Cyber Risk Perception

Aaron Fister – CISSP, CISA, CISM

PhD Candidate – University of Oklahoma

aaron.fister@ou.edu

Presented @ SIRACON 5/1/2019 – Cincinnati, OH

Do not cite information from this presentation without contacting the author first (Incase a result changes)

About Me – Aaron Fister

- **PhD Student** @ the **University of Oklahoma**
  - Areas of Study – Public Management, Risk Perception, and Research Methods
  - Dissertation – Understanding factors that influence cyber risk perceptions
  - My Interest – Study cyber risk from a human and organizational factors perspective
- 15+ years of professional experience in various Information Security roles – Federal Government, Retail, Financial Services, Insurance
  - My e-mail – **aaron.fister@ou.edu**

Outline

- Research Questions
- Overview of Data Collection
- Exploring Perception of Identity Theft / Stats 101 Refresher
- Exploring Risk Perception Scenarios
- Future Directions of this research
- Opportunities for future research collaboration

Types of Scientific Research

- **Exploratory Research** – Cause and effect is unknown
  - Little/no existing research is available
- **Confirmatory Research** – Existing research provides potential cause and effect theories
  - There should be multiple existing studies with previous findings
- **Notes:**
  - Often exploratory research is reported as confirmatory research
  - **Key** – Science is about replication
  - Disclaimer – This is exploratory research

Research Questions and Goals

- **Q1** – Is there differences in how cyber risk is perceived between the non expert and expert?
  - Or between the expert and executives?
- **Q2** – Is there difference in how people respond or react to cyber risk?
- **Additional Goal** – Learn about the process of different approaches to data collection and survey research
  - Working toward a long-term research agenda/laying the ground word

Data Collection Details

Sample	Dates of Collection	Raw count	Adjusted
Wave 1 – US Demo Sample	Sep 2018 to Dec 2018	2055	1669
Wave 2 – Cyber Risk Pro*	Dec 2018 to Feb 2019	107	90
Wave 3 – Executives*	Feb 2019	168	157
Wave 4 – Direct	Jan 2019 to Feb 2018	84	72
Wave 5 – Social Media Ads	Feb 2019	762	692
Wave 6 – MTurk P1/P2	Feb 2019 Mar 2019	1726	1322
	Total	4,902	4,002

* Over sample of Cyber Risk Pros and Executives
In addition there are approximately ~1,000 “extra” response

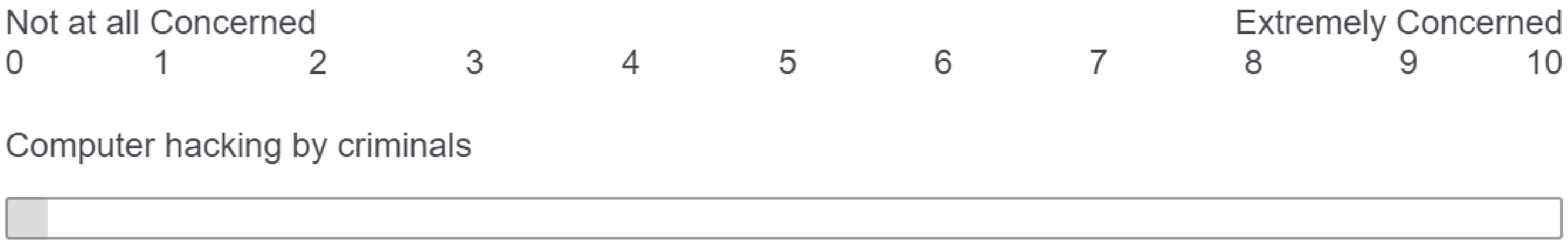
Data Collection – Notes

- **Measurement of social and human phenomena is hard**
- All information collected is self-reported
- There is no perfect data collection method
  - All collection methods have bias or sources of error
  - There were problems or interesting items of note not discussed
- **Final note** – dissertations are solo projects
  - This may explain why something was done the way it was…

Risk Perception

Survey Question: The next several questions are about important issues facing U.S. policymakers today.

For each of the following issues, please rate your level of concern using a scale from zero to ten, where zero means you are *not at all concerned* and ten means you are *extremely concerned*. How concerned are you about:



Not at all Concerned — Extremely Concerned

0 1 2 3 4 5 6 7 8 9 10

Computer hacking by criminals

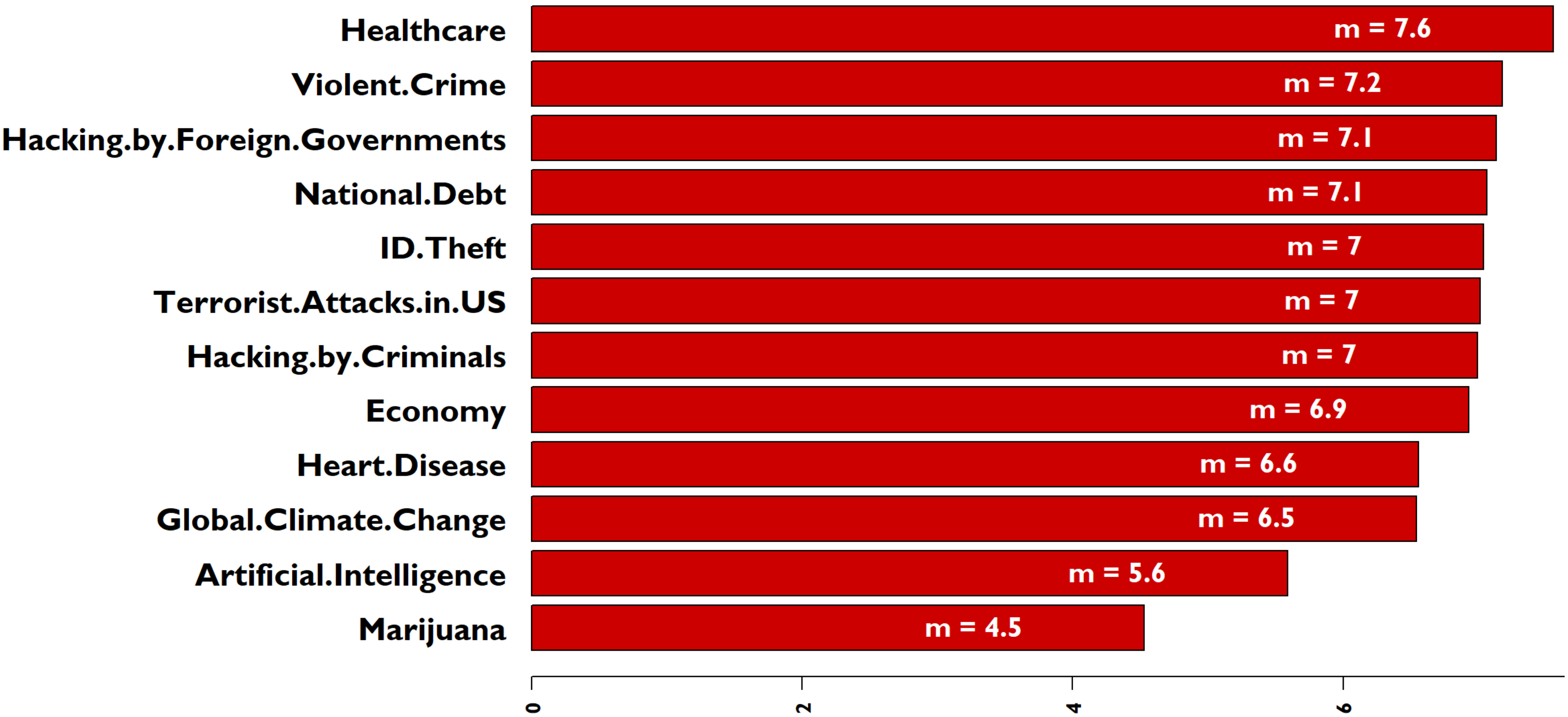
Partial List of Risks

- Artificial Intelligence
- Identity Theft
- Size of the National Depth
- State of the economy (…)
- Computer Hacking by Criminals
- Computer Hacking by Foreign Governments
- State of education
- Delivery and Cost of Healthcare
- Terrorist Attacks in the US
- Global Climate Change
- Violent Crime
- Marijuana

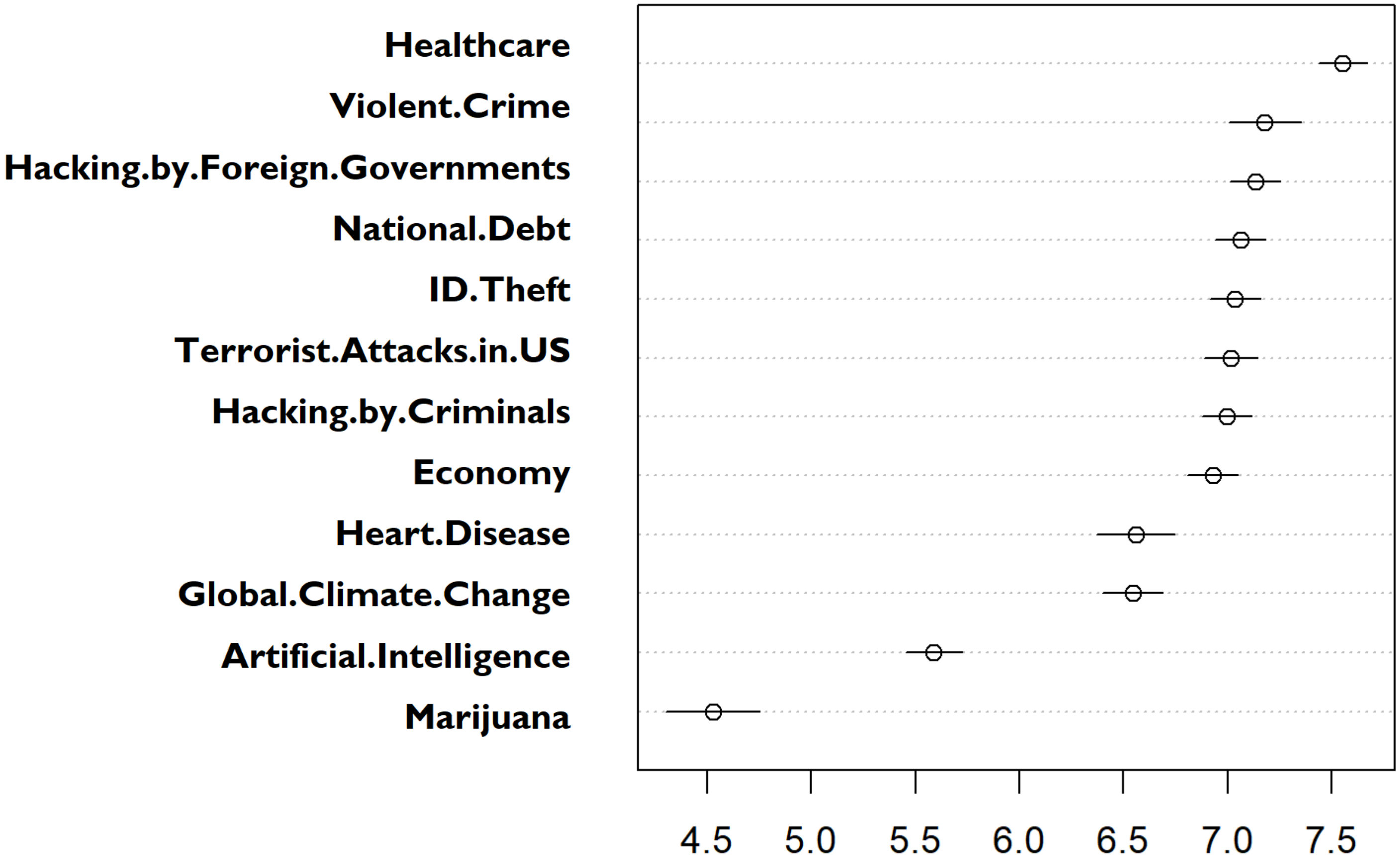
Questions to think about – Scope Wave 1

- Which do you think were be perceived as the riskiest by the US Population?
- Which ones do **you** personally perceive as the riskiest?

