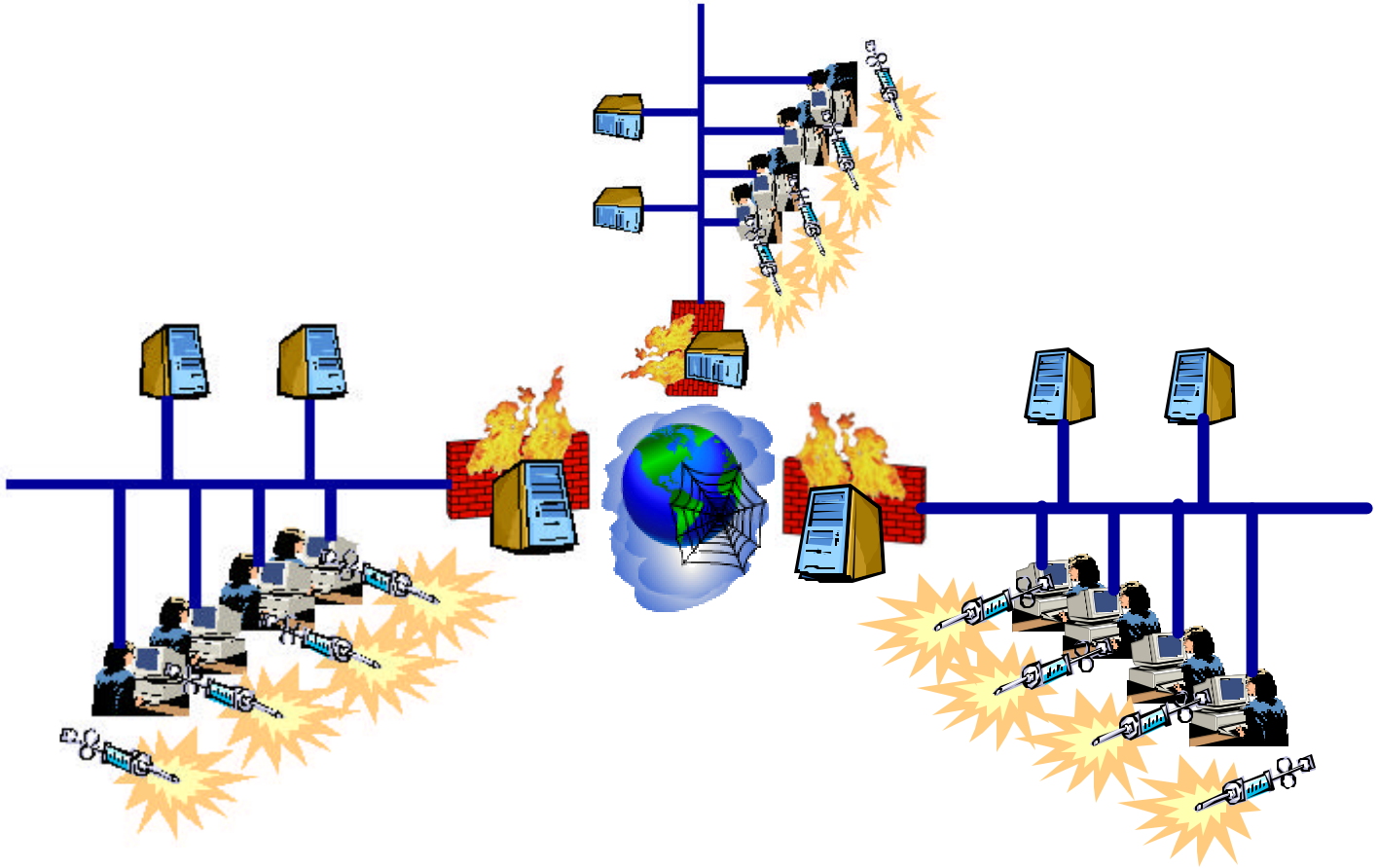
Status of Information Security - Beginning 2001

Status: Everyone has anti-virus and firewalls but yet Nimda/Code Red/etc shuts down the world. Why????



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

And The Cost Keeps Rising

World Virus Costs (blns)

2001 (-July)	11.8
2000	17.1
1999	12.1
1998	6.1
1997	3.3
1996	1.8
1995	0.5

Michael Erbschloe, vice president of research at Computer Economics and author of "Information Warfare: How to Survive Cyber Attacks' led the team at Computer Economics in this analysis

Company Virus Costs

If productivity analyses and cost modeling of the effects of virus disasters are considered, the average company could spend between $100,000 and $1,000,000 in total ramifications (both soft and hard costs) per year for virus disasters (Source: ISCA Labs Survey, 2000).

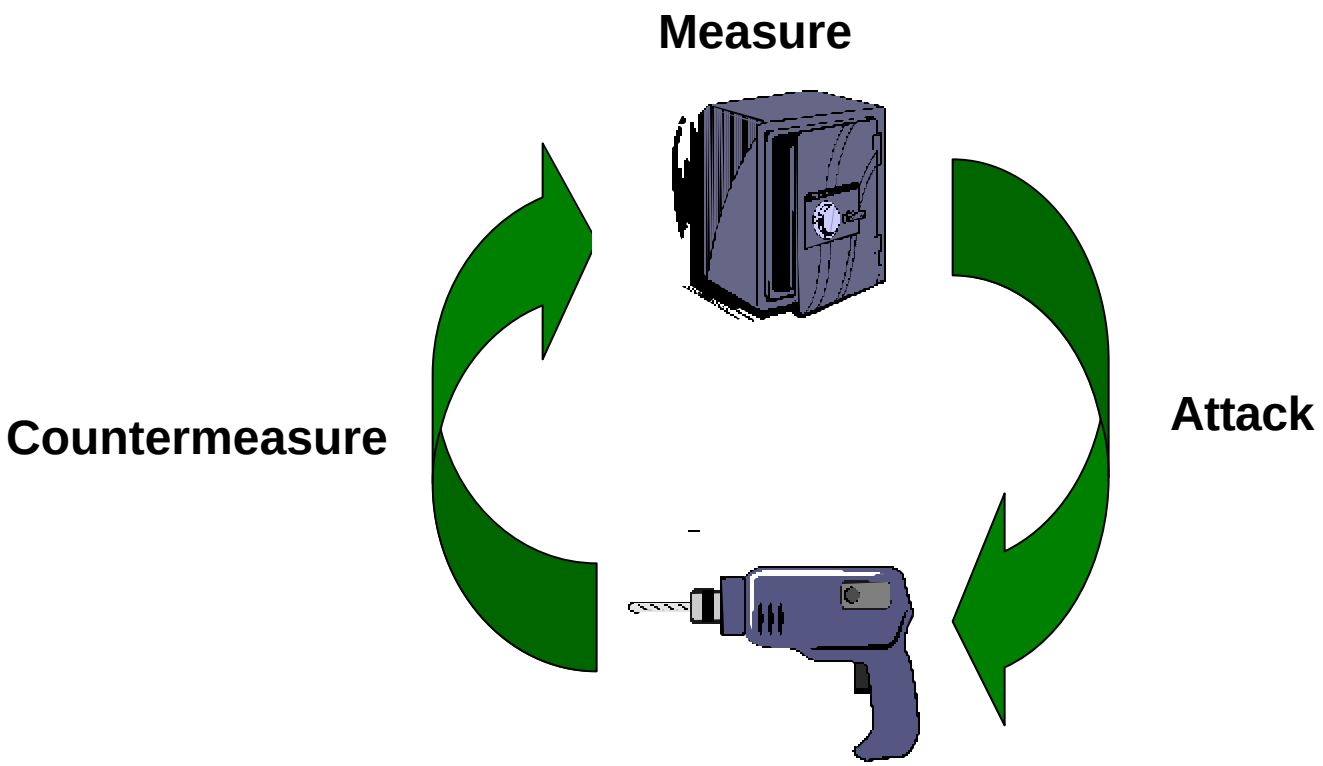
*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Outline

