



Information Assurance in Practice: Information Security in Small Businesses

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

Assistant Professor

Engineering Management and Systems Engineering Department

School of Engineering and Applied Science

The George Washington University

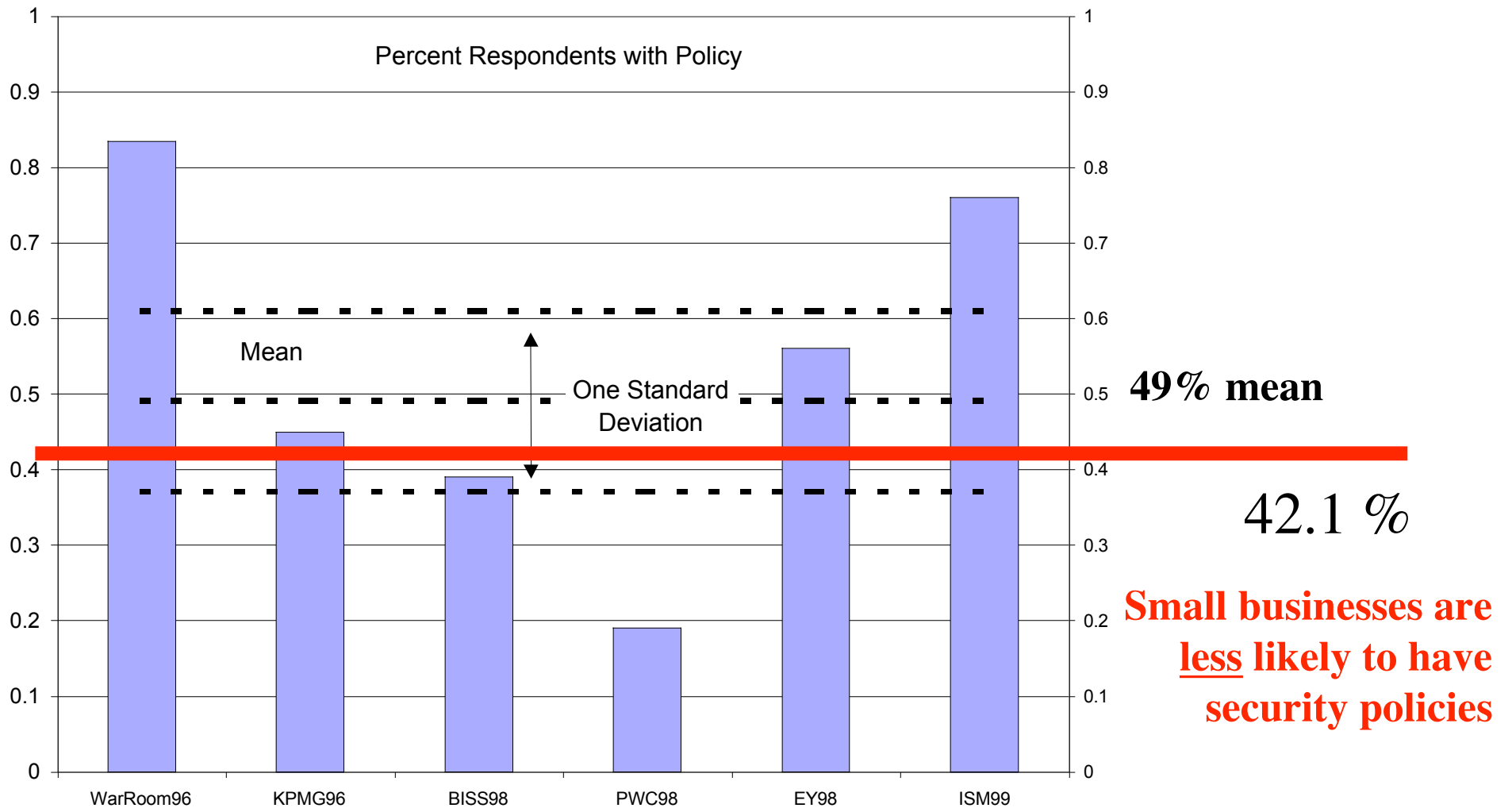
- Business Information Security Experiences, Practices
 - Meta-analysis of 14 large surveys:
 - About half of respondents have security policies
 - About half have experienced security breaches
 - About 12 % have been hacked
 - About half have had problems with insiders
 - Of those with \$\$ loss, only 37% can quantify amount
 - Viruses, theft, and component failure are big concerns
 - About half have business continuity plans
- Questions for Research:
 - 1: How do small businesses match up?
 - 2: Does having connectivity make a difference?