Risk Perception – Mean Comparison – W1

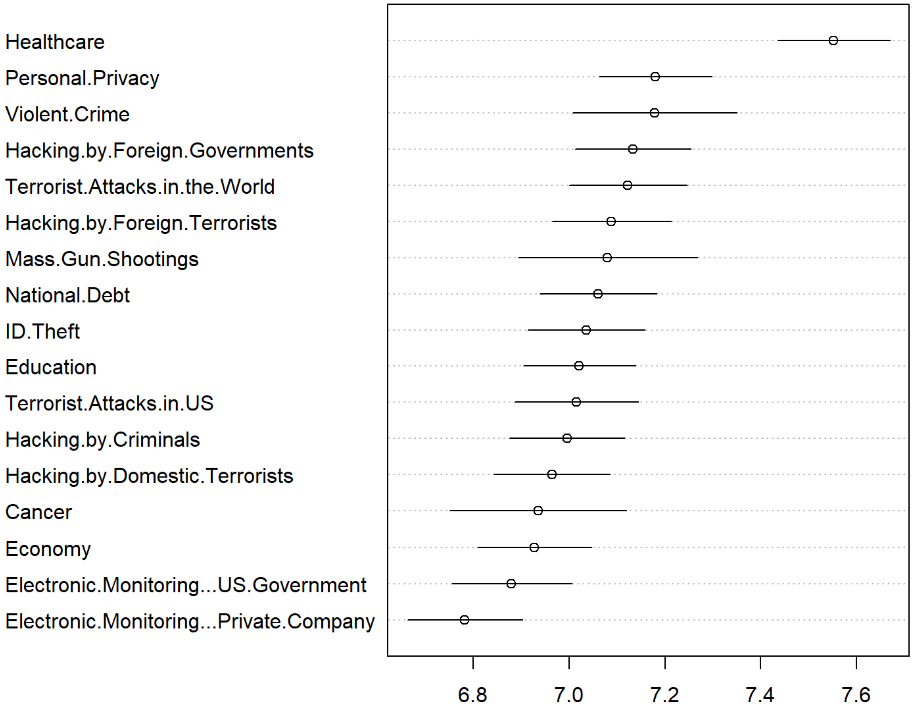


Results – Mean w/ Confidence Interval

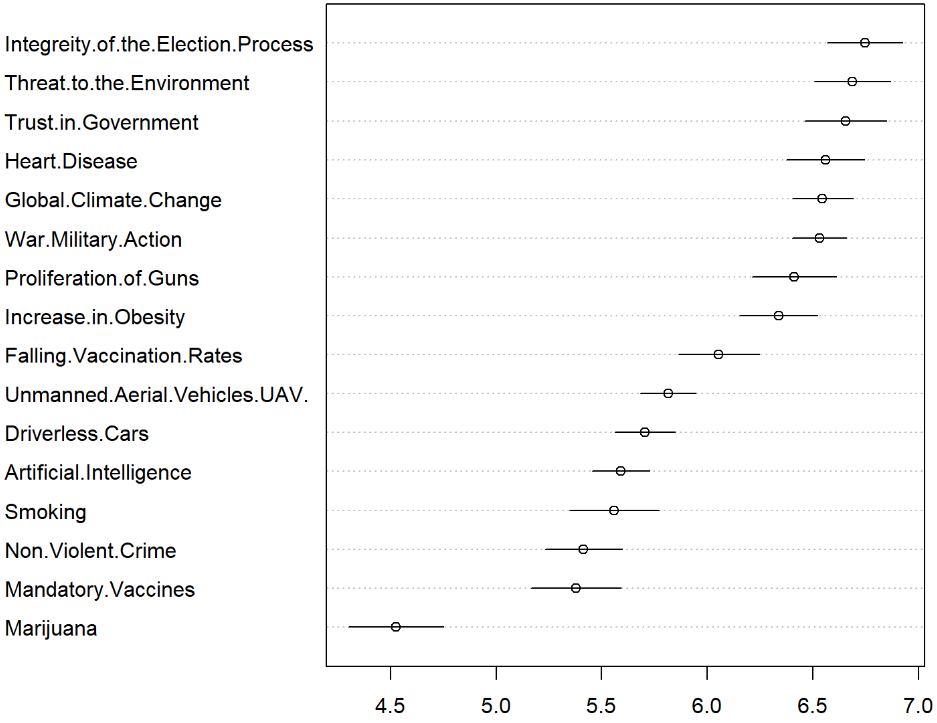


Wave I – Risk Perception Comparison

Top 17



Bottom 16



(Note the X-axis is not the same)

Risk Perceptions Detailed Results

Measure	n	Mean	Median	SE
1 Healthcare	1657	7.5	8	0.06
2 Personal Privacy	1666	7.2	8	0.06
3 Violent Crime	848	7.2	8	0.09
4 Hacking by Foreign Governments	1667	7.1	8	0.06
5 Terrorist Attacks in the World	1667	7.1	8	0.06
6 Hacking by Foreign Terrorists	1666	7.1	8	0.06
7 Mass Gun Shootings	847	7.1	8	0.1
8 National Debt	1668	7.1	8	0.06
9 ID Theft	1669	7	7	0.06
10 Education	1660	7	7	0.06
11 Terrorist Attacks in US	1661	7	8	0.07
12 Hacking by Criminals	1669	7	7	0.06
13 Hacking by Domestic Terrorists	1666	7	7	0.06
14 Cancer	818	6.9	7	0.09
15 Economy	1660	6.9	7	0.06
16 Electronic Monitoring US Government	1665	6.9	7	0.06
17 Electronic Monitoring Private Company	1667	6.8	7	0.06
18 Integrity of the Election Process	849	6.7	7	0.09
19 Threat to the Environment	849	6.7	7	0.09
20 Trust in Government	849	6.6	7	0.1
21 Heart Disease	818	6.6	7	0.1
22 Global Climate Change	1665	6.5	7	0.07
23 War Military Action	1666	6.5	7	0.07
24 Proliferation of Guns	850	6.4	7	0.1
25 Increase in Obesity	819	6.3	7	0.09
26 Falling Vaccination Rates	818	6	6	0.1
27 Unmanned Aerial Vehicles UAV	1666	5.8	6	0.07
28 Driverless Cars	1666	5.7	6	0.07
29 Artificial Intelligence	1666	5.6	6	0.07
30 Smoking	818	5.6	5	0.11
31 Non-Violent Crime	848	5.4	5	0.09
32 Mandatory Vaccines	819	5.4	5	0.11
33 Marijuana	819	4.5	4	0.11

Exploring Identity Theft
&
Statistics 101

Research Question

- Is there an observable difference in the risk perception of **Identity Theft** by different groups?

Defining the Groups for Comparison

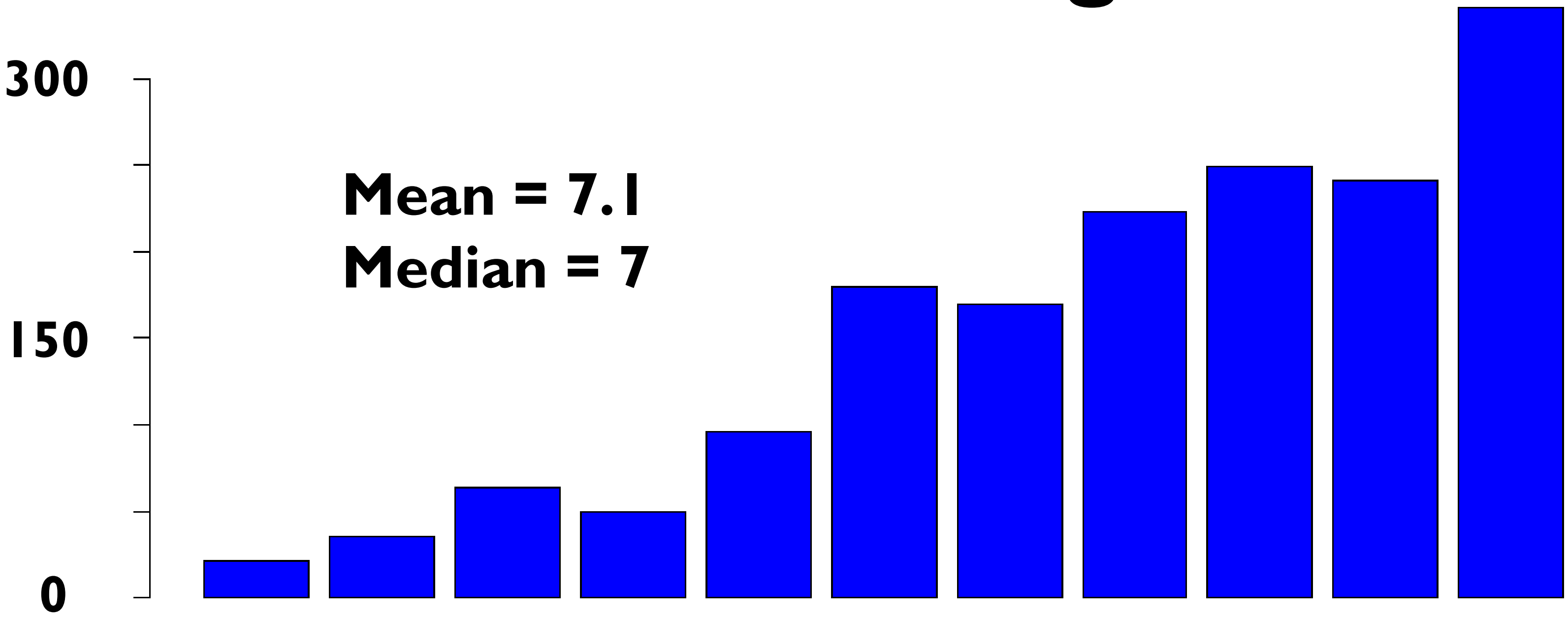
- **General Population** – Anyone who doesn't fall into one of the categories bellow.
- **IT Professionals** – An IT professional that doesn't have a CISSP, CISA, or CISM certification.
- **Information Security Professionals** – An Individual with a CISSP, CISA, or CISM certification.
- **Executives** – Any non-IT/IS Executive

Comment – there are other ways to develop this concept

Sample Counts – Wave 1 to 3

Sample	Count (n)
General Population	1387
IT Pros	135
Executives	234
Information Security Pros	160
Total	1,916

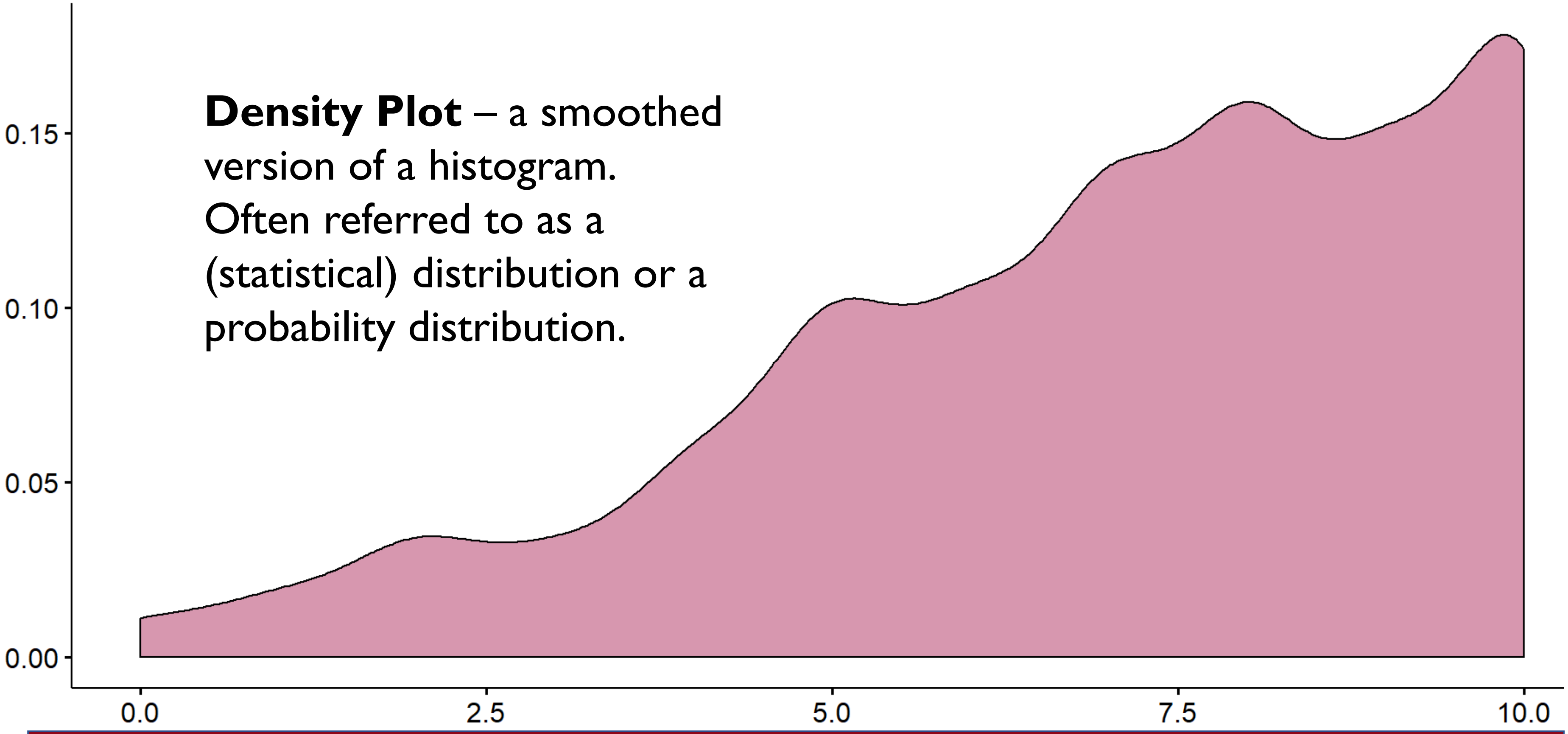
ID Theft – Bar Plot/Histogram



Mean = 7.1
Median = 7

	0	1	2	3	4	5	6	7	8	9	10
Count	21	35	64	50	96	180	169	223	249	241	341
%	1.3	2.1	3.8	3	5.8	10.8	10.1	13.4	14.9	14.4	20.4