- History and challenges of information security
- **Attack/Countermeasures - Still chasing our tails**
- In search of the silver bullet by studying the history of viruses
- Demo: Losing the virus war again
- Back to the future - Finding the silver bullet

*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

History of Safe Cracking

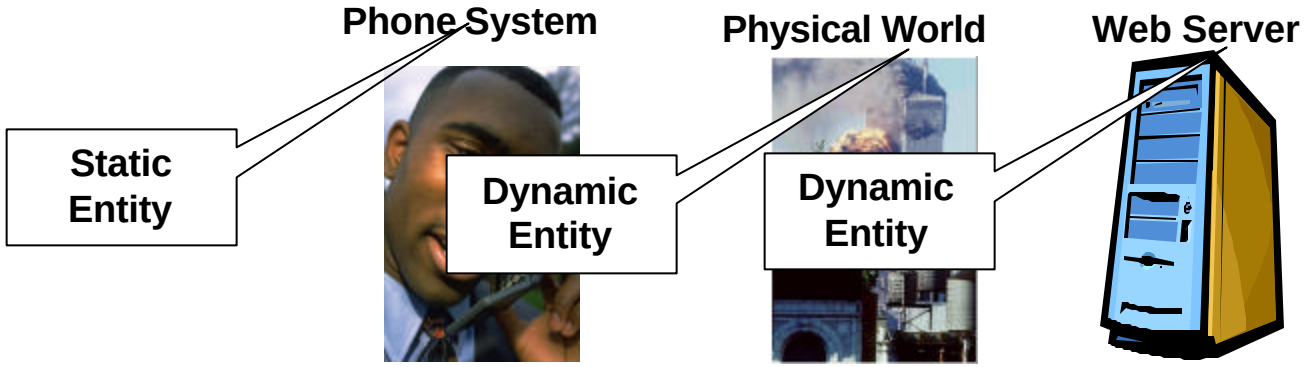


*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

People Think Computers are Like Telephones

*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Compare Telephones to Physical World and Computers

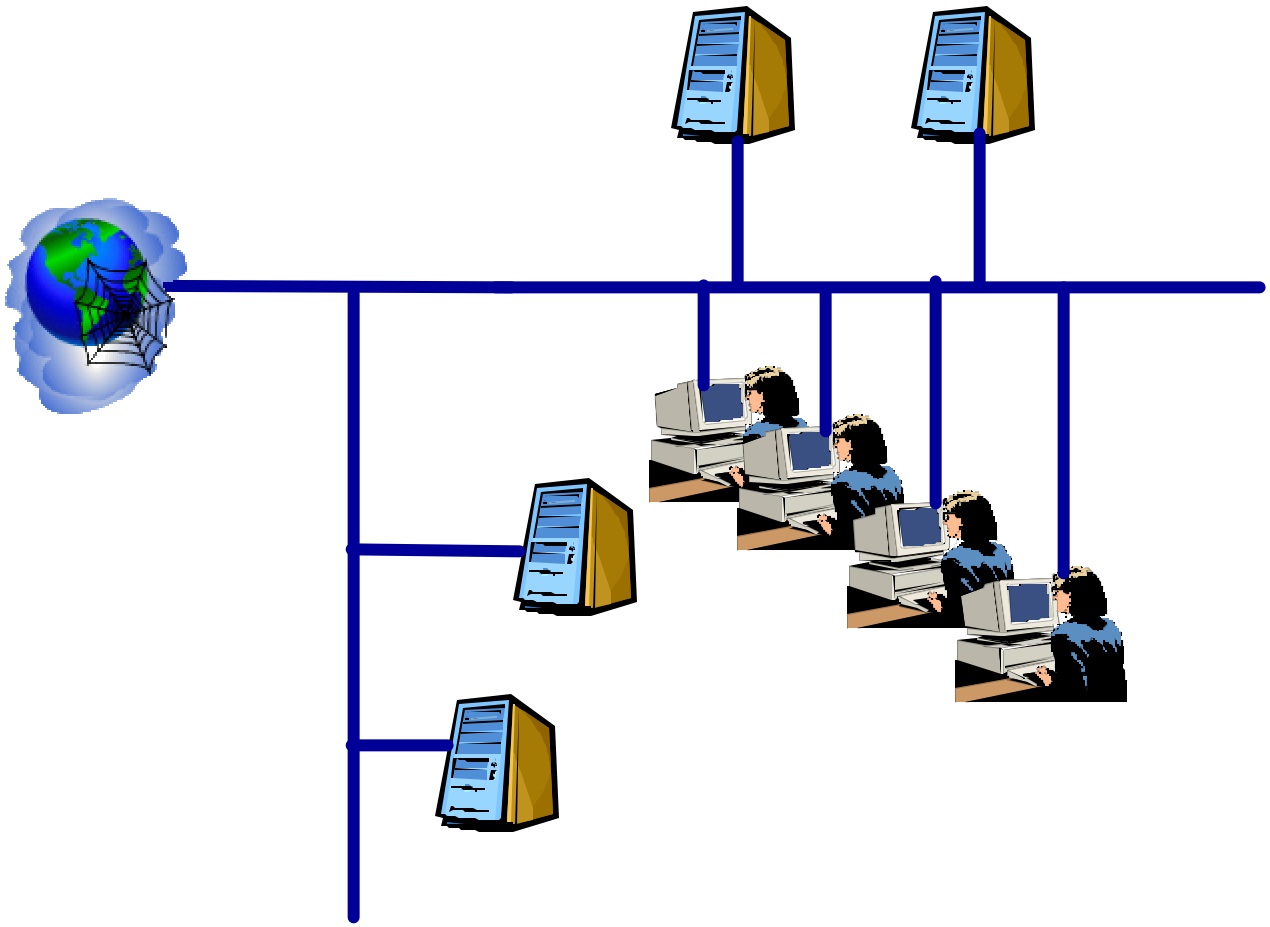


Number of Vulnerabilities	FEW	EXTREME	EXTREME
Threat Level	LIMITED (closed system)	MEDIUM (local access)	HIGH (world access)
Attack Technology	LIMITED	CAN"T PREDICT	CAN"T PREDICT
Complexity (increase failure rate)	LIMITED and FINITE	EXCESSIVE and INFINITE	EXCESSIVE and INFINITE
Target Value	LIMITED	EXCESSIVE	EXCESSIVE
Modifications/Updates	RARE	RARE	CONSTANT

