

Security of Pharmaceutical Intellectual Property in the Era of Electronic Regulatory Submissions

Kevin B. Johnson, PhD

President

PharmaKnowledge Consulting

www.pharmaknowledge.com

Information in Pharmaceutical Development

- Distributed – virtual teams, international development; more open
- Integrated – teams interact more closely; shared information across disciplines
- Portable – information in digital form
- More valuable – competition; increasing costs

Topics

- General Elements of Computer Security
- Assets, Threats and Risk Management
- Most Common Threats
- Passwords and Firewalls
- Social Engineering
- Public Key Encryption



Risk Management

- Risk – the possibility that something adverse may happen
- Risk management – process of:
 - assessing risk,
 - taking steps to reduce risk to acceptable levels,
 - maintaining the level of risk
- For example, your personal Y2K plan

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Risk Assessment

Uncertainty

Unc

Risk Mitigation

Unc

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

**Define
Scope**

Uncertainty

**Risk
Analysis**

Uncertainty

**Interpret
Analysis**

Uncertainty

Uncertainty

Uncertainty

**Select
Safeguards**

**Accept
Residual
Risk**

**Implement
Controls**

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

Uncertainty

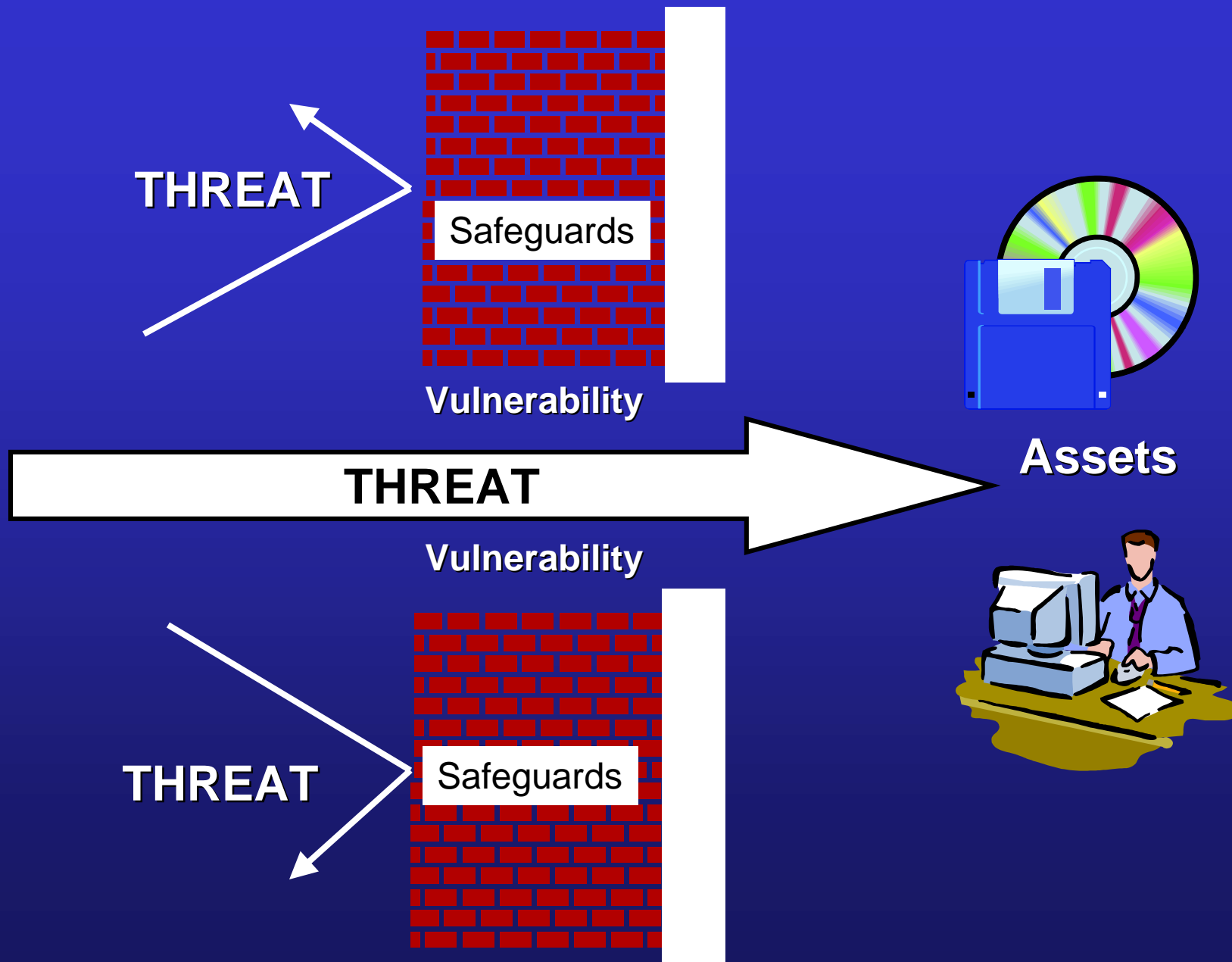
Uncertainty

Uncertainty

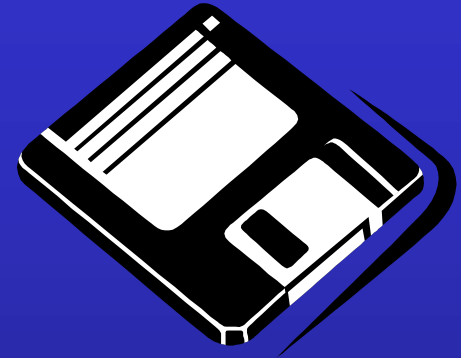
Uncertainty