ID Theft – Density Plot

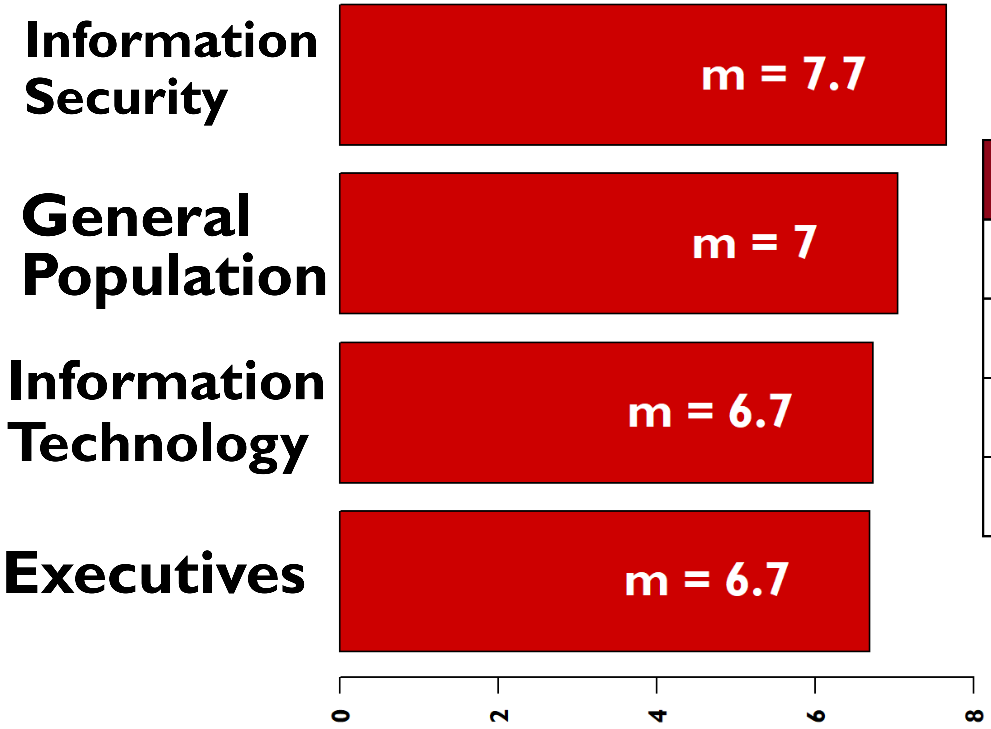


Density Plot – a smoothed version of a histogram. Often referred to as a (statistical) distribution or a probability distribution.

Presenting Differences Between Groups

- **Traditional Methods (in Scientific Journal Articles)**
  - Point Values – e.g. Present the mean with a P-Value
  - **Problem** – Point Estimates and P-Values may misrepresent an effect or not represent the actual data.
- **Newer approach**
  - Present confidence intervals (CI) of estimates visually (e.g. CI of the mean)
  - Present the distributions visually comparing the results
  - **Goal** – to express the uncertainty of estimates
  - Discussion on topic is greater than what is listed here.
  - This does not discuss a **Bayesian** workflow

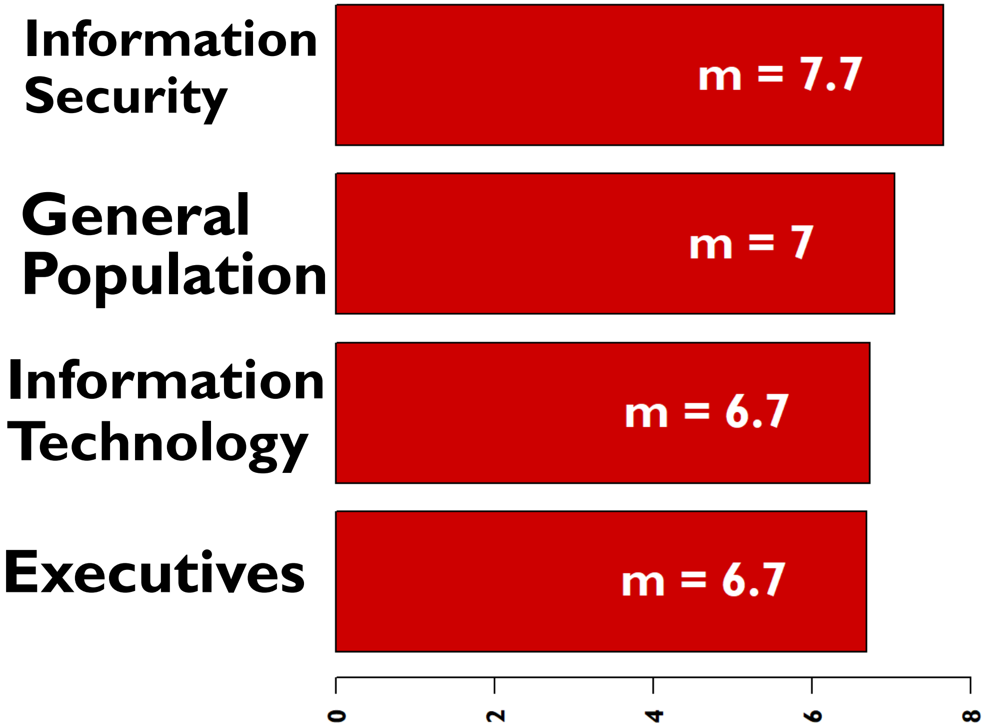
ID Theft – Point Estimates



	Median
Info Sec	8
General Population	7
Executives	7
Information Technology	7

Traditional Approach
Present Point Estimates

ID Theft – P – Values



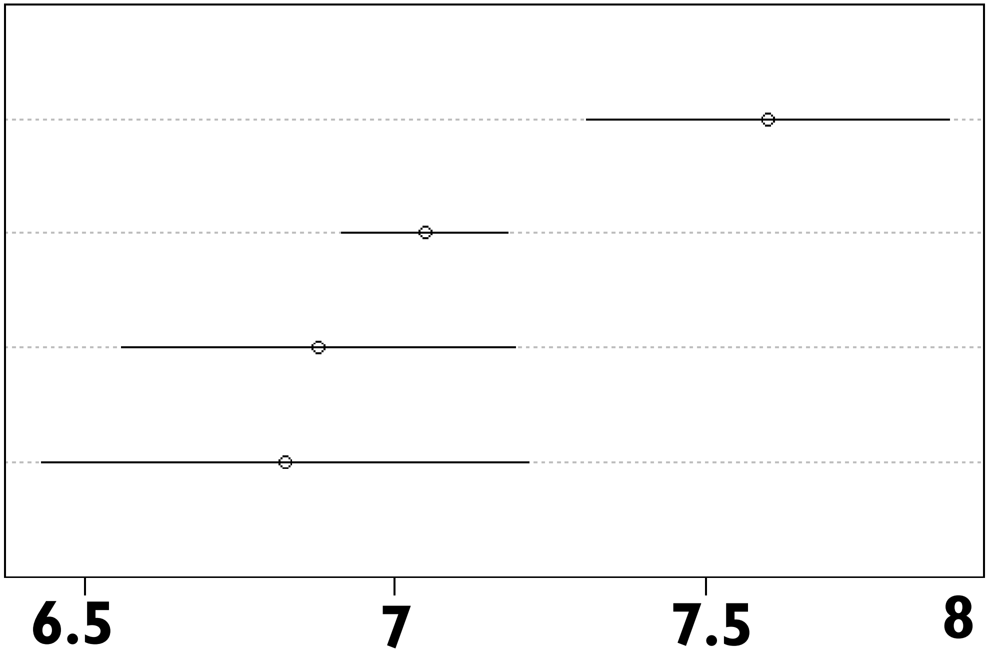
Traditional Approach – P-Value

Non-Directional T-Test	Info Sec
General Population	.0009
Executives	.001
Information Technology	.0009

Wilcox Test	Info Sec
General Population	.06
Executives	.01
Information Technology	.005

Traditionally p < .05 means a statistically significant difference between comparisons

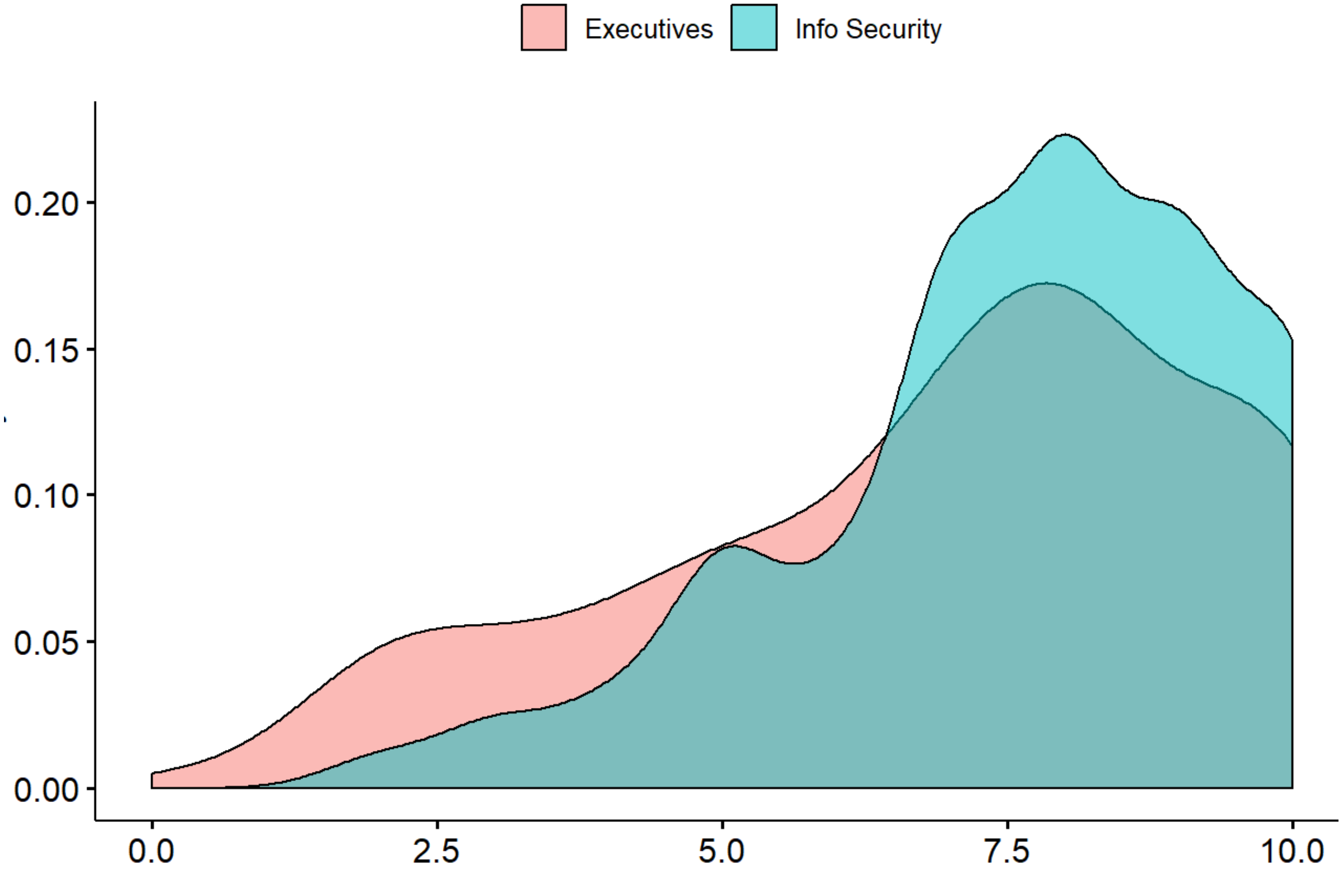
Confidence Intervals – ID Theft by Profession



Group	Mean
Information Security	7.7
General Population	7.0
Executives	6.7
Information Technology	6.7

“Dot Plot with 95% Confidence Intervals”