*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

History of Network Security

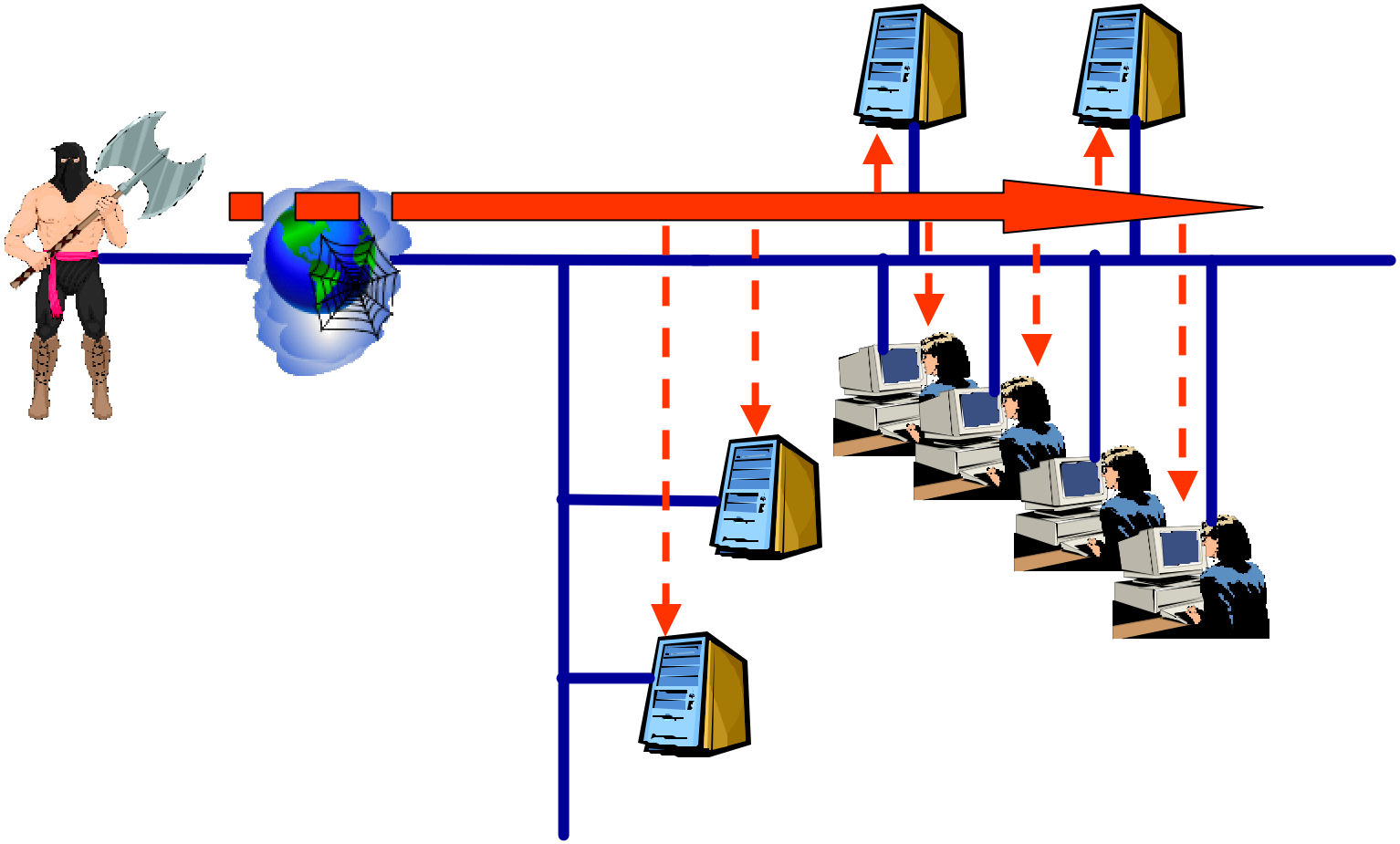
Measure: Host based security (e.g. passwords)



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Password Attack

Attack: Password attack amongst many others



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Cracking/Stealing Passwords

Brute Force

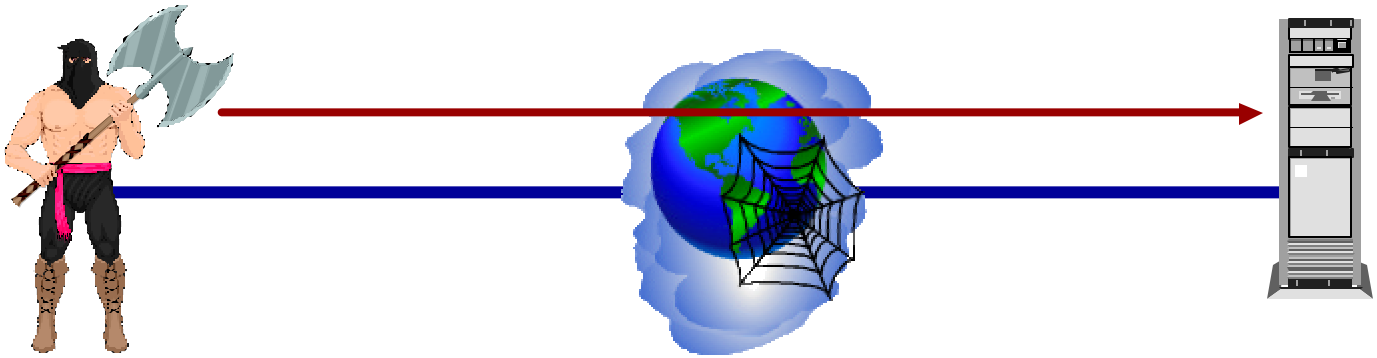
A,AA,AAA,AAAA,AAAAA,AAAAA
B,BAA,BAAA,BAAAA,BAAAAA,
C,CAA,CAAA,CAAAA,CAAAAAA
etc.

Dictionary

- Common names in a text file on net
- Dictionary in a text file on net
- Phone book in a text file on net
- Encyclopedia in text file on net