Why Small Businesses?

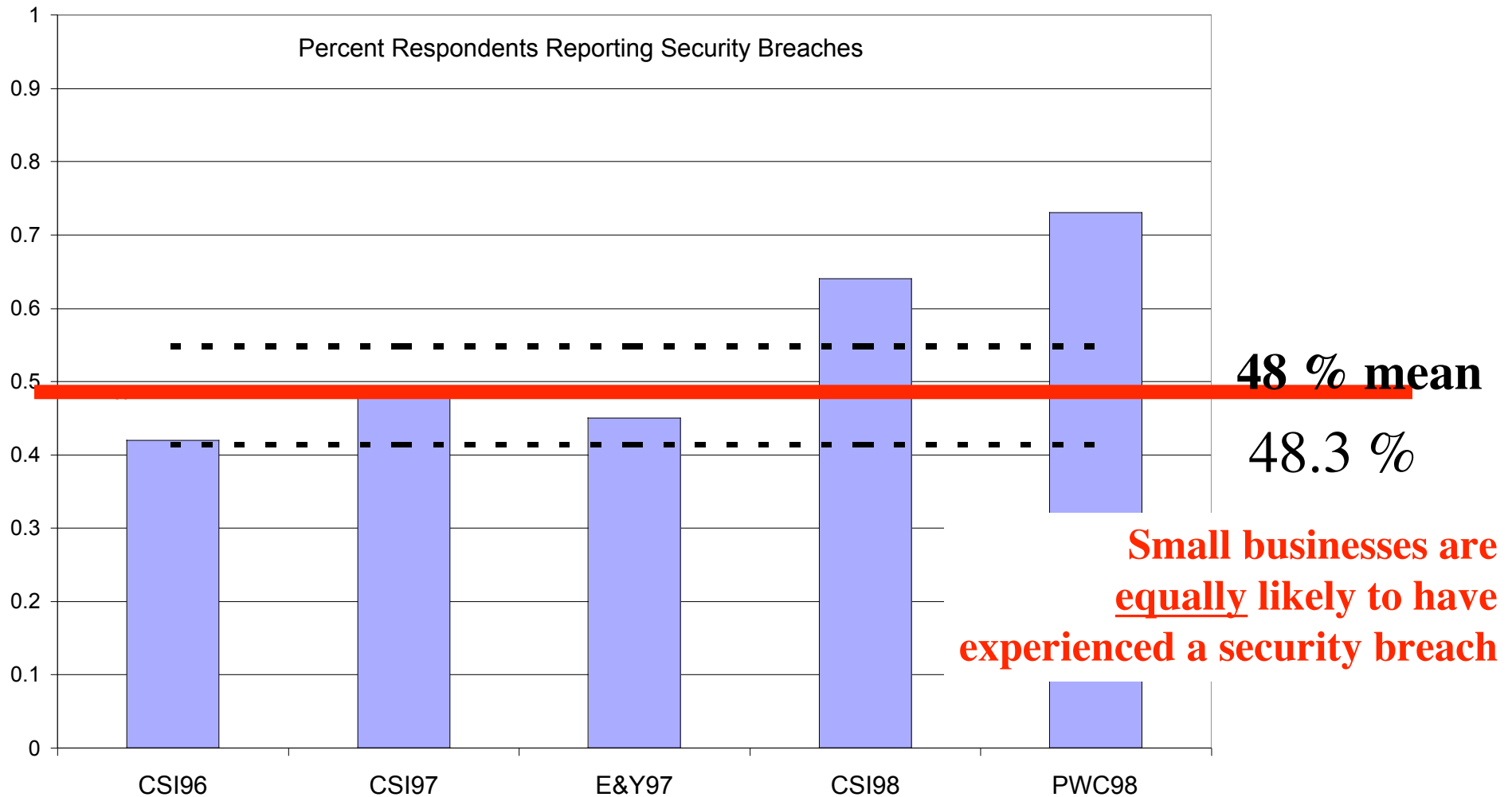
- A lot easier to research than huge businesses
 - One and only one response from each business
- Small businesses in the US:
 - Are 99 % of all employers
 - Employ 53 % of all workers
 - Employ 38 % of private sector high tech workers
 - Account for 51 % of private sector output
- Most importantly:
 - Small businesses account for 55 % of innovations and register more patents
 - And occasionally they grow up to take over the world
 - AOL, Microsoft