ID Theft – Distribution Comparison

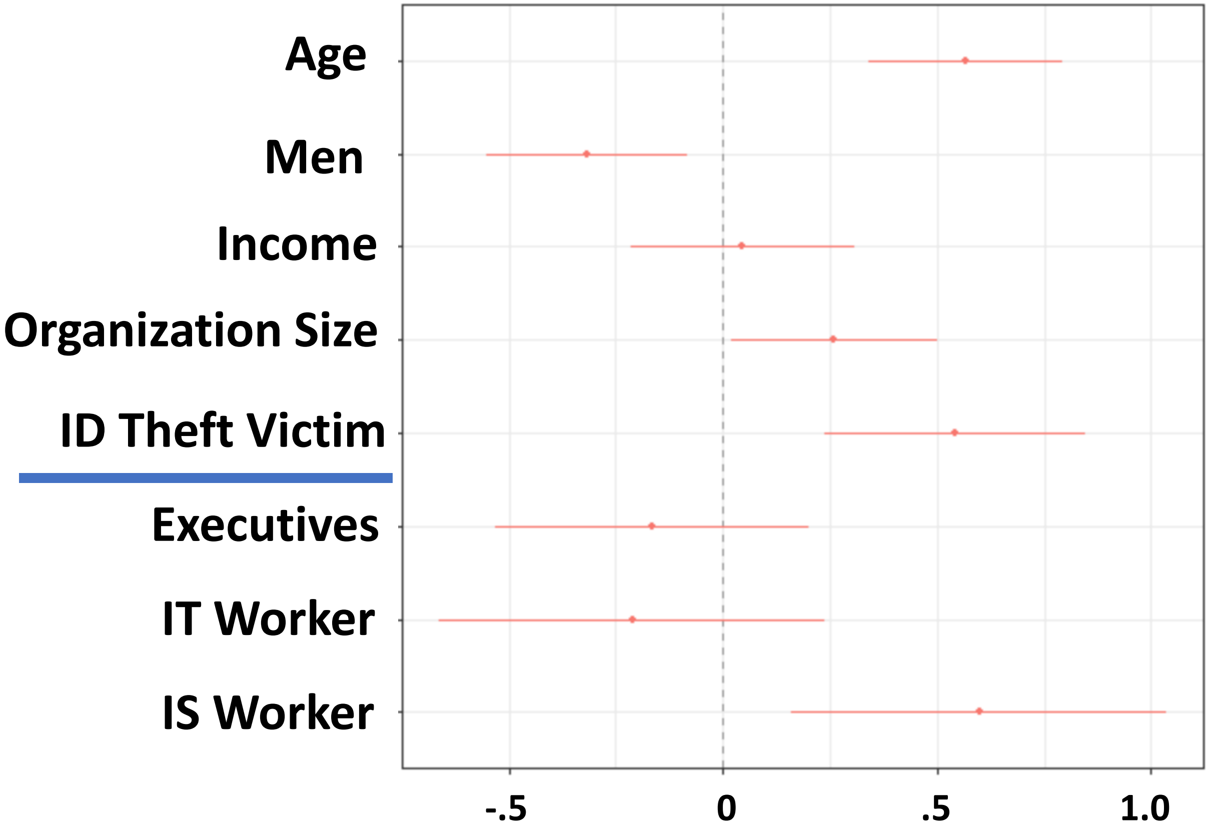


Comparing the distributions we can see the difference between information security professionals and executives.

Let's Talk About Effects Size

- **Example (of an effect/difference size)**
  - At work, if a $200,000 project is over budget by 5% – no one may care
  - At home, if you are buying a $200,000 house – a 5% increase in price – you may care
  - This is part of the reason topic such as p-values, difference comparisons are misunderstood.
    - There are statistical measures known as effect size – blindly following them is a bad practice.
    - Yes – this does apply when developing machine learning algorithms and artificial intelligence.
- The **size of an effect between comparisons** is highly contingent based on:
  - Situation
  - Values of the decision maker (or reader)
- **Final Note** – Recall, science is about replication, a second study may have a different effect size

ID Theft Model – Coefficient Plot



- Additional Variables with no effect*
  - Education
  - Race
  - Income
  - Political Ideology
  - Political Party
- Executives, IT Workers, and IS Workers are in comparison with the General Population (aka the reference category)

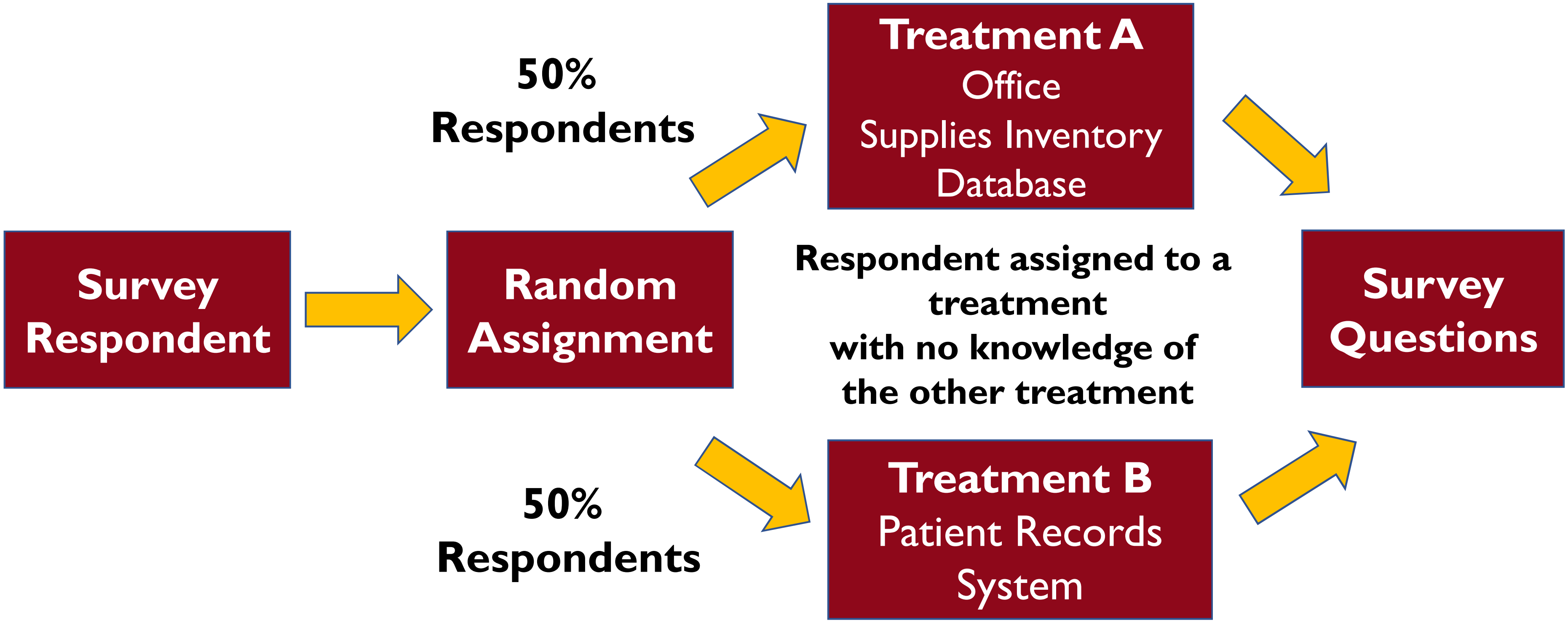
* Additional modeling is needed; Org size needs more exploration.

Scenario One – System Type

Question Wording

- For this question, you take on the role of Chief Executive Officer (CEO) of a health care provider to 15 million patients in 30 different states.
  - You have been notified by your Chief Information Security Officer (CISO) that healthcare regulators have identified a serious vulnerability in the **[SYSTEM X – See next Slide]** that allows an unauthorized third party to gain access to all data stored on the system.
  - Utilizing a scale of zero to ten, where zero means *no risk* and ten means *extreme risk*, how much risk is this to the organization?

Survey Experiment



Survey Respondent

Random Assignment

50% Respondents

Treatment A
Office
Supplies Inventory
Database

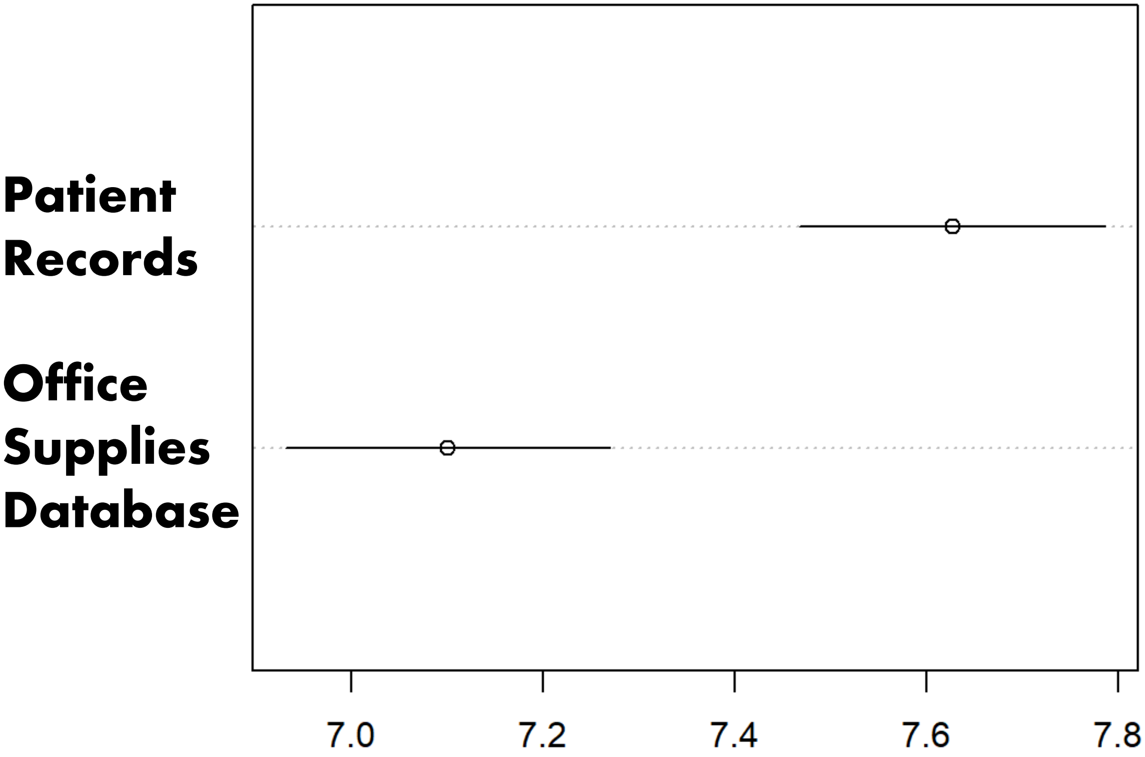
50% Respondents

Treatment B
Patient Records
System

Respondent assigned to a treatment with no knowledge of the other treatment

Survey Questions

Mean Comparison – Gen Pop – Wave 1

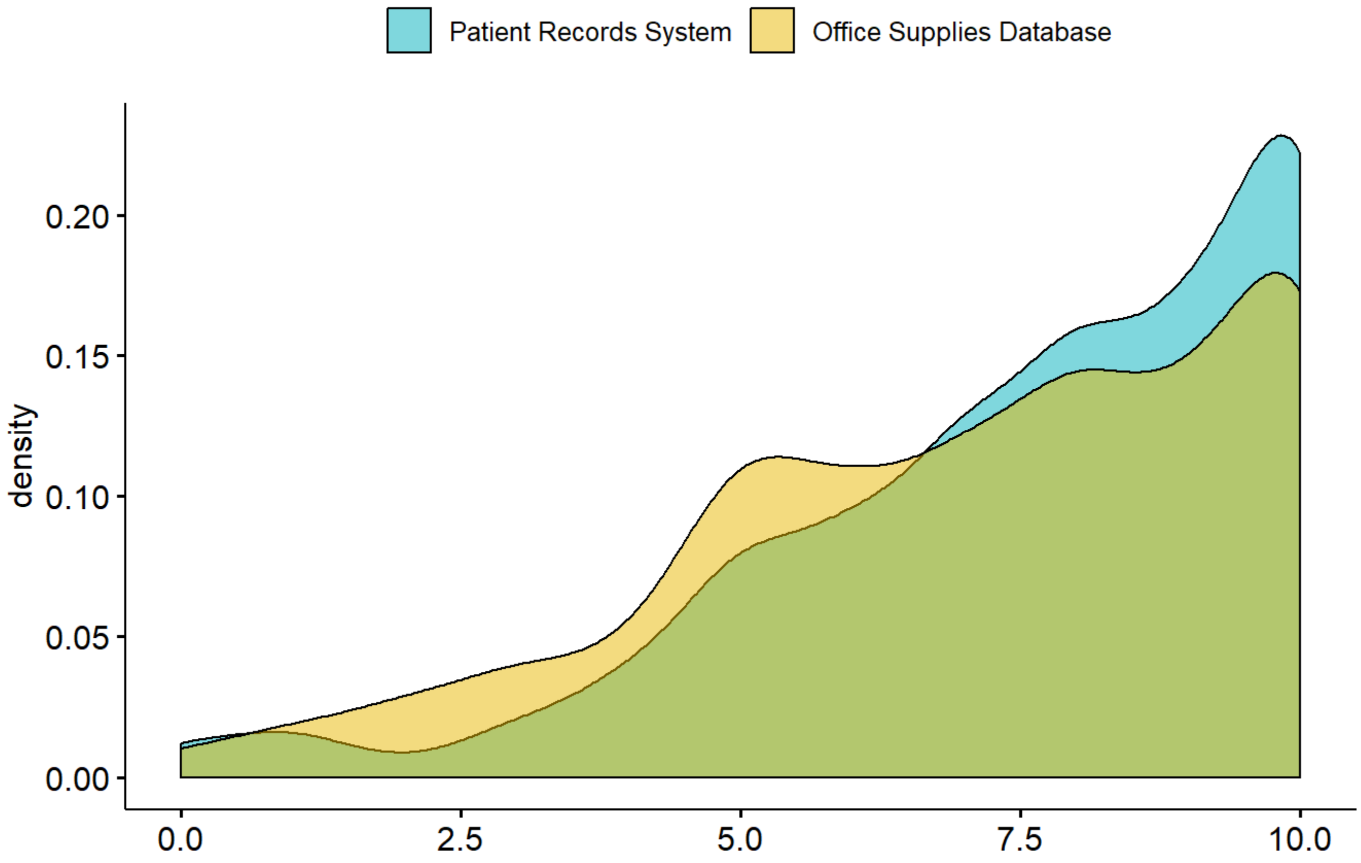


The treatment groups have clear differentiation.

