Research Imperatives

Areas of Research Needed in Information Security

Julie J.C.H. Ryan, D.Sc.

Assistant Professor

The George Washington University

jjchryan@gwu.edu

What We Know

- Technology
  - Fabulous research going on in tech development
- Management Practices
  - This is where it all comes together
    - Resource allocation
    - System integration plans
- What works?

jjchryan@gwu.edu

The Biggest Problems

- **Are also the biggest challenges**

jjchryan@gwu.edu

Research in INFOSEC

- Product development
  - Cryptography – nearly 4,000 years
    - Privacy
    - Authentication
    - Integrity
  - Recent efforts
    - Malicious code detection and evaluation
    - Barrier technologies
      - Access control
      - Firewalls
      - Smart cards
      - Biometrics
    - Intrusion detections systems
    - Vulnerability analysis systems

jjchryan@gwu.edu

Research in INFOSEC

- Mathematical Models in INFOSEC
  - Bell-LaPadula
  - Graham-Denning
  - Harrison-Ruzzo-Ullman
  - Biba
  - Clark-Wilson
- Trustedness models
  - Orange Book and Rainbow series
  - ITSEC
  - Common criteria
  - ISO 17799

jjchryan@gwu.edu

Serious Shortfalls

- Situational awareness
  - Is it an attack?
  - By whom?
- Resource allocation
  - Probabilistic risk assessment
  - Operations research
    - Stochastic programming
  - Business continuity and crisis management
  - Knowledge management
    - Security v reliability

jjchryan@gwu.edu

Common Assumptions

- Inside attacks pose a greater threat than outside attacks
  - If true, we're going about security backwards
  - But is it true?
- Lack of security is the vendors' fault
  - Security is a product of implementation and environment
  - Vendors don't supply the environment

jjchryan@gwu.edu

Common Assumptions

- We can automate security
  - Security is a function of trust
  - How can you quantify trust?
  - Policies evolve, so automated security must evolve
- Certification of security experts will improve the state of security
  - Certification by whom, and how, and for what purpose?
  - Testing does not demonstrate performance proficiency; it tests cognitive knowledge

jjchryan@gwu.edu

Common Assumptions

- We must teach security to everyone, including users
  - Home users of PCs?
  - Managers?
- We can achieve complete security
  - Different definitions?
  - Different institutional goals?
  - Different environments interoperating?

