of increasing the communication rate
- Key question: When is the basic reproduction ratio for macro viruses greater than or less than unity?


(a) AV = 0.80
Basic Reproduction Ratio
10
1
0.1
0
100
200
300
400
500
600
700
800
900
1000
1100
Average Number of Communication Events per Day
N = 0.1
N = 0.25
N = 0.5
N = 0.75
N = 0.9


(b) AV = 0.95
Basic Reproduction Ratio
1
0.1
0.01
0
100
200
300
400
500
600
700
800
900
1000
1100
Average Number of Communication Events per Day
N = 0.1
N = 0.25
N = 0.5
N = 0.75
N = 0.9

Risk Communication propagates virus.

Protection Communication propagates notification.

Followon Ideas

- Information assurance for real-time surveillance for bioterrorism or other disaster response
- Joint threat of biological infectious agents and computer infectious agents
- Public health authorities look at vaccines, drugs, detection of agents and capacity of health care system -- but less so at communications system

Information Security Question

Do you have the phone numbers of your e-mail correspondents?

System managers trying to stop the 1988 Internet worm did not.

Cross-sectoral training needed

- As systems become more distributed in public and private infrastructure, even system managers may not really know the maps of their own systems.
- An assertion that a system is "secure" is virtually meaningless.
- Confidentiality -- patient data, financial data in private sector ; national security in public sector