	Mean	Median	n
Patient Records	7.6	7	823
Office Supplies	7.1	7	844

Statistical Tests
T-Test p-value: < .0001 (T = -4)
Wilcox Test: < .0001
(non directional)

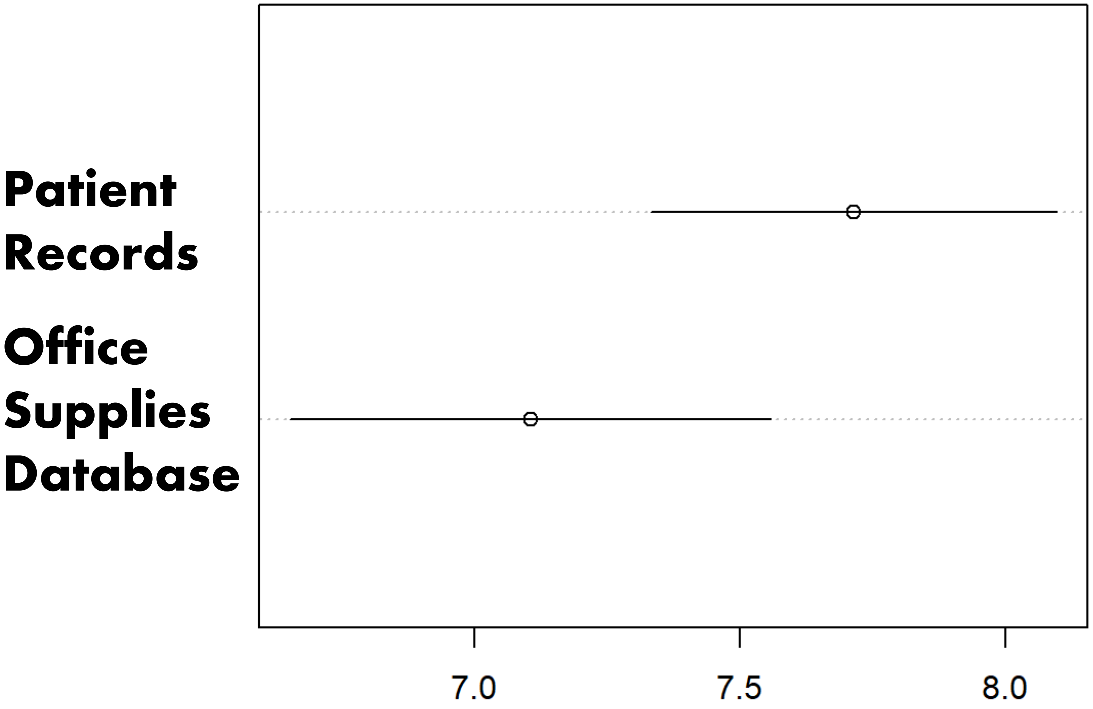
Wave I – Gen Pop – Distribution



Analysis:
The distribution shows the survey experiment is working. The different samples (on average) are reading and interpreting the risk like we assume they would.

There is a concern, that too many people are over estimating the Office supplies database risk.

Comparing Executives – Wave 1 to 3



	Mean	Median	n
Patient Records	7.7	8	112
Office Supplies	7.1	8	122

Statistical Tests

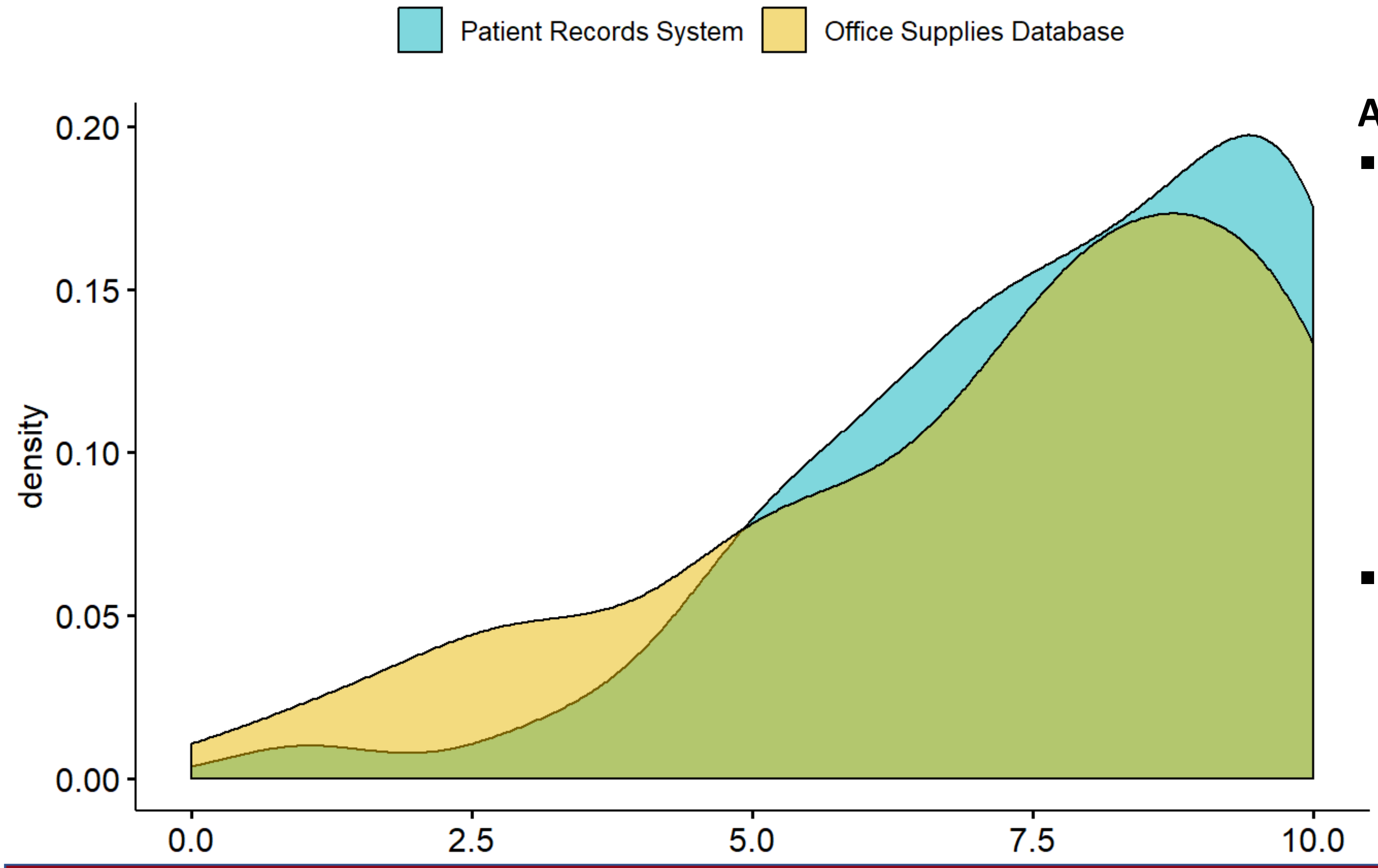
T-Test p-value: = .05 (T = -2)

Wilcox Test p-value: = . 1

(non directional tests)

There is an effect, it doesn’t appear to be as strong, but the sample size is smaller.

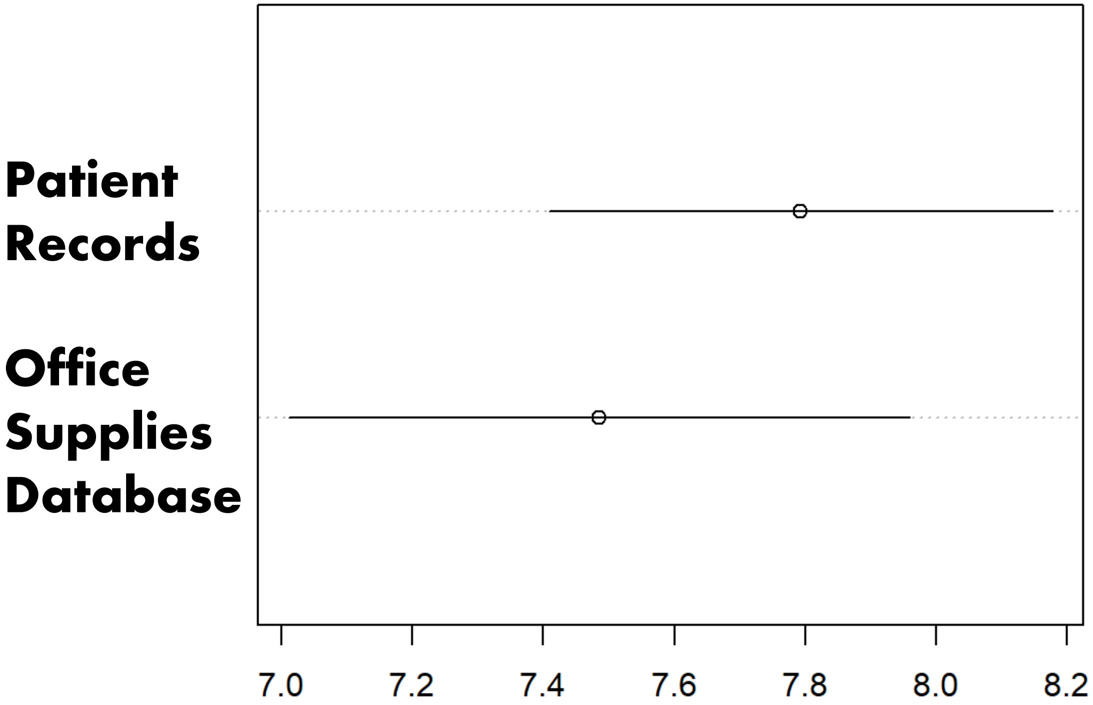
Executives Distribution (Wave 1 to 3)



Analysis:

- We see the same pattern as the general population. There is a shift. Less % people rated the office supplied as a "10" risk.
- There is a concern, that too many people are over estimating the Office supplies database risk.

Comparing IS Professionals

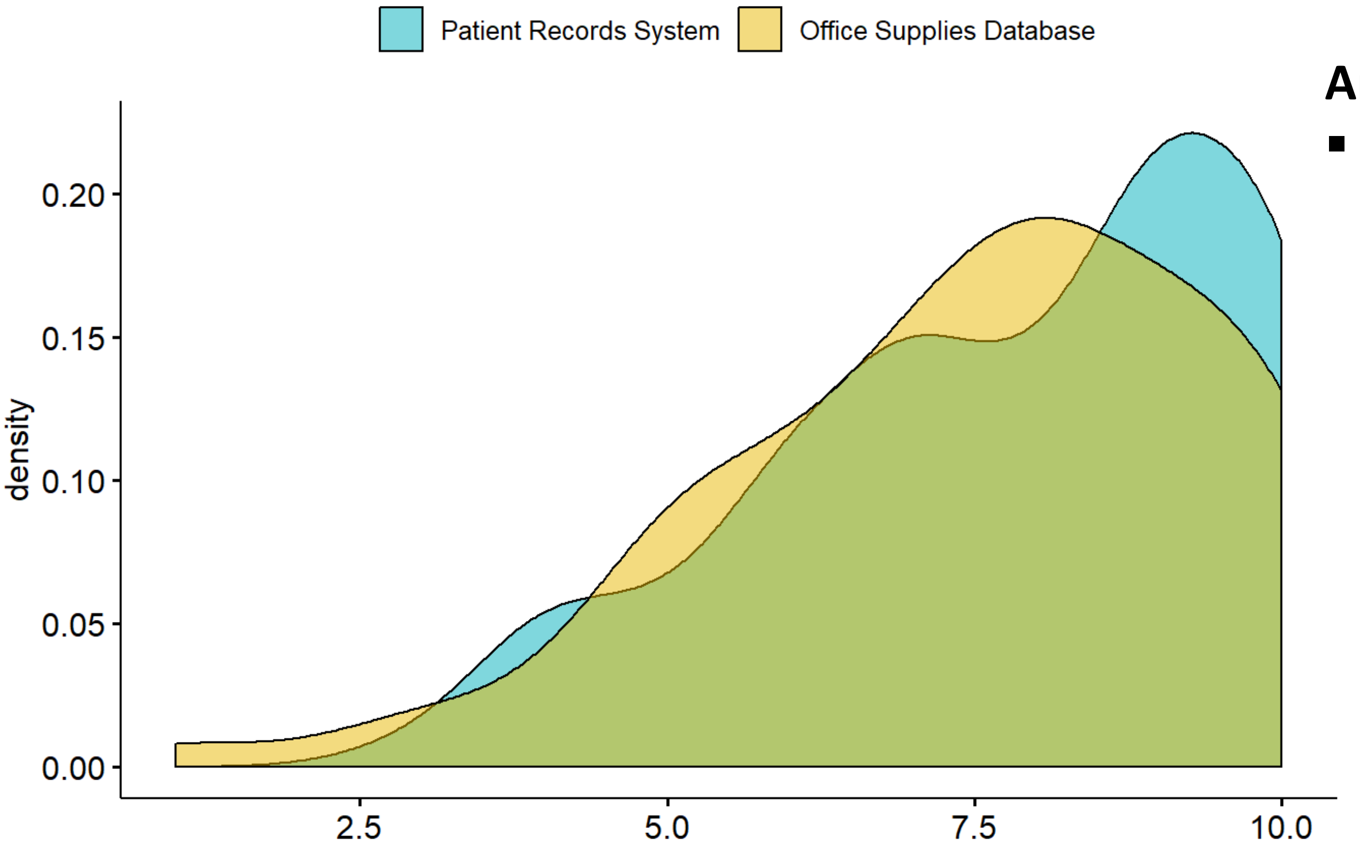


	Mean	Median	n
Patient Records	7.8	8	92
Office Supplies	7.5	8	68

Statistical Tests
T-Test p-value: = .3 (T = -1)
Wilcox Test p-value: = .3
(non directional tests)

There is an effect, it appears to lessen with IS Pros. Though it may be due to the sample size.