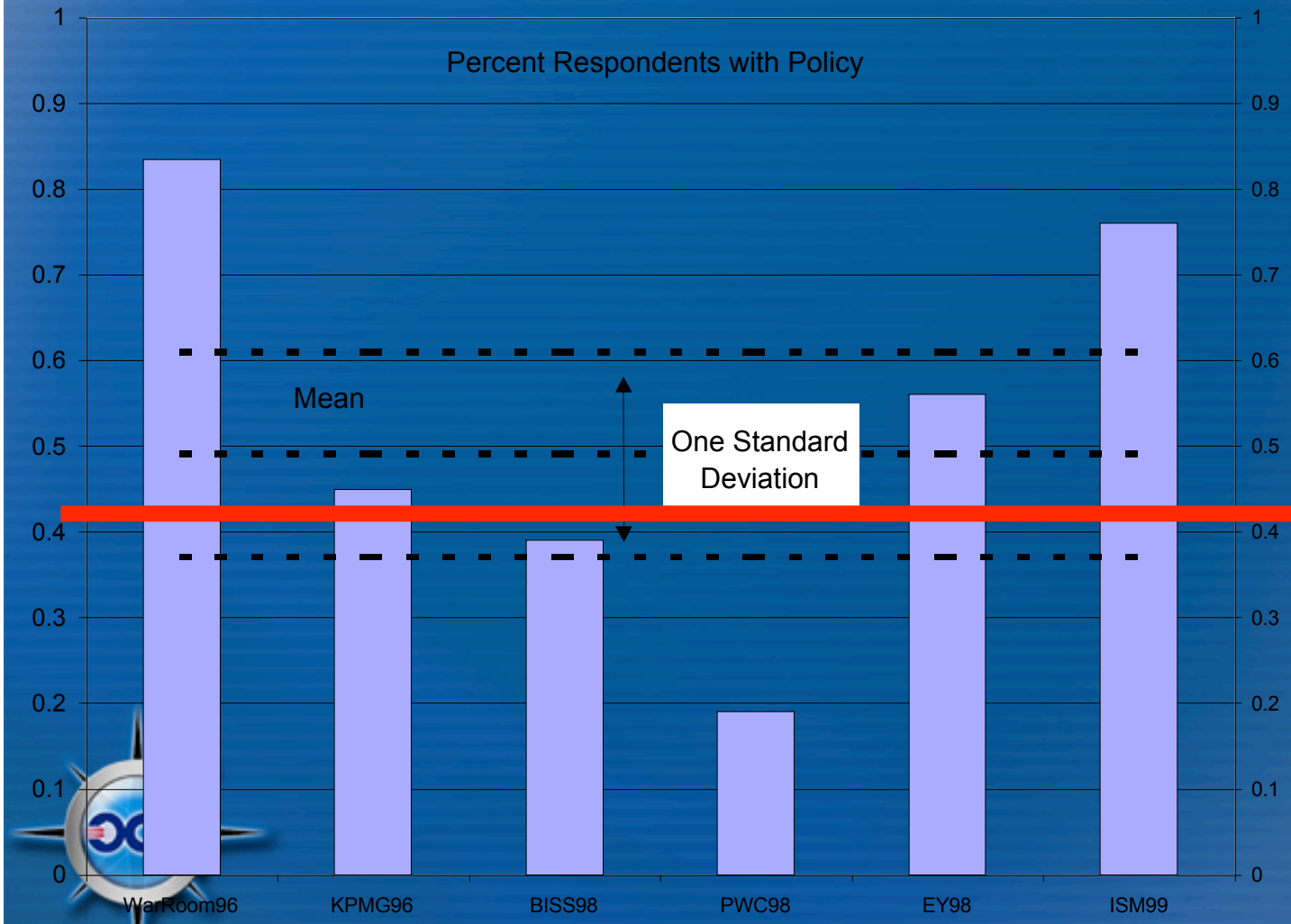
jjchryan@gwu.edu

The Practice of InfoSec

- According to surveys taken over past decade:
  - About half have security policies
  - About half have experienced security breaches
  - About 12 % have been hacked
  - About half have had problems with insiders
  - Of those with $$ loss, only 37% can quantify amount
  - Viruses, theft, and component failure are big concerns
  - About half have business continuity plans