NT or Unix Login

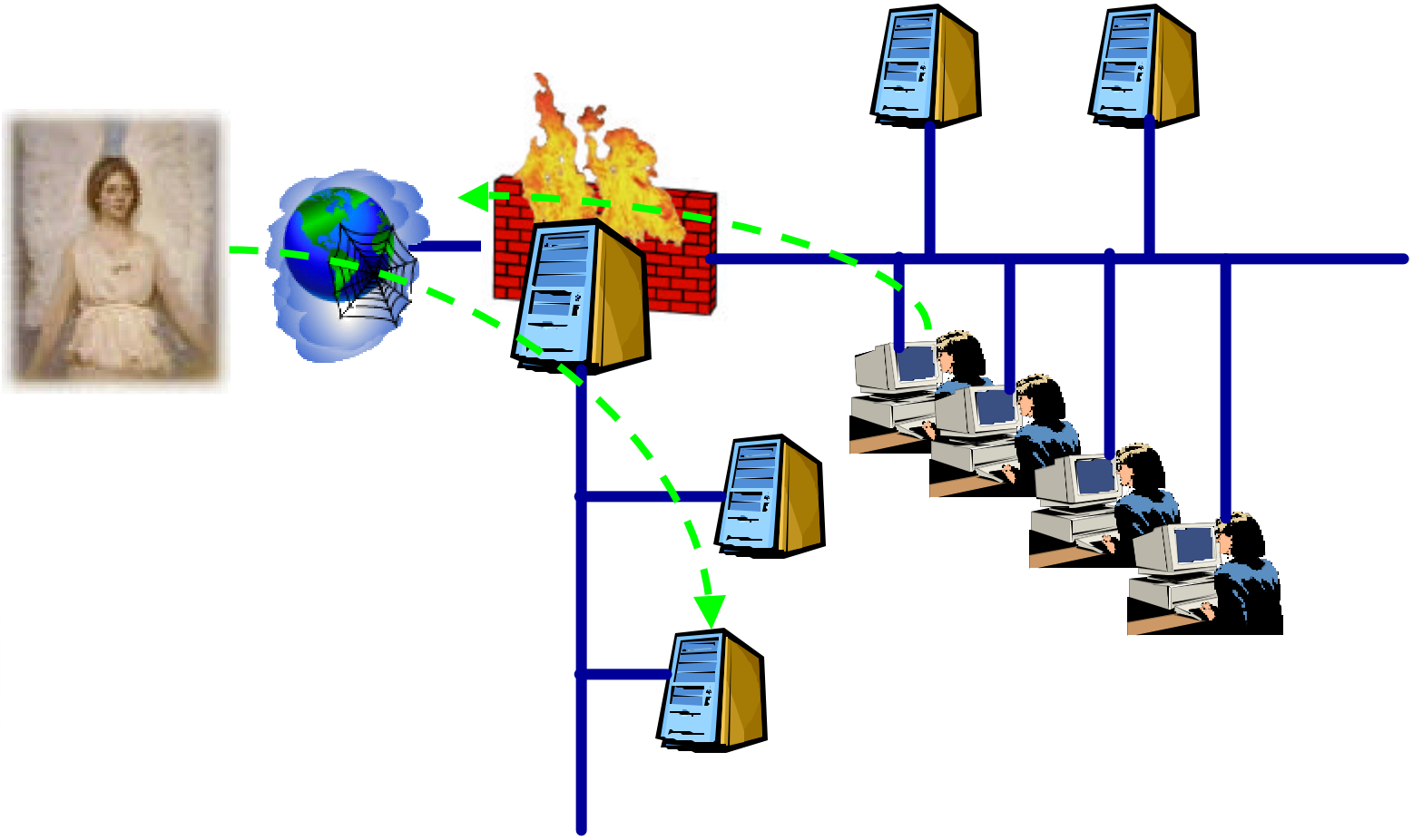
UserName: Administrator
Password: A, AA, AAA, AAAA, AAAAA, AAAAAA, AAAAAAA
B, BA, BAA, BAAA, BAAAA, BAAAAA, BAAAAAA…



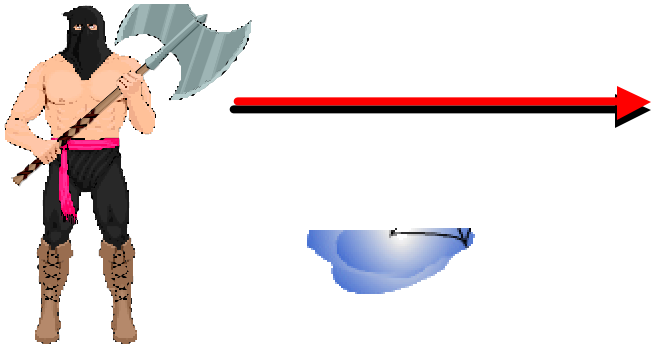
*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

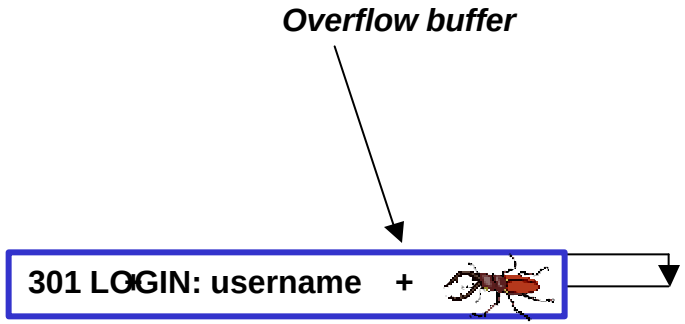
Firewall Countermeasure

Countermeasure: Firewalls restrict traffic flows



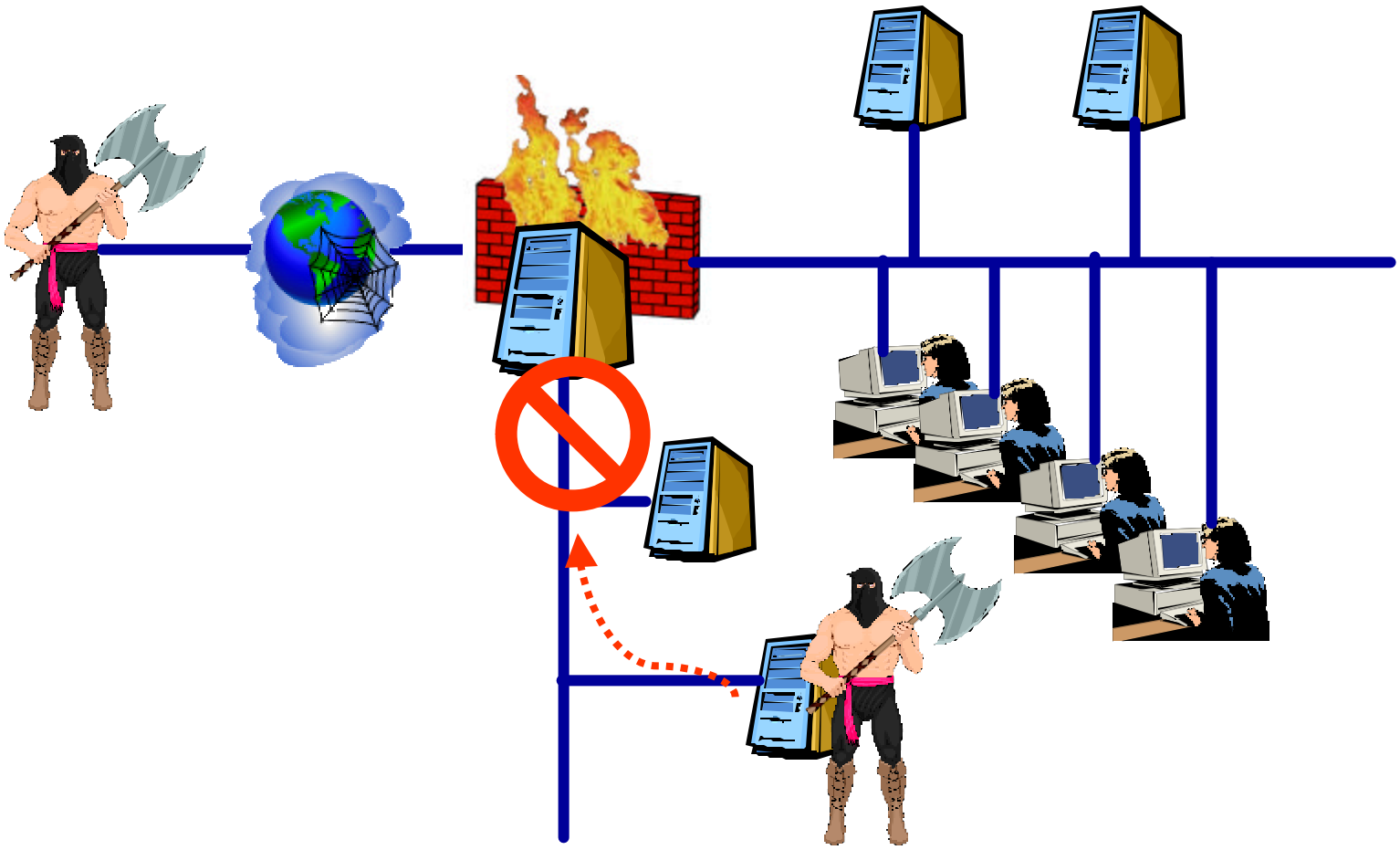
*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.