Uncertainty

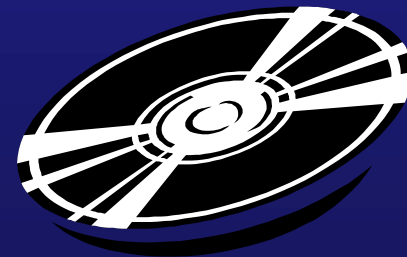
Uncertainty



Assets



- Data/information
 - databases, data files, hardcopy
- Software/Hardware
 - Customized applications, operating systems, infrastructure
- Personnel



Asset Valuation

Asset value consists of:

- intrinsic value,
- near-term impacts,
- long-term consequences of compromise



Threat Assessment

1. Identify potential agents/events that could place the asset at risk
2. Classify each threat
3. Assess likelihood of event
4. Determine impact of event
5. Determine consequences of event



1. Identify Potential Agents/Events That Could Place the Asset at Risk

- Errors and Omissions
- Fraud and Theft
- Employee Sabotage
- Loss of Physical and Infrastructure Support
- Malicious Hackers
- Industrial Espionage
- Malicious Code



2. Classify each Threat

- Disclosure
- Interruption
- Modification
- Removal
- Destruction



3. Assess Likelihood of Event

- Low Likelihood
 - no history; threat is unlikely
- Medium Likelihood
 - some history; threat may occur
- High Likelihood
 - significant history; threat is quite likely to occur



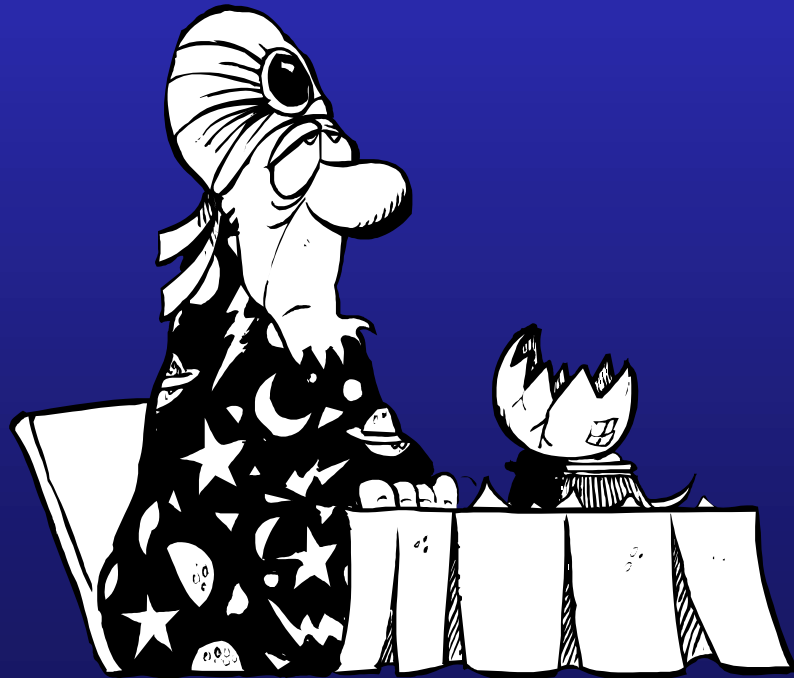
4. Determine Impact of Event

- Very serious
 - may compromise safety/patient care
- Serious
 - may disrupt normal operations,
 - cause significant inconvenience to clients, or
 - be costly to rectify
- Less serious
 - may disrupt non-critical operations,
 - cause limited inconvenience to employees