from:
SBA Office of Advocacy
<http://www.sba.gov/advo/>

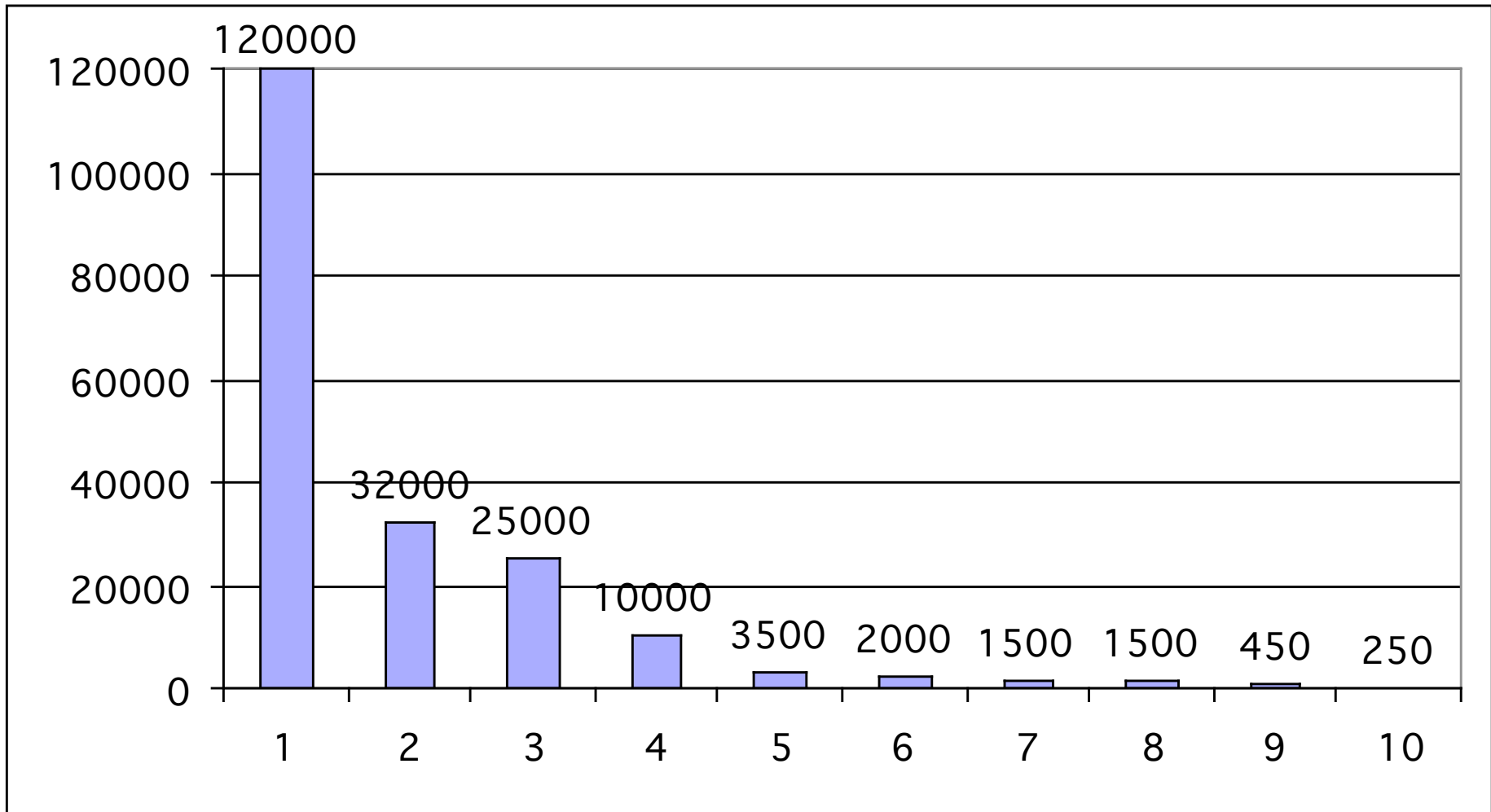