jjchryan@gwu.edu

Policies



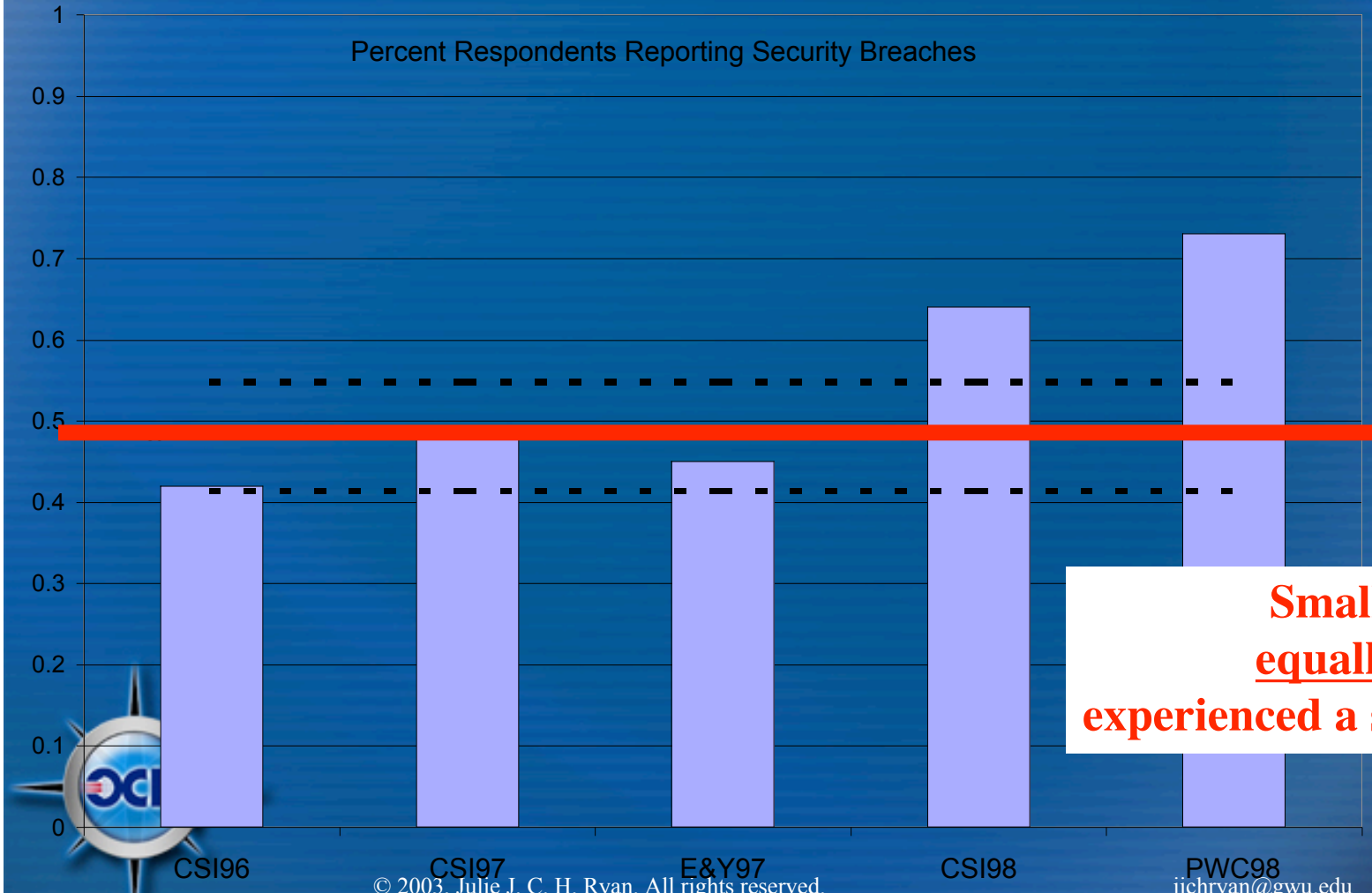
49% mean

42.1 %

Small businesses are <u>less</u> likely to have security policies

jjchryan@gwu.edu

Security Breaches



48 % mean

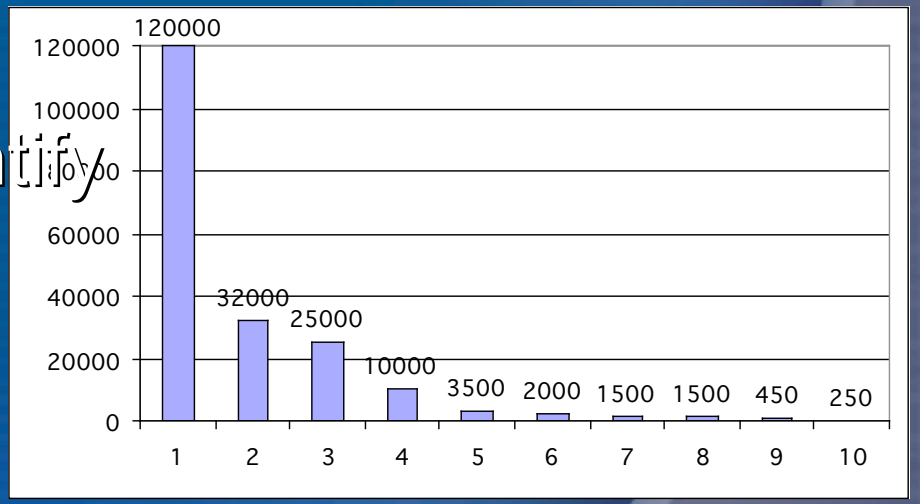
48.3 %

Small businesses are <u>equally</u> likely to have experienced a security breach