5. Determine Consequences of Event

- Loss of privacy/competitive advantage
- Loss of trust
- Loss of service
- Loss of asset

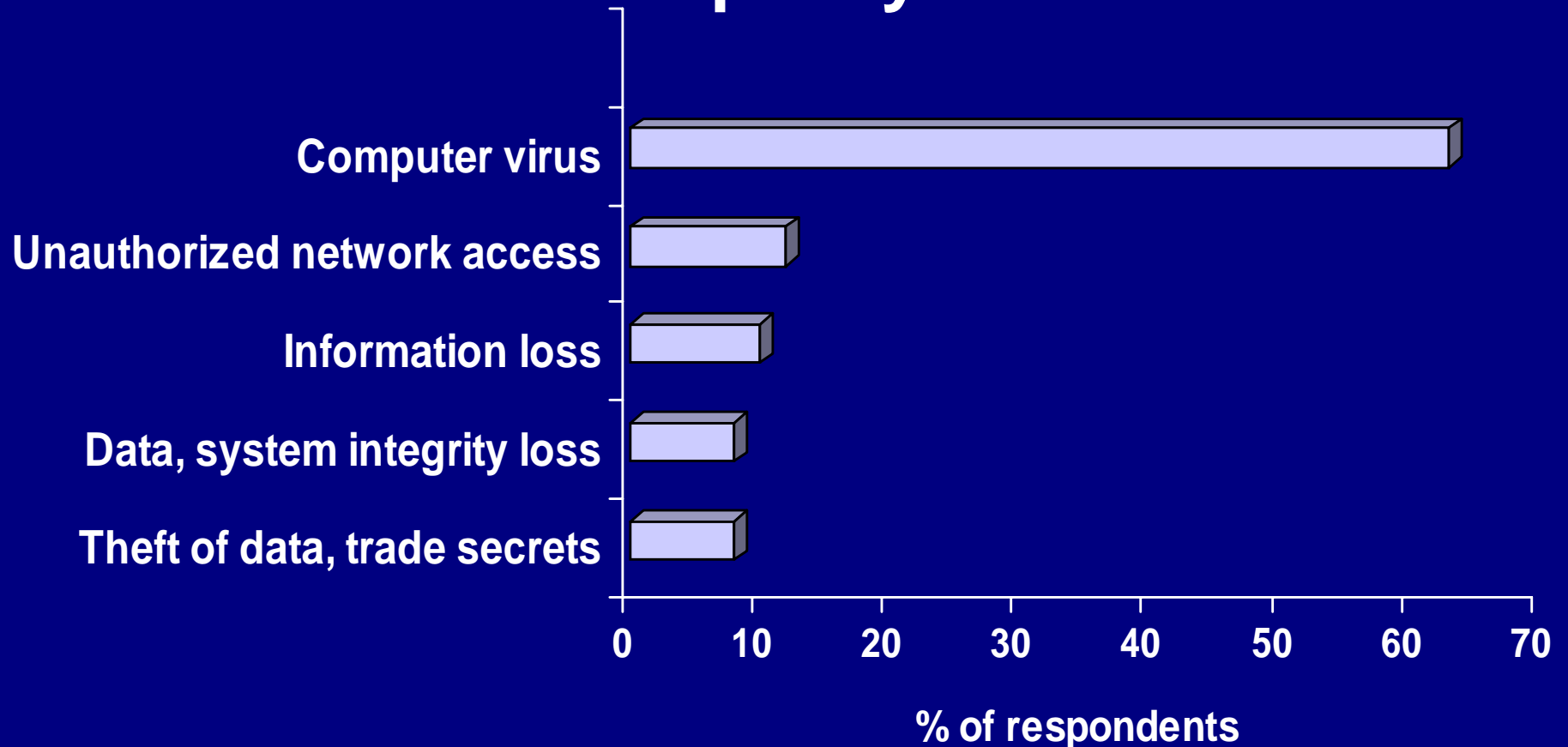


What/Who is the biggest threat?