Policies



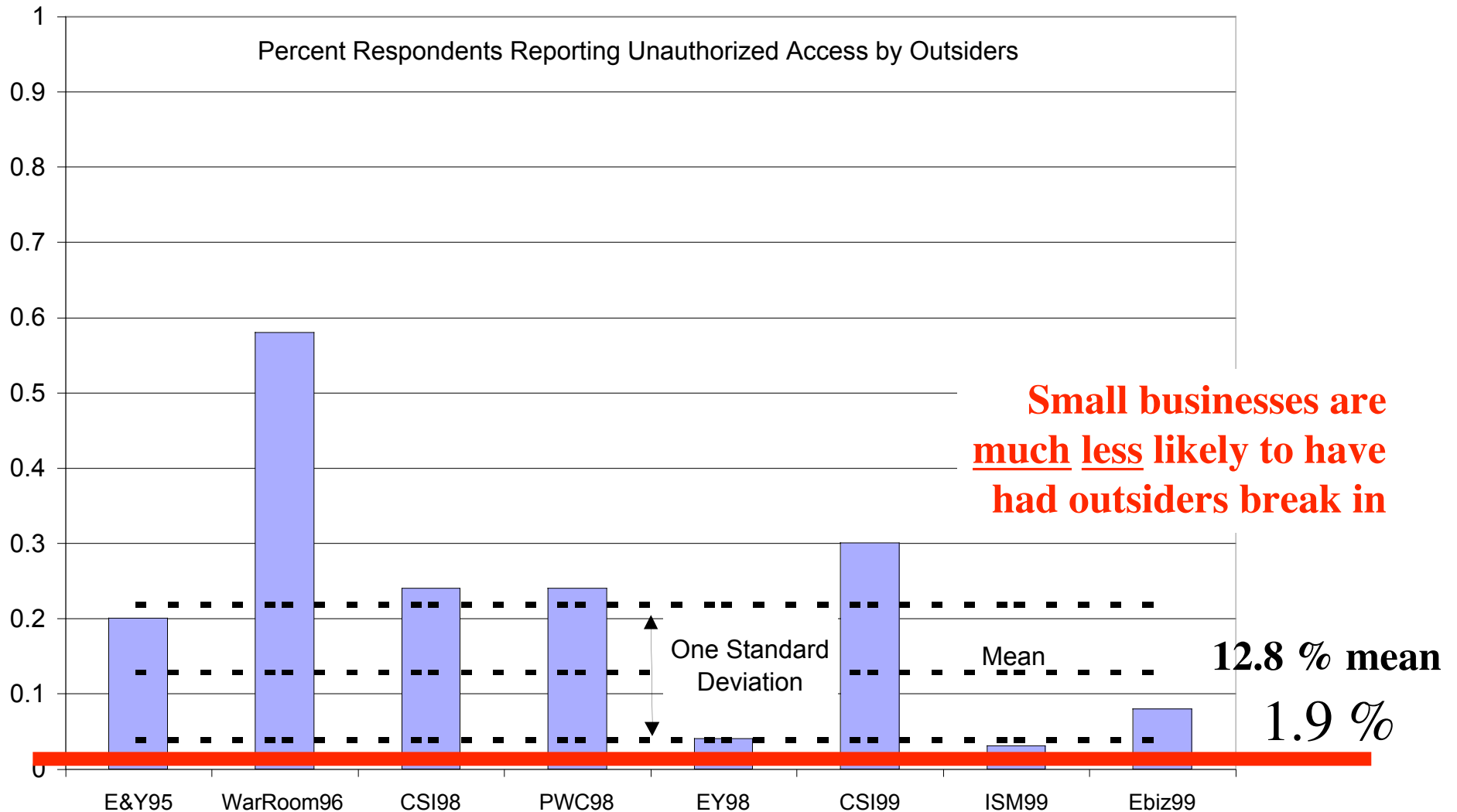
Security Breaches