jjchryan@gwu.edu

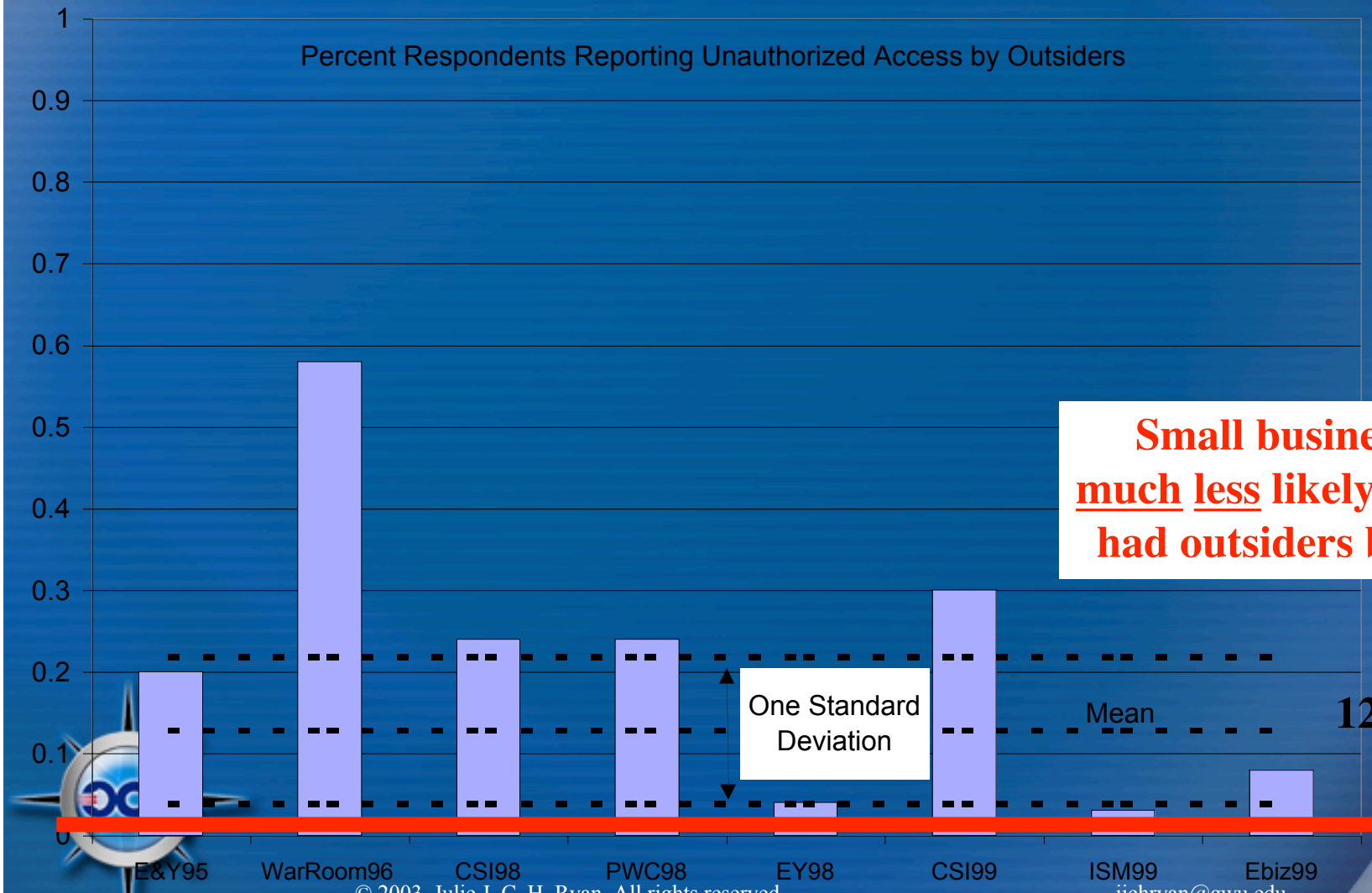
Financial Losses

- Experienced financial loss?
  - 82 % reported losses for one survey (PWC98)
  - Quantification of losses varies
    - From 31% (CSI99) to 48 % (CSI97)
- Small businesses much less likely to lose money
  - 9 %
- But better able to quantify when it happens
  - 73.7 %