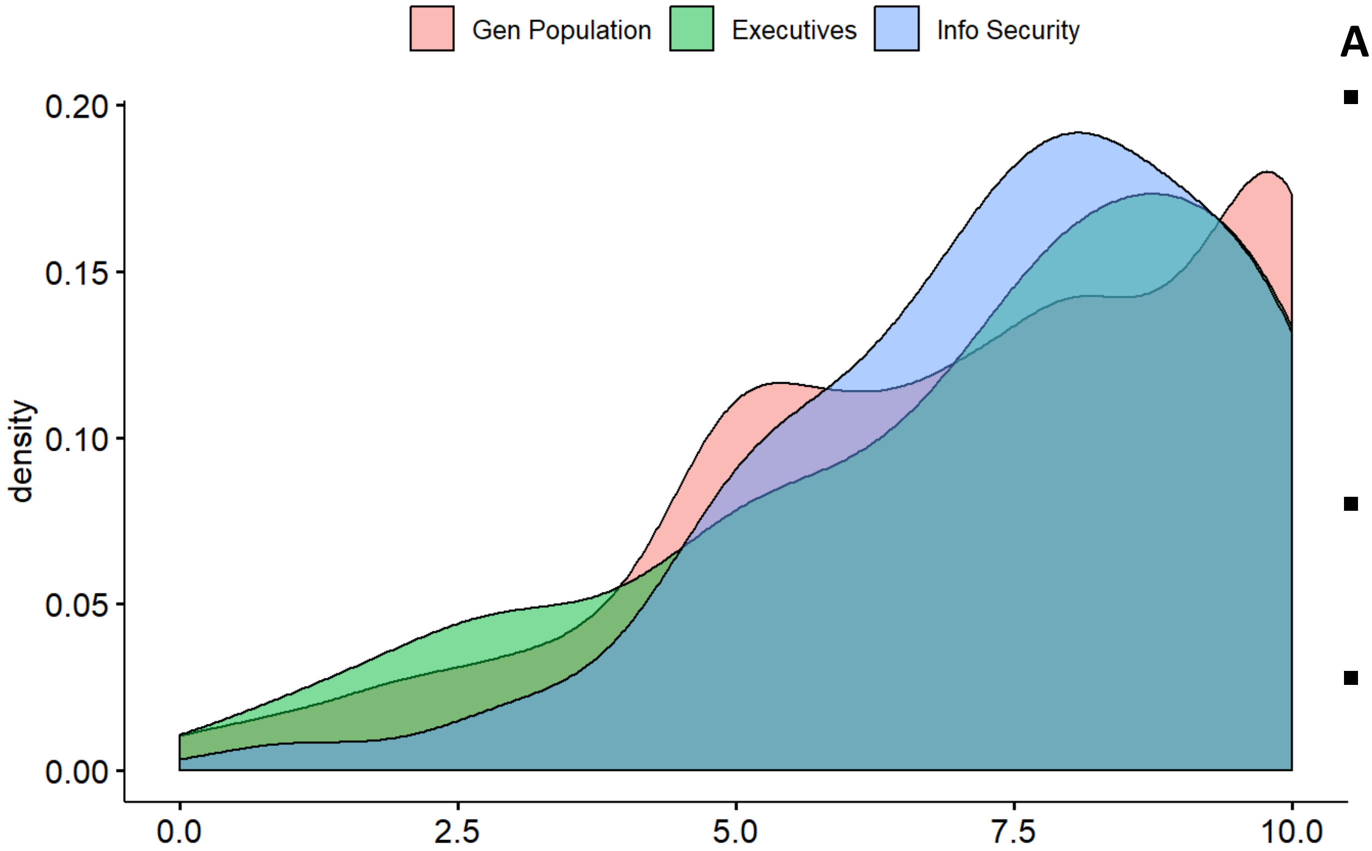
Distributions – IS Pros – Wave 1 to 3



Analysis:

- There is a concern, that too many people are over estimating the Office supplies database risk.

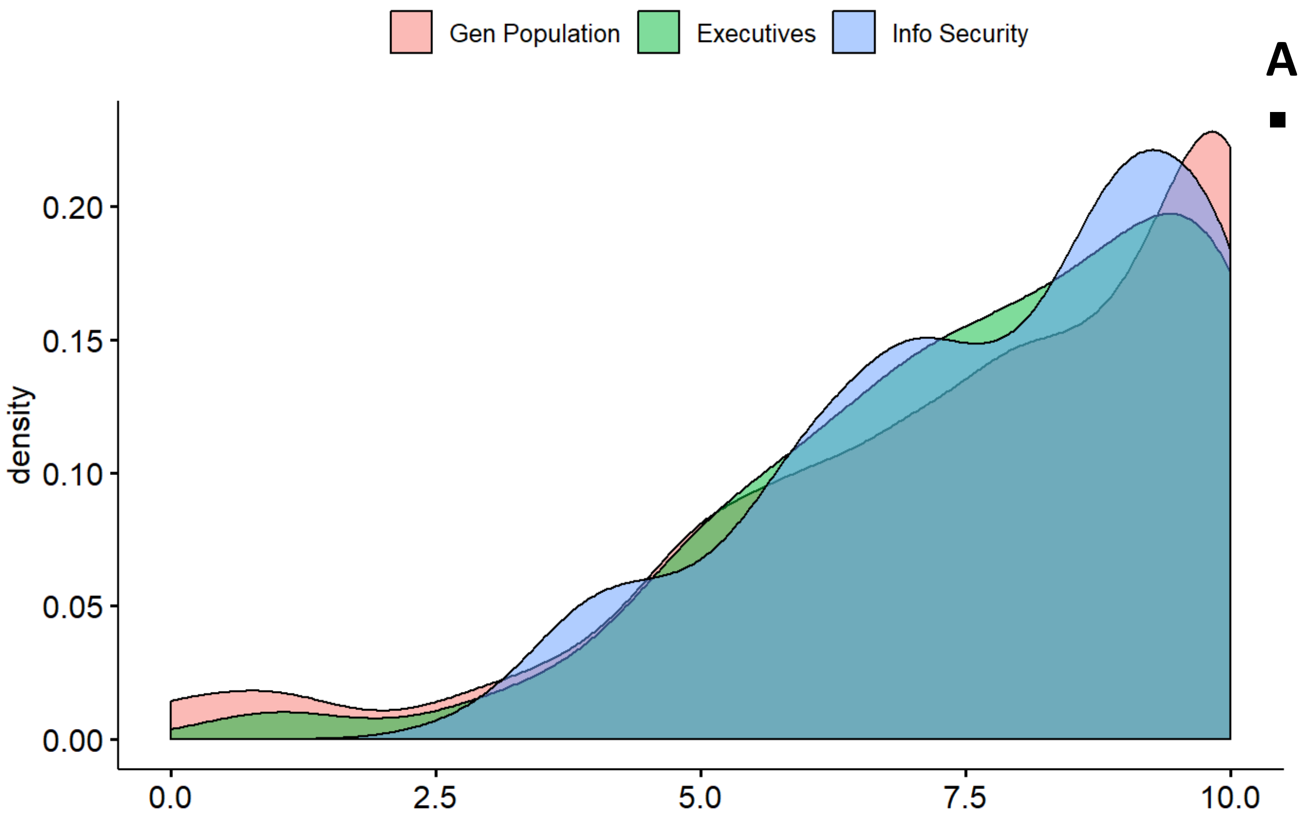
Office Supplies Database by Profession



Analysis:

- We can see how the (over) estimation is differences between the General Population, IS Professionals, and Executives.
- Percentage wise more Executives rate the risk lower.
- Most IS professionals rate the risk in the top half of the scale.

Health Database by Profession



Analysis:

- Overall similar distributions

What did we learn?

- The survey experiment is working
- There may be an overestimation of risk with the office supplies database.
  - “Treat diamonds like diamonds, pencils like pencils” – Quote unknown

- **Criticism**
  - But there isn’t enough information, so we really don’t know risky this is…
  - True, the formal writeup/analysis would need to state limitations.

Scenario
Comparing Risk Prioritization

Quantitative vs Qualitative Scenario

- You are CEO for an e-commerce company with $100 Million per year in Revenue
- 95% of revenue is generated through website sales.
- A Critical Vulnerability in the e-commerce websites was identified an it has the potential to impact sales.
- **Two Treatments** – exact same information but…
  - Quantitative Treatment has
    - Two Extra Columns (2/3) in the table (next slide)
    - Additional sentence was added

Quantitative vs Qualitative – Text

For this scenario, you are the Chief Executive Officer (CEO) for an e-commerce retailer Star Industries. Star Industries markets home gaming systems directly to consumers through their website. Star Industries has $100 million per year in revenue. Ninety-five percent of the of the revenue is generated via website sales.

The Chief Information Security Officer (CISO) has notified you of a critical vulnerability in the main e-commerce website that has the potential to impact sales. The vulnerability potentially allows a hacker to take control of the e-commerce website, stealing customer information including credit card numbers. If an event were to occur, a website outage may last up to one week and would receive media attention.

A risk analysis was completed.

Analysis Findings

- The final risk has a rating of **High** based on the table below.
- The vulnerability is such that the risk scenario is very likely to occur.
- Based on a quantitative simulation of the risk event, the annualized 90% confidence estimate for the impact of the risk event is $1.2 million to $10.8 million. The best estimate (median loss) is estimated at $6.2 million. - Additional Language

Previously company executives and the board of directors agreed to the following criteria for company risks.

** Table **

Analysis Methodology

- The analysis was based on estimates of both the likelihood of the event and the potential impact.
- The potential impacts include estimates for the loss of sales, incident response costs, recovery costs, fines, and future legal action.

Utilizing a scale of zero to ten, where zero means *no risk* and ten means *extreme risk*, how do you perceive the risk to the organization from the above scenario?

Quantitative vs Qualitative Table

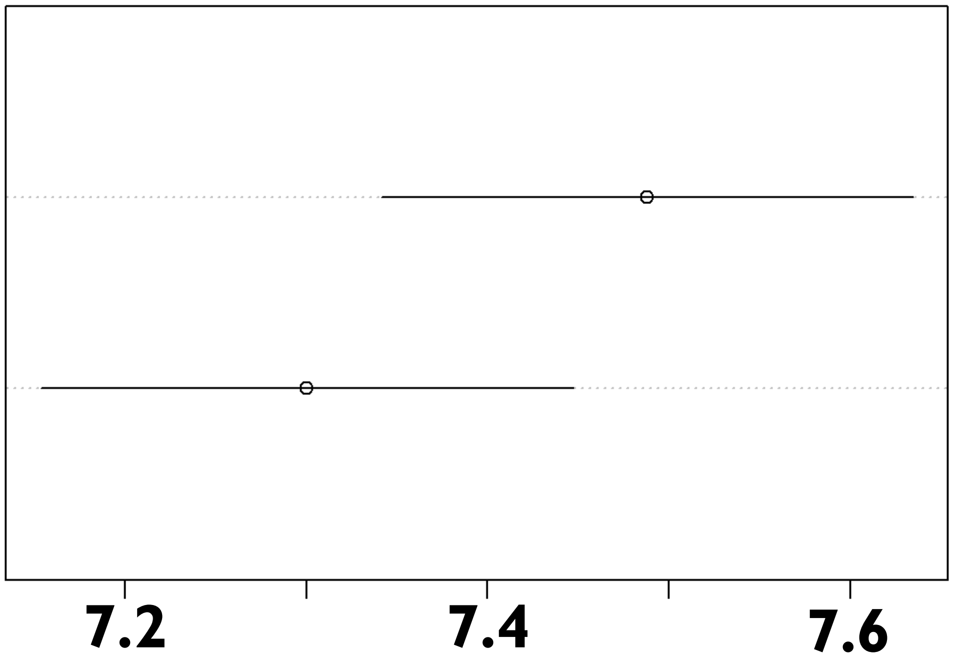
Rating	Financial Impact	Financial Impact as % of Yearly Revenue	Description
Very High	$10 Million +	10% or more	The risk could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets or individual.
High	$2 Million to $10 Million	2% to 10%	The risk could be expected to have a severe or catastrophic adverse effect on organizational operations or organizational assets. The event may cause severe degradation in one or more of the organization’s primary functions, or the risk may result in a major financial loss or loss of life.
Moderate	$500,000 to $2 Million	.5% to 2%	The risk could be expected to have a serious adverse effect on organizational operations or organizational assets. The event may cause significant degradation in one or more of the organization’s primary functions, or the risk may result in a significant financial loss or significant harm to individuals that do not involve the loss of life.
Low	$100,000 to $500,000	.1% to .5%	The risk could be expected to have a limited adverse effect on organizational operations or organizational assets. The event may cause a noticeable degradation in one or more of the organization’s primary functions, or the risk may result in a minor financial loss or minor harm to individuals.
Very Low	<$100,000	Less than .1%	The risk could be expected to have a negligible adverse effect on organizational operations or organizational assets.