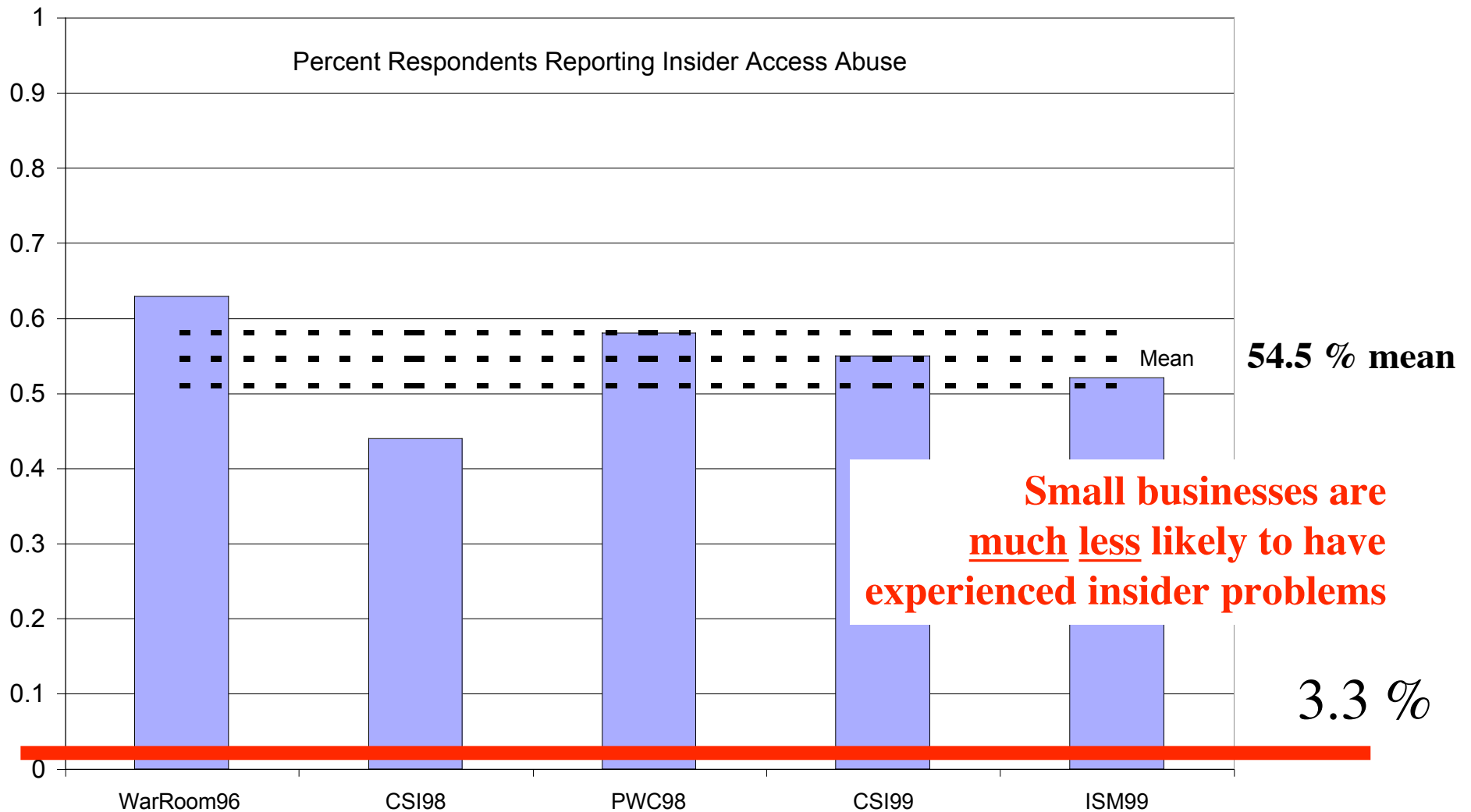
Financial Losses



Outsiders



Insiders



Concerns