jjchryan@gwu.edu

Outsiders



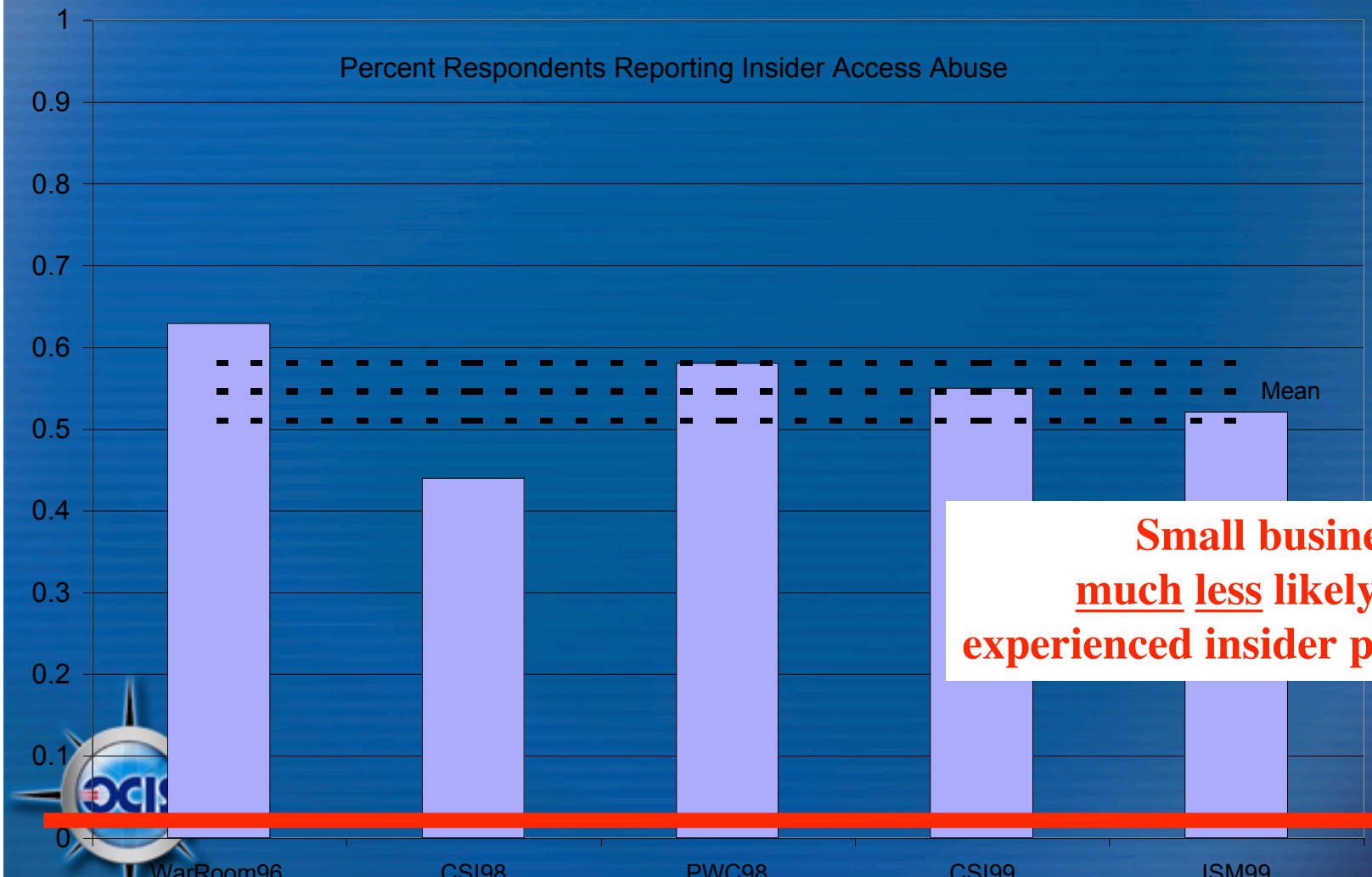
Small businesses are <u>much</u> <u>less</u> likely to have had outsiders break in