Overflow buffer
301 LOGIN: username +

Firewall Blocks Again

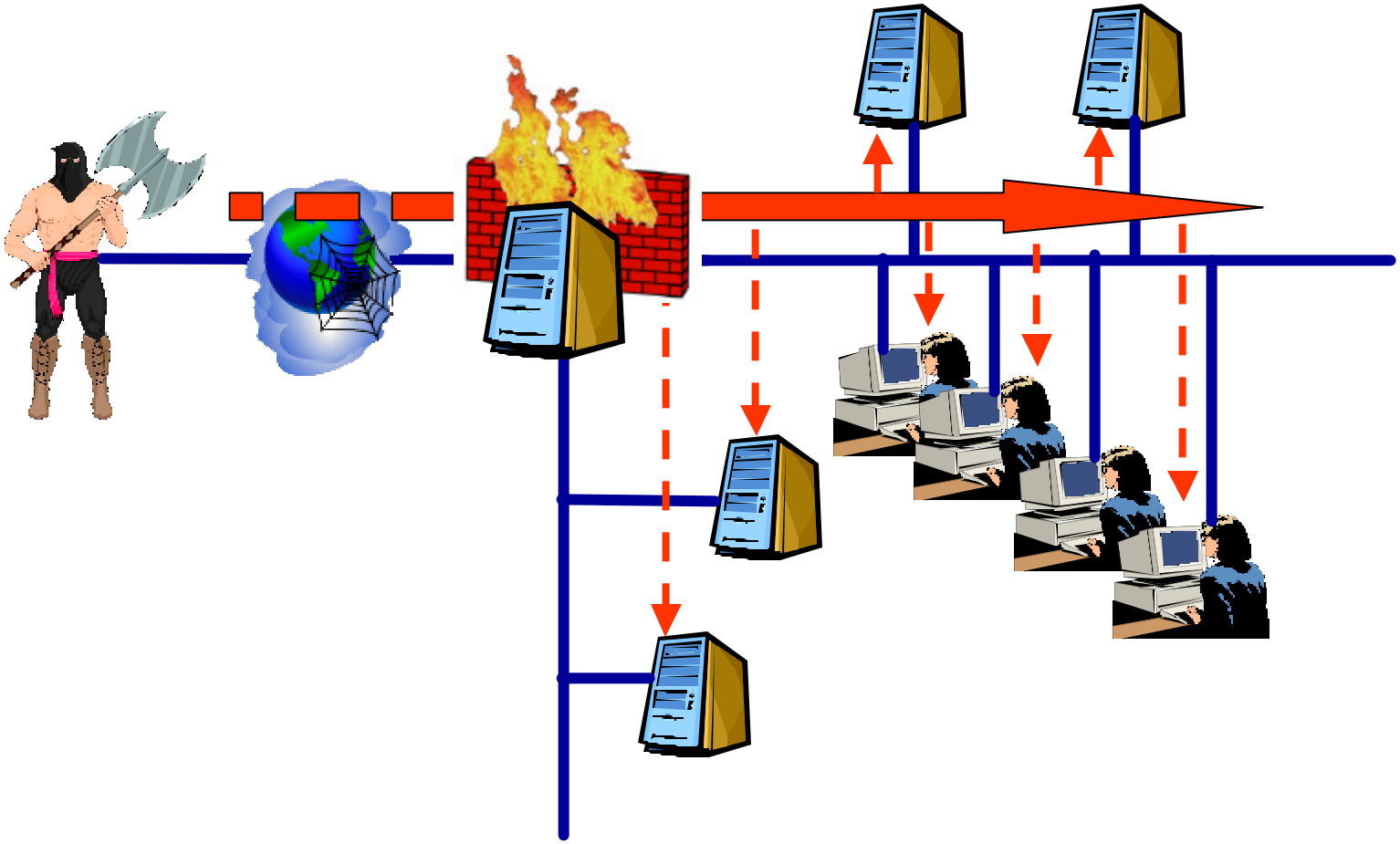
Countermeasure: Block access to internal systems