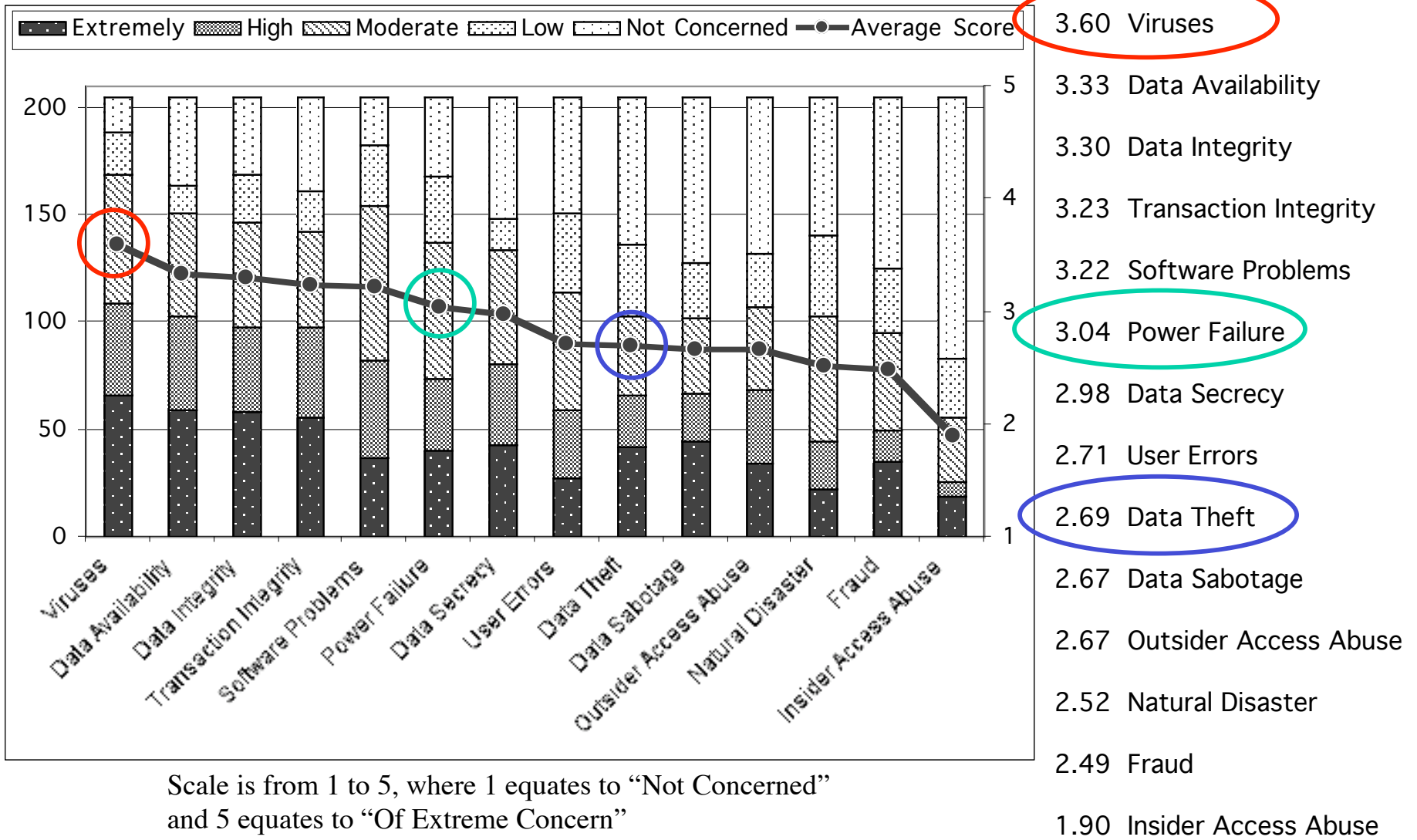
53% of small businesses think viruses are of extreme of high concern