12.8 % mean

1.9 %

jjchryan@gwu.edu

Insiders



54.5 % mean

Small businesses are much less likely to have experienced insider problems

3.3 %

jjchryan@gwu.edu

Concerns

53% of small businesses think viruses are of extreme of high concern

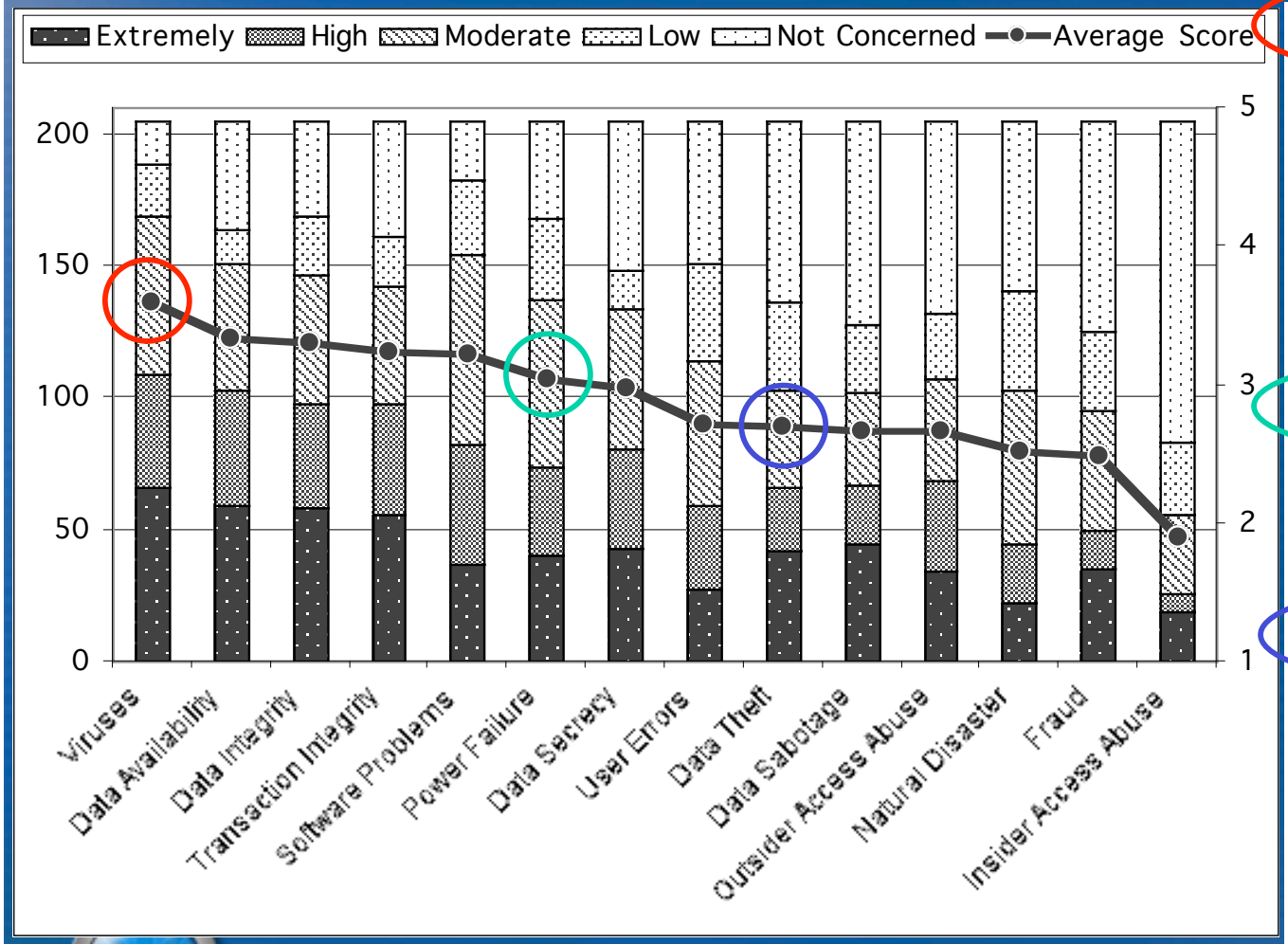
36.1 % think that power failure is of extreme or high concern