Additional – "Quantitative" Sentence

- Based on a quantitative simulation of the risk event, the annualized 90% confidence estimate for the impact of the risk event is $1.2 million to $10.8 million. The best estimate (median loss) is estimated at $6.2 million.
- **Question** – Which group will have the higher risk perception?

Wave I Comparison – Risk Perception

Group	Mean
Qualitative	7.5
Quantitative	7.3



"Dot Plot with 95% Confidence Intervals"

Note – This effect may not be substantive

Statistical Tests

T-Test p-value: = .08
(T = -2)
Wilcox Test: = .06
(non directional)

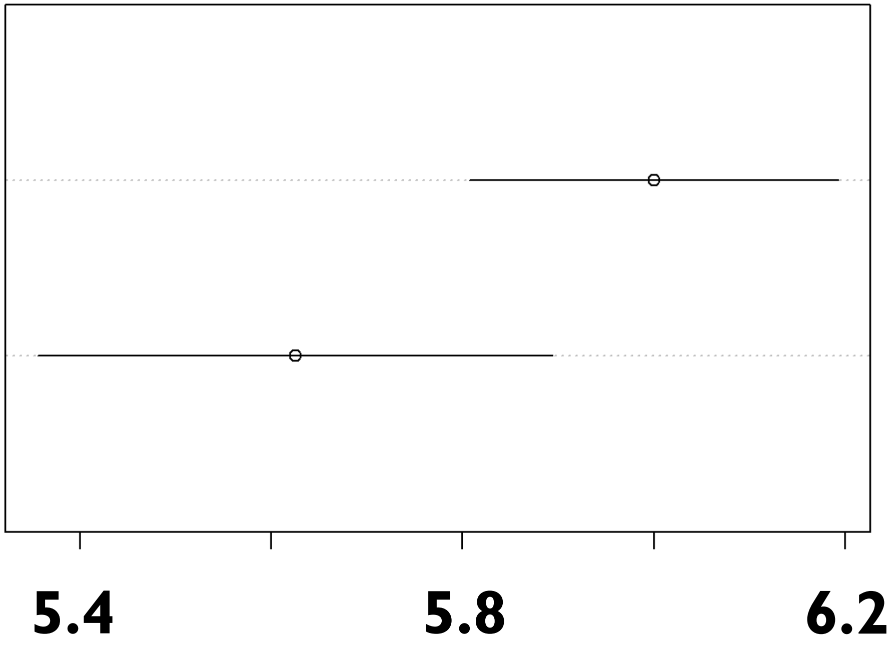
Follow up questions…

- On a scale of one to seven where one means *strongly disagree* and seven means *strongly agree*, please respond to the following statement.
  - If management should take immediate action to address the issue...

- Let's look at executives only...

Wave 1 to 3 – Executive Response

Group	Mean
Qualitative	6.0
Quantitative	5.6



“Management should immediately respond”

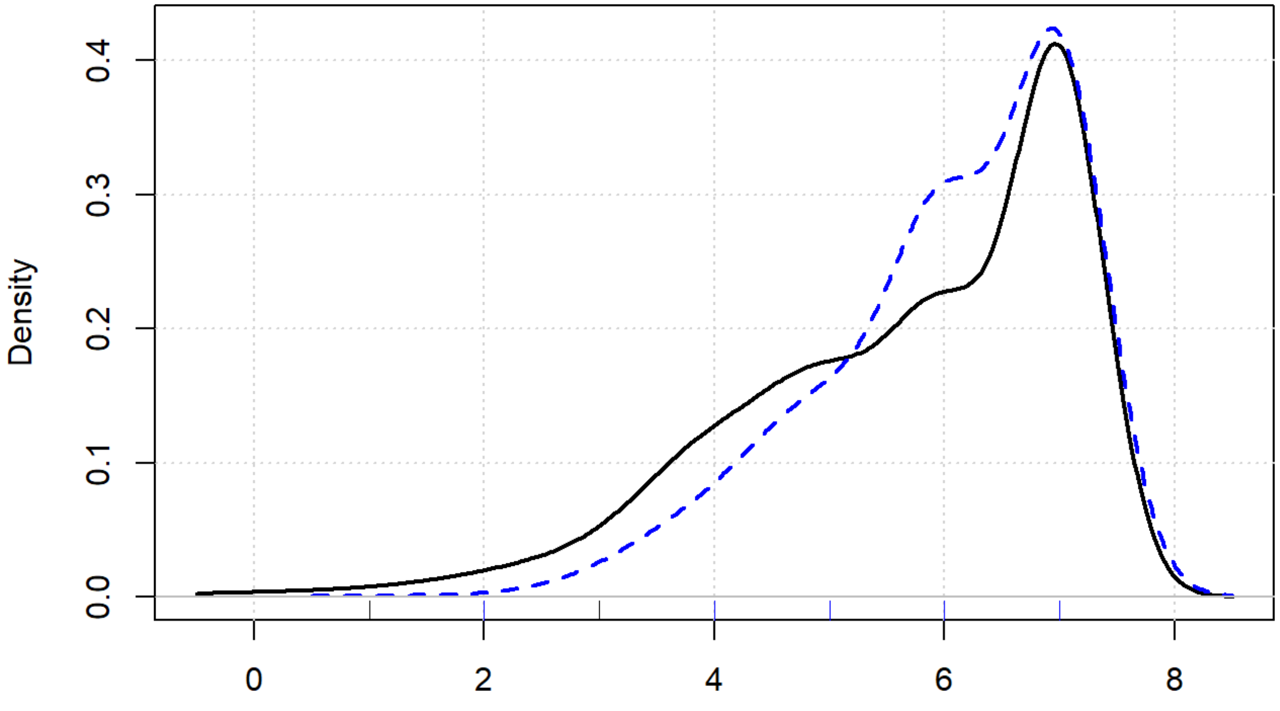
7 = Agreement with Statement

Statistical Tests

T-Test p-value: = .03
(T = -2)

Wilcox Test: = .1
(non directional)

Management Response – Distribution Comparison – Executives



Legend

- **Dotted Line is Qualitative**
- **Solid Line is Quantitative**

Analysis

- There appears to be a response difference in the presentation
- This does not provide evidence for or against Quantitative/Qualitative Analysis
- Potentially education on quantitative output is needed
- More research is needed

Scenario
Comparing Risk Prioritization by Industry

Risk Prioritization by Industry

- **Scenario**
  - You are Chief Executive Officer (CEO) of a $10 billion per year in revenue company with 6,000 employees.
- **Experiment**
  - **Text A** – … ***advanced tank weapons system manufacturing*** *company where 95% of the revenue is based on established contracts with the United States military.*
  - **Text B** – …***low-cost furniture manufacturing company*** *where 95% of the revenue is based on sales directly with home consumers.*

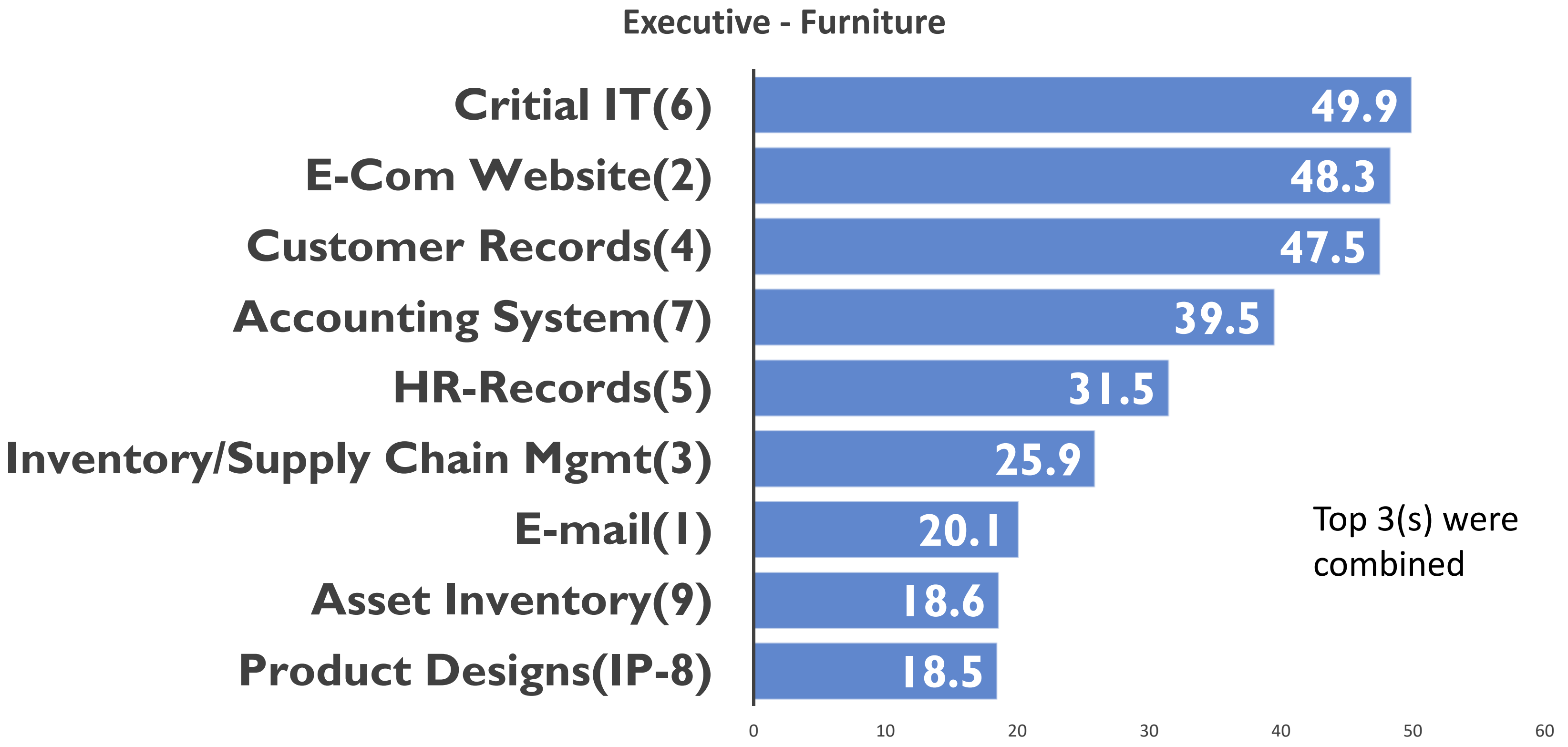
Rank the Top 3 Highest Priority Systems

- E-Mail
- E-commerce website (including Credit Card Information)
- Inventory/Supply Chain Planning and Management
- Customer Records system
- Human Resources system that contains employee records
- Critical IT Support Infrastructure (Firewalls / Network Equipment)
- Accounting System (Accounts Payable / Accounts Receivable / General Ledger)
- Product Designs and Development System (Including Intellectual Property)
- Asset Inventory System

Questions

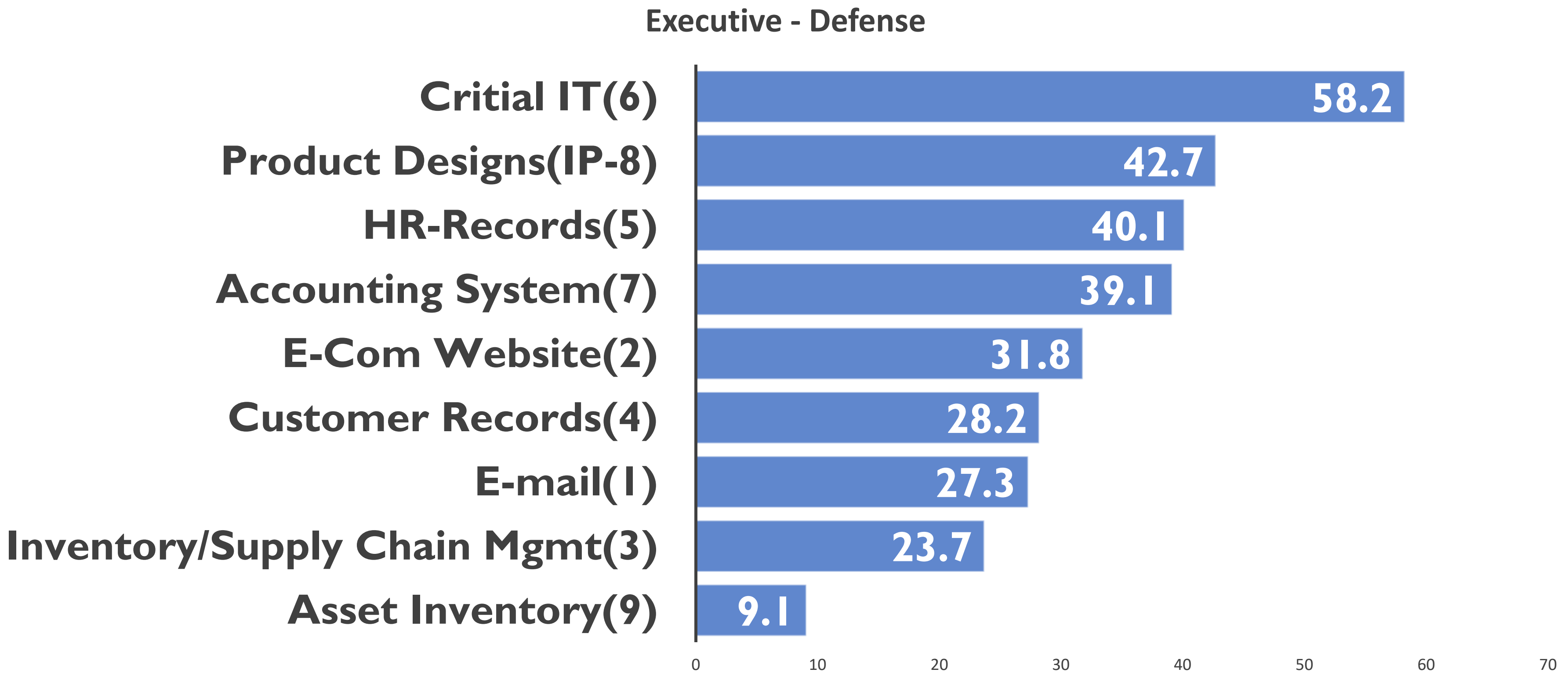
- Will the ranking/priorities be different between furniture and defense manufacturing companies?
- Will the ranking/priorities be different between Executives and Information Security Professionals?