- A. Viruses
- B. Disgruntled workers
- C. Hackers and crackers
- D. Pokemon



What security breaches or espionage occurred in your company in the past year?



“Viruses used to be like a mosquito bite to most companies. Now they look more like malaria”

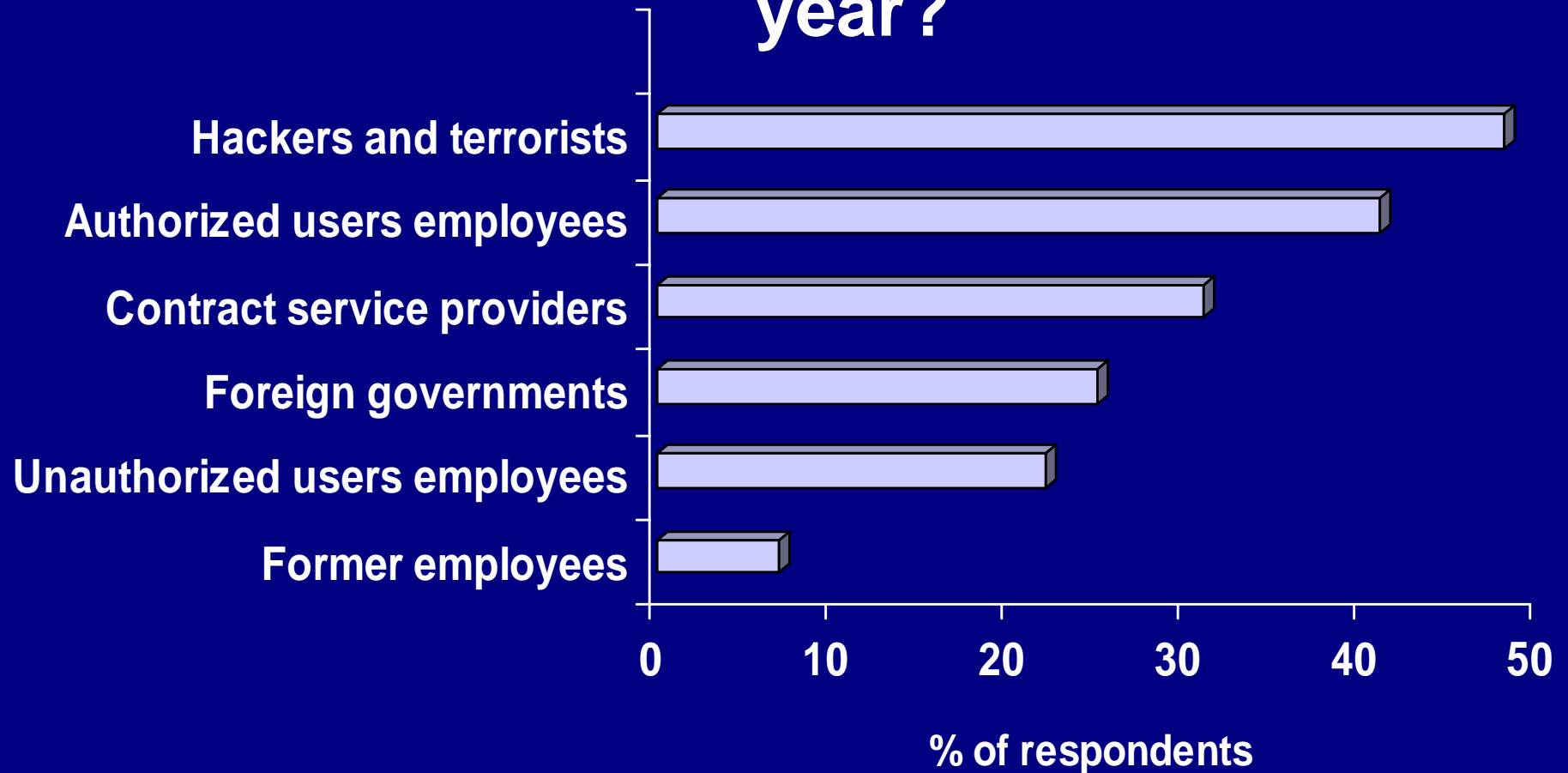
Melissa virus
> 80% of Fortune 1000
companies affected

Who is responsible for most security threats?