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

Concerns



Business Continuity Plans

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%

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**

Question

- Does having connectivity make a difference???
 - In concern for information security?
 - In use of written policies?
 - In information security experiences?
 - Information security breach, financial loss, insider problems, outsiders
 - Use of business continuity plans?
 - In use of technologies?
- Types of connectivity considered:
 - Internet access
 - Web presence
 - E-commerce participation

Concerns

- Internet connectivity
 - Related to only one type of concern: viruses
 - Less likely to indicate low or no concern, more likely to indicate moderate concern, and equally likely to indicate high or extreme concern
- Web presence
 - More likely to be extremely or highly concerned in two areas:
 - Outsider access abuse (41.7% vs. 26.6%)
 - Data Availability (59.4% vs. 42.2%)
- E-Commerce
 - More likely to be extremely or highly concerned in two areas:
 - Transaction integrity (67.6% vs. 43.4%)
 - Data Availability (67.6% vs. 46.4%)

Written Policies

- Internet access alone doesn't make a difference
- Those with web presence more likely to have:
 - Computer Use & Misuse Policy 32% vs. 18.7%
 - Proprietary Data Use & Misuse Policy 24.7% vs. 12.5%
 - Communications Use & Misuse Policy 19.6% vs. 8.9%
- Those participating in E-commerce more likely to have:
 - Information Security Policy 54.1% vs. 25.6%
 - Computer Use & Misuse Policy 43% vs. 20.9%
 - Proprietary Data Use & Misuse Policy 35% vs. 14.5%
 - Communications Use & Misuse Policy 29.7% vs. 10.5%

Experiences

- Null hypotheses cannot be rejected in those areas, but:
 - For those with Web presence
 - Viruses (27.8% vs. 14.3%); secret data divulged (4.1% vs. 0%)
 - For those participating in E-commerce
 - Natural disaster (13.5% vs. 1.2%); secret data divulged (8.1% vs. 0.6%)

	Internet Access			Web Presence			E-Commerce		
	chi sq	chi sq p	Fisher's P	chi sq	chi sq p	Fisher's P	chi sq	chi sq p	Fisher's P
<i>Past 12 month:</i>									
Info security incident	0.128	0.7201	0.7214	3.249	0.0715	0.0859	3.303	0.0692	0.0993
Natural disaster	1.167	0.2800	0.5967	4.498	0.0339	0.0512	14.349	0.0002	0.0022 *
Fraud	0.013	0.9086	>.9999	0.043	0.8356	>.9999	0.155	0.6942	>.9999
Insider access abuse	0.001	0.9745	>.9999	0.335	0.5625	0.7067	0.587	0.4435	0.6098
Outsider access abuse	0.657	0.4176	>.9999	1.340	0.2470	0.3391	2.920	0.0875	0.1450
Theft proprietary data	2.205	0.1376	0.2588	0.010	0.9186	>.9999	1.446	0.2292	0.3234
Viruses	2.75E-04	0.9868	>.9999	5.840	0.0157	0.0171 *	0.075	0.7837	>.9999
Secret data divulged	0.657	0.4176	>.9999	4.709	0.0300	0.0449 *	9.189	0.0024	0.0182 *
Data corruption, lost	1.058	0.3037	0.3798	3.559	0.0592	0.0669	0.023	0.8796	0.8443
Reliability problems	2.002	0.1571	0.1926	0.722	0.3953	0.4727	1.642	0.2000	0.2458
Theft computers	0.040	0.8410	0.5967	0.032	0.8581	>.9999	4.423	0.0355	0.0699
Employees abuse l'net	0.002	0.9633	>.9999	0.078	0.7805	0.7893	0.143	0.7054	0.7177
Financial loss	0.196	0.6578	>.9999	0.325	0.5685	0.6338	2.762	0.0965	0.1144