32.2 % think that data theft is of high or extreme concern

Survey	Top Five Security Concerns				
E&Y95	Network failure	Software error	Viruses	Hardware failure	Stolen data
E&Y98	Unauthorized users access violation	Authorized user access violation	Contract worker access violation	Former employee access violation	Competitors access violation
BISS98	Power failure	User error	LAN failure	Viruses	Theft
CSI98	Denial of Service attack	System penetration from outside	Theft of proprietary data	Financial fraud	Sabotage
PWC98	Viruses	Loss of information	Loss of integrity	Denial of Service	Software manipulation
CSI99	Insider abuse	Viruses	Laptop theft	Denial of service attacks	Sabotage
Ebiz99	Viruses	E-mail incidents	Spam	Power failure	Hoaxes, jokes, pranks
ISM99	Viruses	Employee access abuse	Unauthorized outsider	Theft or destruction of computer resources	Loss of proprietary data

jjchryan@gwu.edu

Concerns -- Overall Ranking



3.60 Viruses

3.33 Data Availability

3.30 Data Integrity

3.23 Transaction Integrity

3.22 Software Problems

3.04 Power Failure

2.98 Data Secrecy

2.71 User Errors

2.69 Data Theft

2.67 Data Sabotage

2.67 Outsider Access Abuse

2.52 Natural Disaster

2.49 Fraud

1.90 Insider Access Abuse

Scale is from 1 to 5, where 1 equates to "Not Concerned" and 5 equates to "Of Extreme Concern"

jjchryan@gwu.edu

Business Continuity Plans

Survey	Business Continuity Plan
BISS98	56 percent had a business continuity plan -- 90 percent of those said it reduced the impact of a security breach
E&Y98	23 percent had incident response teams in place -- 10 percent had put a business continuity plan in place the previous year

Management Tools	Counts		Percentages	
	Yes	No	Yes	No
Data Recovery Procedures	83	126	39.7%	60.3%
Information Security Policy	64	145	30.6%	69.4%
Computer Use & Misuse Policy	52	157	24.9%	75.1%
Information Security Procedures	48	161	23.0%	77.0%
Business Continuity Plan	45	164	21.5%	78.5%
Proprietary Data Use & Misuse Policy	38	171	18.2%	81.8%
Communications Use & Misuse Policy	29	180	13.9%	86.1%
Information Sensitivity Levels or Coding	28	181	13.4%	86.6%
Computer Emergency Response Plan	28	181	13.4%	86.6%
Data Destruction Procedures	27	182	12.9%	87.1%
Computer Emergency Response Team	15	194	7.2%	92.8%
Media Destruction Procedures	14	195	6.7%	93.3%

jjchryan@gwu.edu

Technology Use

Technology Tools			Percentages	
	Yes	No	Yes	No
Anti-Virus Software	182	27	87.1%	12.9%
Data Backup System	157	52	75.1%	24.9%
System Access Control	152	57	72.7%	27.3%
Power Surge Protectors	147	62	70.3%	29.7%
Redundant Systems	95	114	45.5%	54.5%
Shredders	93	116	44.5%	55.5%
Data Segregation	60	149	28.7%	71.3%
Firewalls	54	155	25.8%	74.2%
Encryption	53	156	25.4%	74.6%
Intrusion Detection Systems	47	162	22.5%	77.5%
System Activity Monitor	33	176	15.8%	84.2%
Facility Access Control	30	179	14.4%	85.6%
Security Evaluation System	24	185	11.5%	88.5%
Dial Back Modem	21	188	10.0%	90.0%
Media Degaussers	7	202	3.3%	96.7%

Less than 50% use

Less than 25% use

jjchryan@gwu.edu

Problems

- Existing research is imprecise and limited in applicability
- There are a few surprises
  - Little relationship between experiences, resource allocation
  - What does occur seems to be a matter of advertising, buzz, and fad rather than a reasoned approach to security
- More research is needed to understand causal relationships

jjchryan@gwu.edu