- A. Hackers and crackers
- B. Disgruntled employees (current or former)
- C. Contractors
- D. Competitors



Who do you suspect as the source of breaches or espionage in the past year?



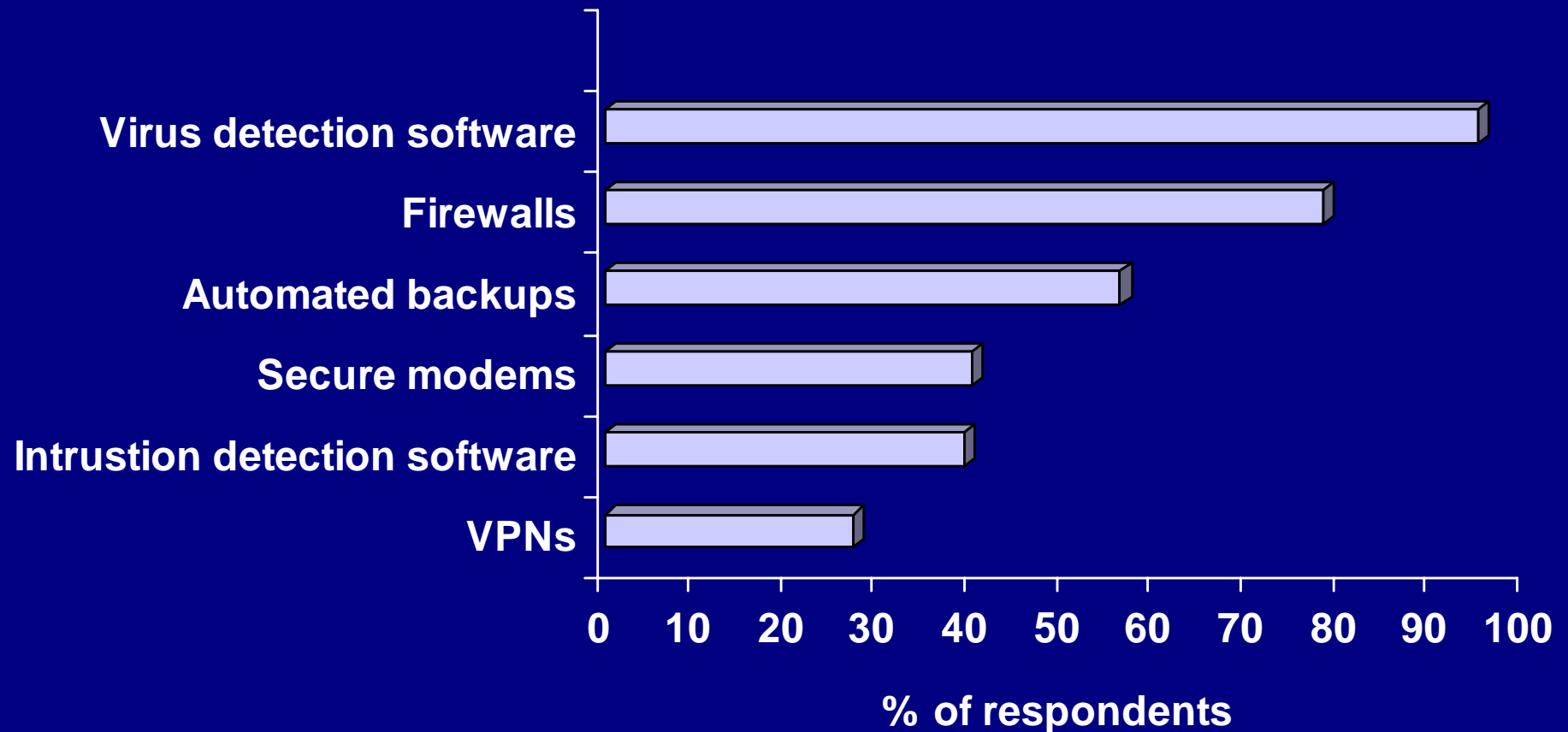
InformationWeek Research Global Security Survey

What methods are most commonly used to protect computer systems?