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Network Virus Attack

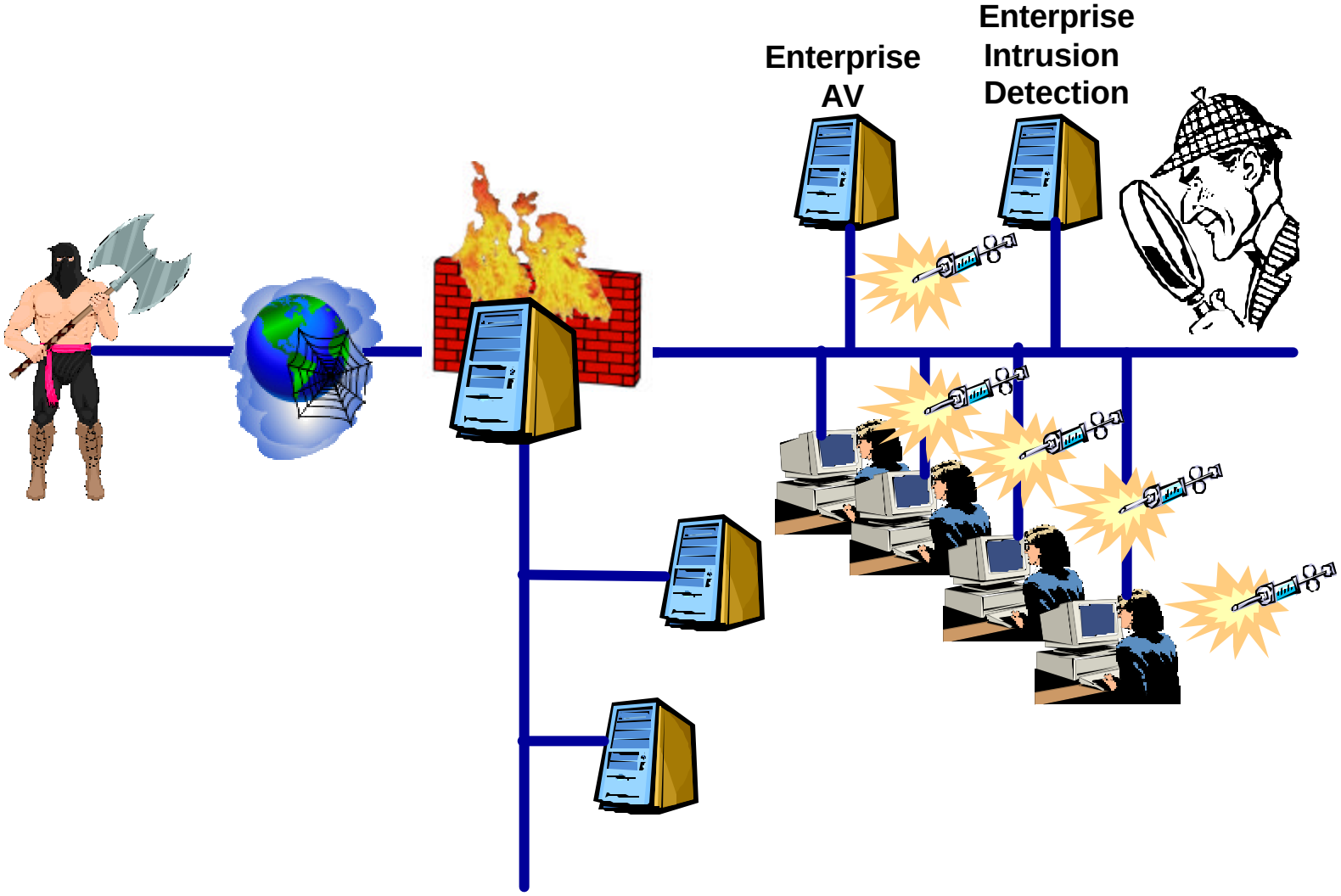
Attack: Bypass firewall again with network viruses (e.g macro viruses) directly to desktop



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Defend the Desktop

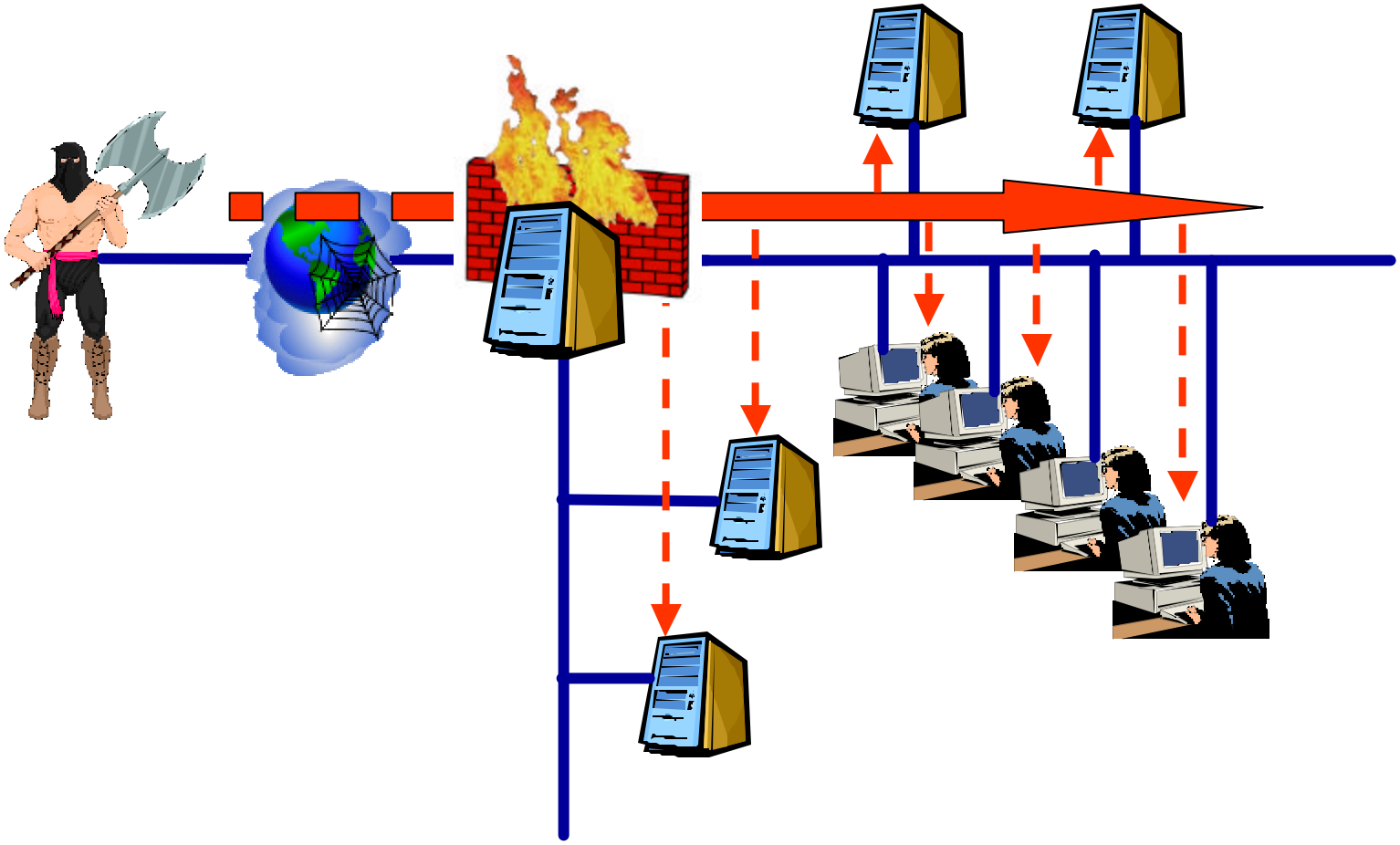
Countermeasure: Intrusion detection and antivirus