Business Continuity Plans

- Null hypotheses of equality could not be rejected
 - Internet access
 - Chi Square p value = 0.7129
 - 21.1 % vs. 24.1 %
 - Web presence
 - Chi Square p value = 0.0844
 - 26.8 % vs. 17 %
 - E-Commerce
 - Chi Square p value = 0.1811
 - 29.7 % vs. 19.8 %

Use of Technology Tools

- Internet access alone not related to aggregate count
 - Unpaired t-test p value = 0.0692
- Web Presence, E-Commerce are related to technology use
 - Unpaired t-test p values = 0.0001 and 0.0007

	Internet Access			Web Presence			E-Commerce		
	chi sq	chi sq p	Fisher's P	chi sq	chi sq p	Fisher's P	chi sq	chi sq p	Fisher's P
Anti-Virus Software	9.823	0.0017	0.0046 *	7.294	0.0069	0.0072 *	2.256	0.1331	0.1790
Data Backup System	0.682	0.4088	0.4873	8.587	0.0034	0.0038 *	0.255	0.6133	0.6805
System Access Control	0.883	0.3475	0.3721	8.670	0.0032	0.0048 *	6.143	0.0132	0.0139 *
Power Surge Protectors	2.215	0.1367	0.1873	5.574	0.0182	0.0226 *	0.150	0.6986	0.8432
Redundant Systems	0.769	0.3806	0.4263	12.930	0.0003	0.0005 *	6.832	0.0090	0.0108 *
Shredders	0.712	0.3988	0.4262	0.263	0.6081	0.6759	0.285	0.5934	0.7158
Data Segregation	3.660	0.0557	0.0754	11.692	0.0006	0.0007 *	4.641	0.0312	0.0441 *
Firewalls	1.298	0.2545	0.3607	14.308	0.0002	0.0002 *	18.681	<.0001	<.0001 *
Encryption	1.172	0.2789	0.6306	4.166	0.0413	0.0553	3.699	0.0544	0.0627
Intrusion Detection Systems	1.460	0.2269	0.3371	9.314	0.0023	0.0027 *	4.126	0.0422	0.0515
System Activity Monitor	2.003	0.1570	0.2691	6.464	0.0110	0.0133 *	2.463	0.1166	0.1362
Facility Access Control	0.440	0.5070	0.7750	5.778	0.0162	0.0183 *	5.873	0.0154	0.0349 *
Security Evaluation System	0.697	0.4038	0.5414	11.696	0.0006	0.0008 *	10.687	0.0011	0.0029 *
Dial Back Modem	0.523	0.4697	0.5037	0.119	0.7306	0.8196	1.893	0.1689	0.2228
Media Degaussers	0.001	0.9745	>.9999	1.823	0.1770	0.2358	0.058	0.8096	>.9999

Conclusions

- Mostly, the data in this research isn't surprising
 - Small businesses don't spend the money or time required to ensure holistic information security
 - Anecdotal evidence tends to indicate that small businesses aren't looking for problems and thus don't find (or see) them
- 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
 - The sociology of information security practice



Contact Information



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

1776 G. Street NW #110

Washington DC, 20052

jjchryan@seas.gwu.edu

<http://www.seas.gwu.edu/~infosec/>



The George Washington University is an NSA Certified Center of Academic Excellence in Information Assurance Education and meets the Federal Training Standards for Information Systems Security Professionals (NSTISSI 4011). We offer Graduate Certificate, Master's, and Doctoral level education in Information Security Management for professionals from all educational backgrounds. GWU is located in the heart of Washington DC very near the White House and other government offices.