- A. Virus detection software
- B. Firewalls
- C. Encryption
- D. Luck and a prayer
- E. All of the above



Which tools do you use to protect information systems



If I don't open an email attachment, I'm protected from most of the new email viruses

- A. True
- B. False
- C. What's an attachment?
- D. What's email?



E-mail virus named after a 'Seinfeld' episode can have unfunny results

“A dangerous new type of e-mail virus has emerged, able to destroy information on computers even when users are careful not to fully open the messages.

The virus, nicknamed "Bubbleboy" after an episode of the TV show "Seinfeld,..."

Deadly Computer Virus Is Circulating Via E-Mail

By a WALL STREET JOURNAL Staff Reporter
CUPERTINO, Calif. — A deadly new computer virus is circulating through the world, spreading via e-mail and wiping out a variety of computer files, antivirus software companies said.

Trend Micro Inc. said three Fortune 500 companies were hit by the "Explorepak" virus in the past few days. The virus can wipe out a user's important data by converting all word-processing documents and other Microsoft Office files into files with nothing but zeroes in them. The virus spreads insidiously via e-mail, sending itself as an e-mail attachment to anyone who writes an e-mail to the infected user.

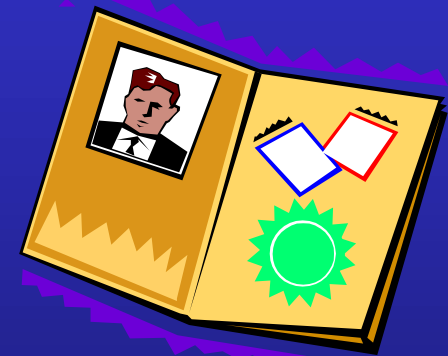
Don't open Xmas

The Prilissa virus has many insidious characteristics.

- ▶ Reformats a hard drive
- ▶ Disables virus-protection security settings, conversion confirmation, and recently opened file lists
- ▶ Displays colored shapes on top of the open document
- ▶ Alerts users with strongly worded messages

Identification and Authentication

- Something they know
 - passwords, PINs, encryption keys
- Something they possess
 - token cards
- Something they are
 - biometrics
 - voice, fingerprint, retinal print



Benefits of Passwords

- Familiar; successful for many years
- Integrated into many operating systems
- When properly managed, effective



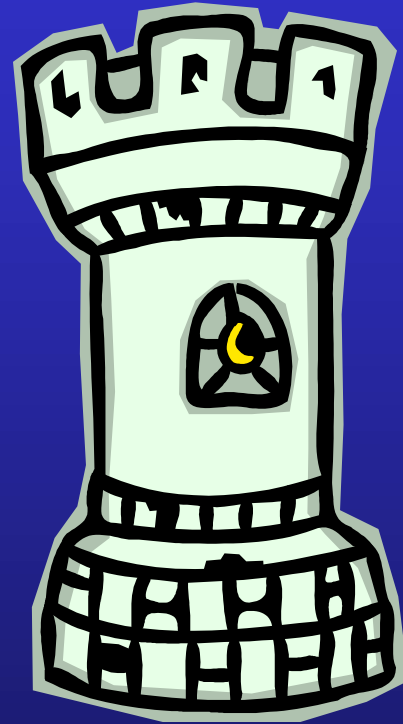
Problems with Passwords

- Need to remain secret
- Guessing or finding passwords
- Giving passwords away
- Electronic monitoring
- Accessing the password file



Firewalls

- Computer system that provides communications security for information coming into or going out of a server
- “Virtual moat around the castle”



Problems with Firewalls

- Firewalls can be bypassed
 - Direct dial modems
 - Diskettes traded between computers
- Data-driven attacks; hidden in emails
 - Melissa, Bubbleboy viruses/worms
- Internal attacks
 - Deliberate – sabotage, damage, theft
 - Accidental – negligence, naivety

Social Engineering



Extracting
information
from untrained
and
unsuspecting
staff

General Security Needs

Privacy

only intended can read

Content Integrity

content not altered

Authentication

recipients are who they say they are

Non-Repudiation

source cannot deny sending or receipt

Encryption

Security Requirement	Security Method
Privacy	Data Encryption Public Key Encryption
Authentication	Digital Signature
Content Integrity	Digital Signature
Non-repudiation	Digital Signature

Compliance

Dilbert® by Scott Adams



Balancing Security and Knowledge Management Issues