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

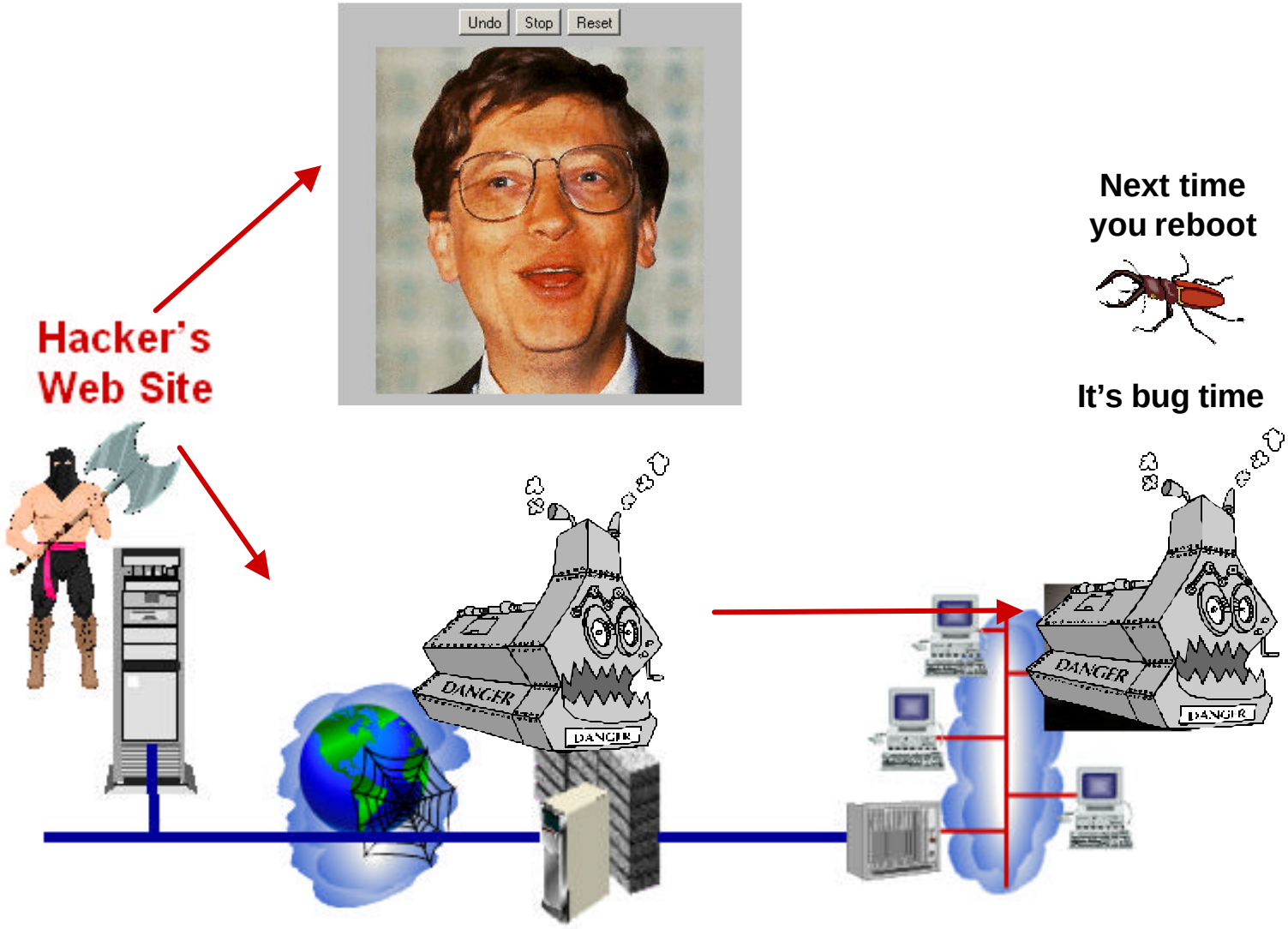
Bypass the desktop defense (again)

Attack: Bypass the firewall, AV and ID with special "viruses" directly to desktop



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

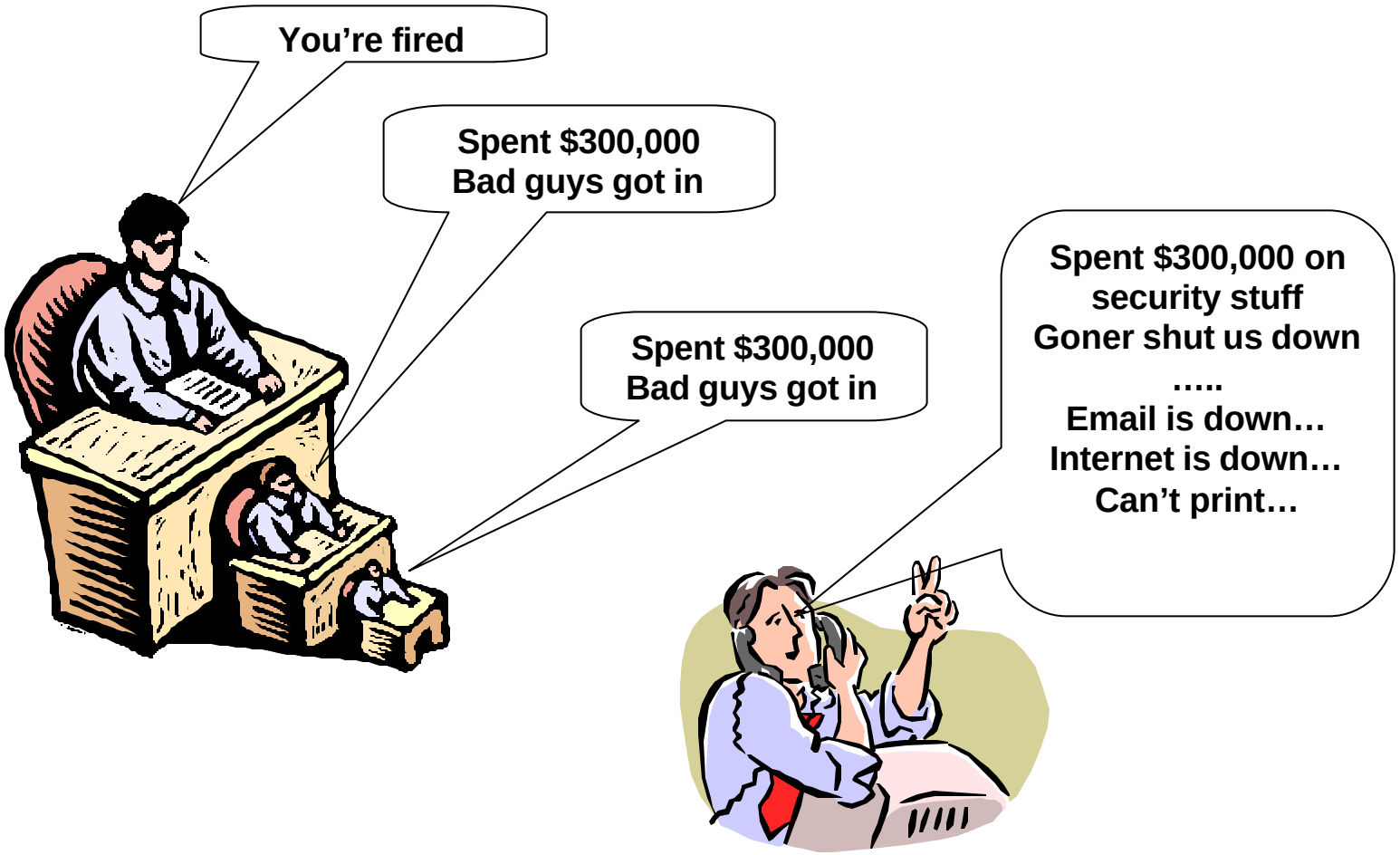
Unauthenticated Data Demo



Course Introduction
Overview of Security
Internet Overview
Security Principles
Day in the Life - Hacker
The Groundwork
Requirements
The Blueprint
Implementation
Vigilance

*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Status of Information Security End of 2001

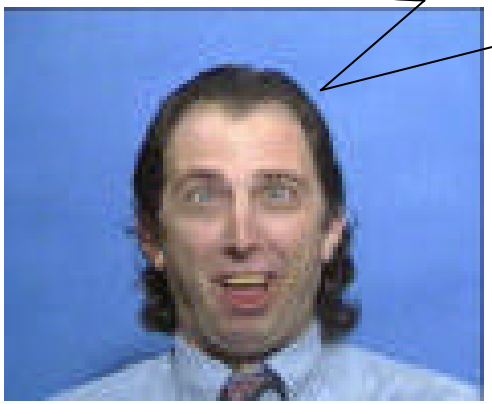


*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

The $300,000 Question Remains

AAAAAAHHHHHHHHHHHH!!!!!