Executive – Furniture – Top 3

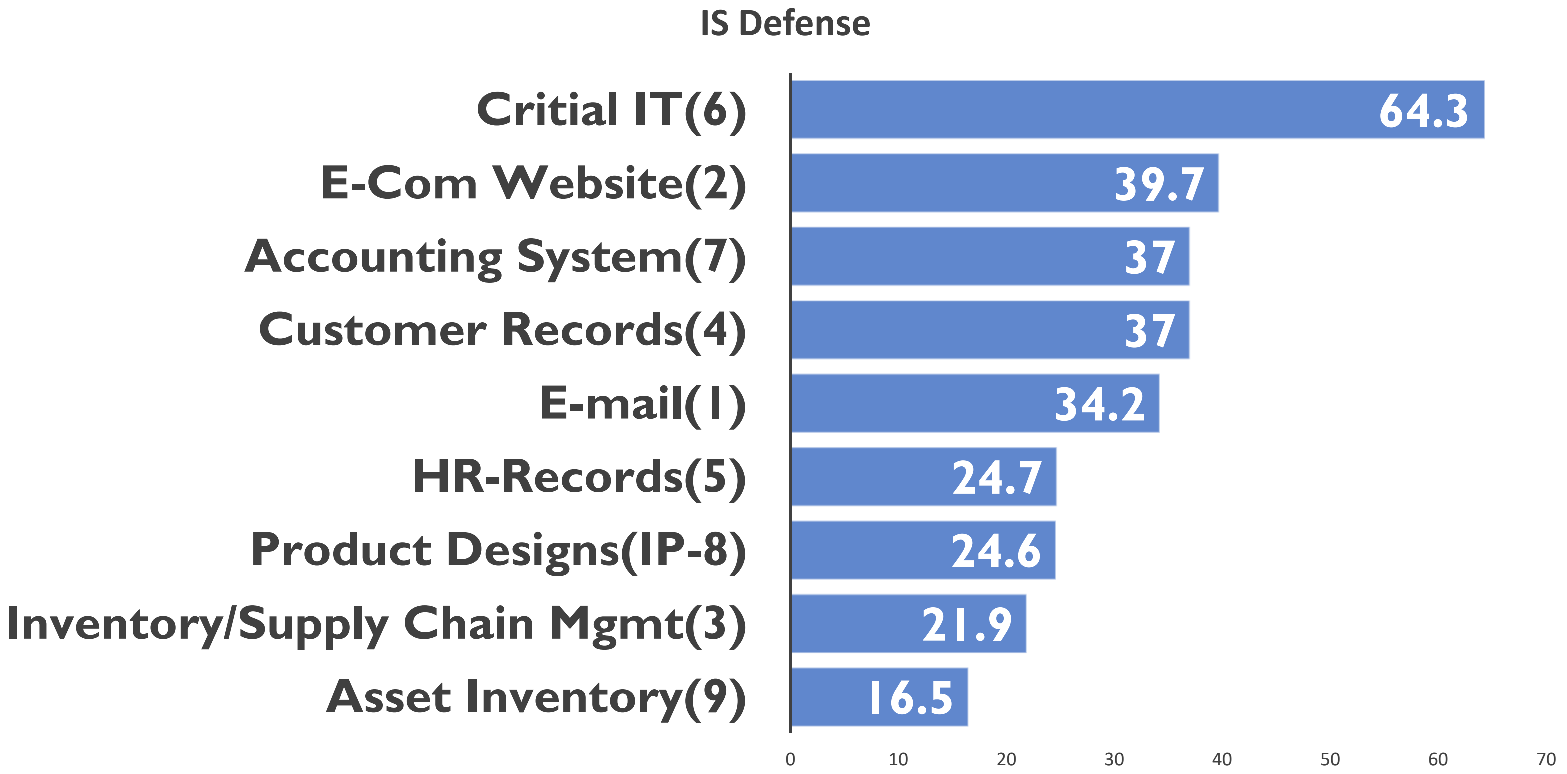


Top 3(s) were combined

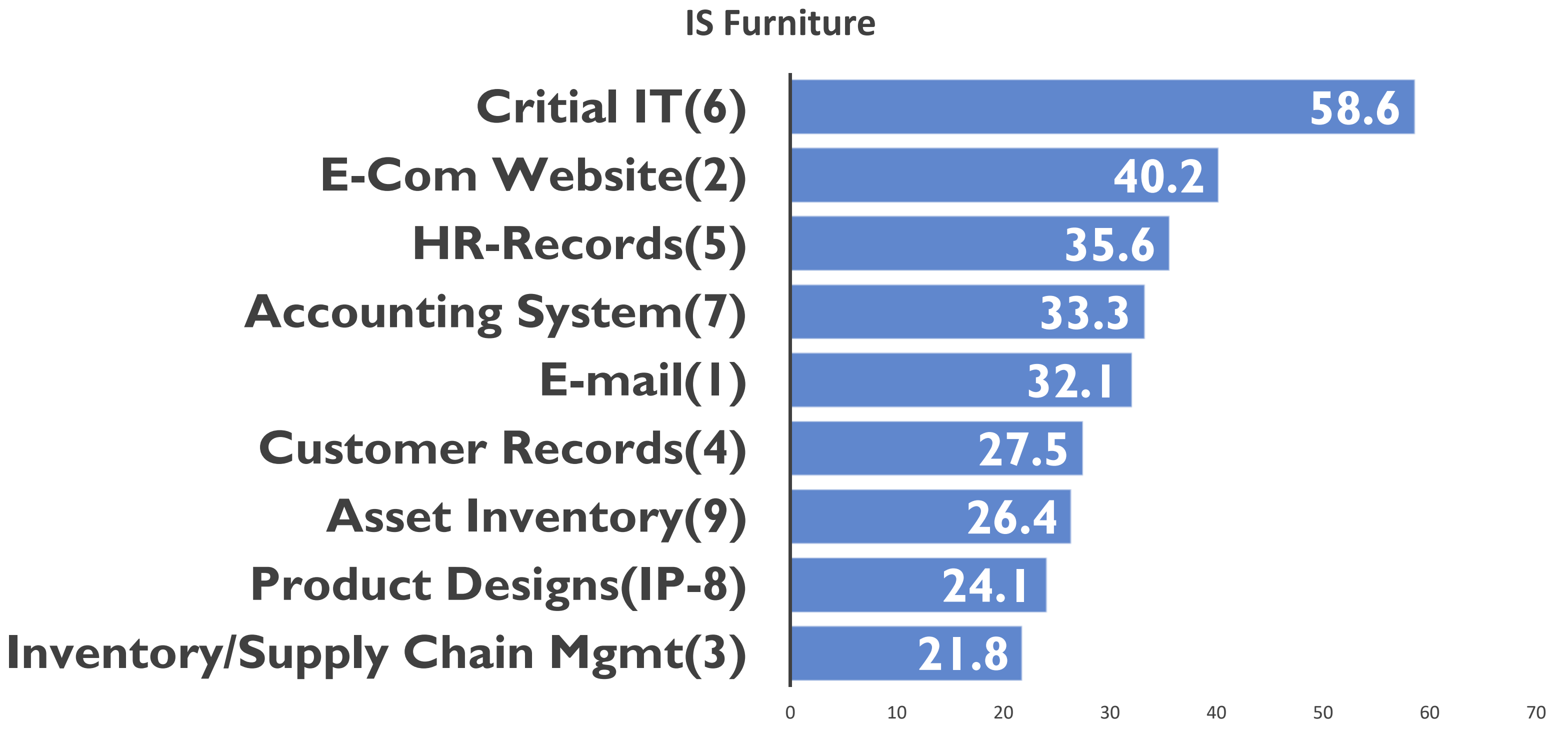
Executive – Defense – Top 3



Info Sec – Defense – Top 3



Info Sec – Defense – Top 3



Defense – Executives vs Info Sec

Exec-Defense	% in Top 3
Critical IT	58
Product Designs (IP)	42
HR Records	40.1
Accounting System	39.1

IS-Defense	% in Top 3
Critical IT system	64.3
E-commerce Web Site	39.7
Customer Records	37
Accounting System	37

What can explain this difference?

Furniture – Executives vs Info Sec

Exec – Furniture	% in Top 3
Critical IT	49.9
E-Commerce Web Site	48.3
Customer Records	47.5
Accounting System	39.5

Info Sec – Furniture	% in Top 3
Critical IT system	58.6
E-Commerce Web Site	40.2
HR Records	35.6
Accounting System	33.3

Recommendations

- Make sure to have discussion with IS, IT and Risk teams about understanding what is the purpose of the organizations, what are the goals?
    - IT and IS needs to understand what the organization does.
- **IS Pros** – You may need to communicate why a system is higher risk from a (technical) risk perspective
    - E-commerce web site is an ingress point to a network.
    - (This could explain why E-commerce web site was # 2)

Detailed Results

Executives (n = 234 – then split)	Top IT Risk		Second IT Risk		Third IT Risk			
Top IT Risk	**Defense**	**Furniture**	**Defense**	**Furniture**	**Defense**	**Furniture**	**Defense Top 3**	**Furniture Top 3**
E-mail(1)	10.9	10.5	9.1	4	7.3	5.6	27.3	20.1
E-Com Website(2)	10.9	25.8	8.2	17.7	12.7	4.8	31.8	48.3
Inventory/Supply Chain Mgmt.(3)	8.2	7.3	6.4	9.7	9.1	8.9	23.7	25.9
Customer Records(4)	5.5	13.7	11.8	18.5	10.9	15.3	28.2	47.5
HR-Records(5)	6.4	8.9	18.2	8.1	15.5	14.5	40.1	31.5
Critical IT(6)	28.2	16.9	21.8	15.3	8.2	17.7	58.2	49.9
Accounting System(7)	9.1	10.5	10	12.9	20	16.1	39.1	39.5
Product Designs(IP-8)	19.1	4	12.7	4	10.9	10.5	42.7	18.5
Asset Inventory(9)	1.8	2.4	1.8	9.7	5.5	6.5	9.1	18.6

IS Pros (n = 160)	Top IT Risk		Second IT Risk		Third IT Risk			
Top IT Risk	**Defense**	**Furniture**	**Defense**	**Furniture**	**Defense**	**Furniture**	**Defense Top 3**	**Furniture Top 3**
E-mail(1)	17.8	17.2	13.7	6.9	2.7	8	34.2	32.1
E-Com Website(2)	12.3	6.9	11	19.5	16.4	13.8	39.7	40.2
Inventory/Supply Chain Mgmt.(3)	4.1	6.9	5.5	8	12.3	6.9	21.9	21.8
Customer Records(4)	11	6.9	17.8	10.3	8.2	10.3	37	27.5
HR-Records(5)	5.5	5.7	9.6	13.8	9.6	16.1	24.7	35.6
Critical IT(6)	34.2	32.2	13.7	11.5	16.4	14.9	64.3	58.6
Accounting System(7)	9.6	5.7	12.3	16.1	15.1	11.5	37	33.3
Product Designs(IP-8)	4.1	9.2	6.8	6.9	13.7	8	24.6	24.1
Asset Inventory(9)	1.4	9.2	9.6	6.9	5.5	10.3	16.5	26.4

End of Slide Show

- If you happen to see future studies, please take the survey.
- Contact info:
  - aaron.fister@ou.edu
- Twitter
  - https://twitter.com/cyberrisksurvey
- Website
  - https://cyberrisksurvey.org/