What is the silver bullet for information security????



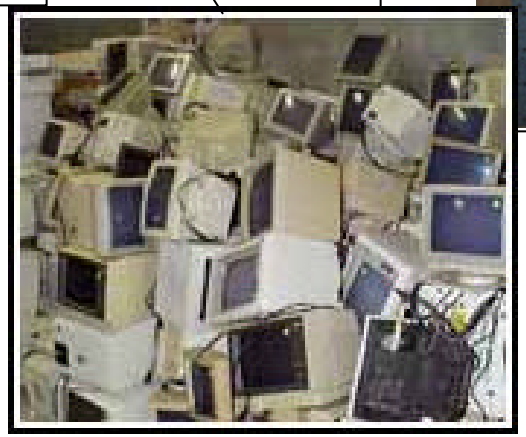
*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

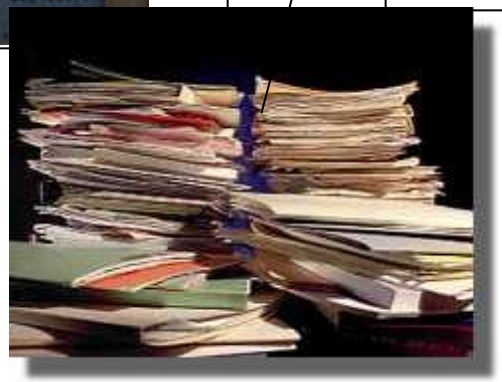
WHY? Physical World Mindset

You are measuring success by the number of toys and paperwork you pile up against the bad guys. NOT by the actual success of their implementation.

Firewalls, AntiVirus, Intrusion Detection, PKI, VPN, Honeypots

Security policy, audit reports, threat assessments and warnings, Security training manuals

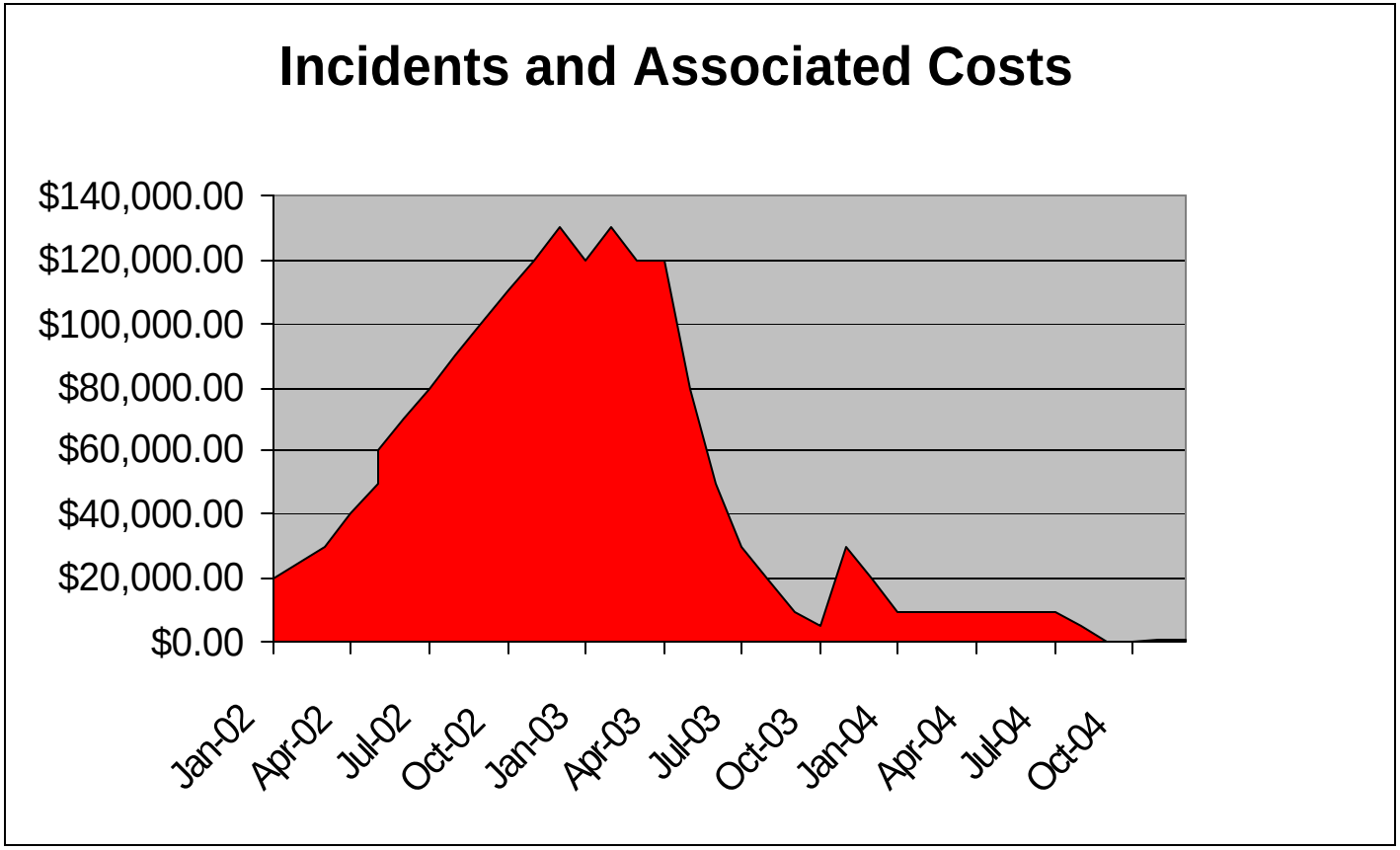




*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

The Silver Bullet Win????

When you can track and measure the impact of your security battles because then you know you have a security infrastructure in place protecting you from both old and impending threats



*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Best Practice Security Model Buys You

- Lower disaster recovery and liability insurance premiums
- Better employee cost utilization because work is scripted and documented so lower cost workers can do the work
- Ability to quickly and safely interconnect network infrastructures with partners and new acquisitions
- Ability to set the bar for security with new acquisitions or else purchase cost is reduced to make up for network retrofit costs
- Decreased downtime due to compromise/accidents
- Lower legal costs of sexual harassment lawsuits
- Reduce employee time/use of non-business resources because they know the security thug is standing guard
- Leverage your security dollars because as employees get trained, they can be your security police instead of expensive security staff
- Let management drive company policy and not IT

*Copyright © 2003, **Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.

Thanks!!

Copyright © 2003, ***Security Evolution, Inc. - All rights reserved.***
All rights reserved. No duplication without written permission.