

CHIME and AEHIS Cybersecurity Survey

October 2016

Fielding and Responses

Responses: 190

Survey fielded: Approximately a month (8/29-9/30)

Demographics

In what state or U.S. territory do you currently work?

Top 5 States

1. California 11.11%
2. Florida 5.82%
3. Texas 5.82%
4. Pennsylvania 5.29%
5. Ohio 4.76%

Answer Choices	Responses	
Alabama	1.06%	2
Alaska	1.06%	2
American Samoa	0.00%	0
Arizona	3.17%	6
Arkansas	0.53%	1
California	11.11%	21
Colorado	1.06%	2
Connecticut	1.06%	2
Delaware	0.53%	1
District of Columbia (DC)	0.53%	1
Florida	5.82%	11
Georgia	2.65%	5
Guam	0.00%	0
Hawaii	0.00%	0
Idaho	0.53%	1
Illinois	4.23%	8
Indiana	1.59%	3
Iowa	2.65%	5
Kansas	1.59%	3
Kentucky	1.59%	3
Louisiana	0.00%	0
Maine	1.06%	2
Maryland	1.06%	2

Massachusetts	1.59%	3
Michigan	3.70%	7
Minnesota	2.65%	5
Mississippi	0.00%	0
Missouri	2.12%	4
Montana	0.00%	0
Nebraska	1.59%	3
Nevada	0.00%	0
New Hampshire	0.53%	1
New Jersey	3.17%	6
New Mexico	1.59%	3
New York	3.70%	7
North Carolina	3.17%	6
North Dakota	0.00%	0
Northern Marianas Islands	0.00%	0
Ohio	4.76%	9
Oklahoma	1.06%	2
Oregon	2.12%	4
Pennsylvania	5.29%	10
Puerto Rico	0.00%	0
Rhode Island	0.00%	0
South Carolina	0.00%	0
South Dakota	0.00%	0
Tennessee	3.17%	6
Texas	5.82%	11
Utah	2.12%	4
Vermont	1.06%	2
Virginia	0.53%	1
Virgin Islands	0.00%	0
Washington	3.70%	7
West Virginia	1.59%	3
Wisconsin	2.12%	4
Wyoming	0.00%	0

North Carolina	3.17%	6
North Dakota	0.00%	0
Northern Marianas Islands	0.00%	0
Ohio	4.76%	9
Oklahoma	1.06%	2
Oregon	2.12%	4
Pennsylvania	5.29%	10
Puerto Rico	0.00%	0
Rhode Island	0.00%	0
South Carolina	0.00%	0
South Dakota	0.00%	0
Tennessee	3.17%	6
Texas	5.82%	11
Utah	2.12%	4
Vermont	1.06%	2
Virginia	0.53%	1
Virgin Islands	0.00%	0
Washington	3.70%	7
West Virginia	1.59%	3
Wisconsin	2.12%	4
Wyoming	0.00%	0

Answered: 189 Skipped: 2

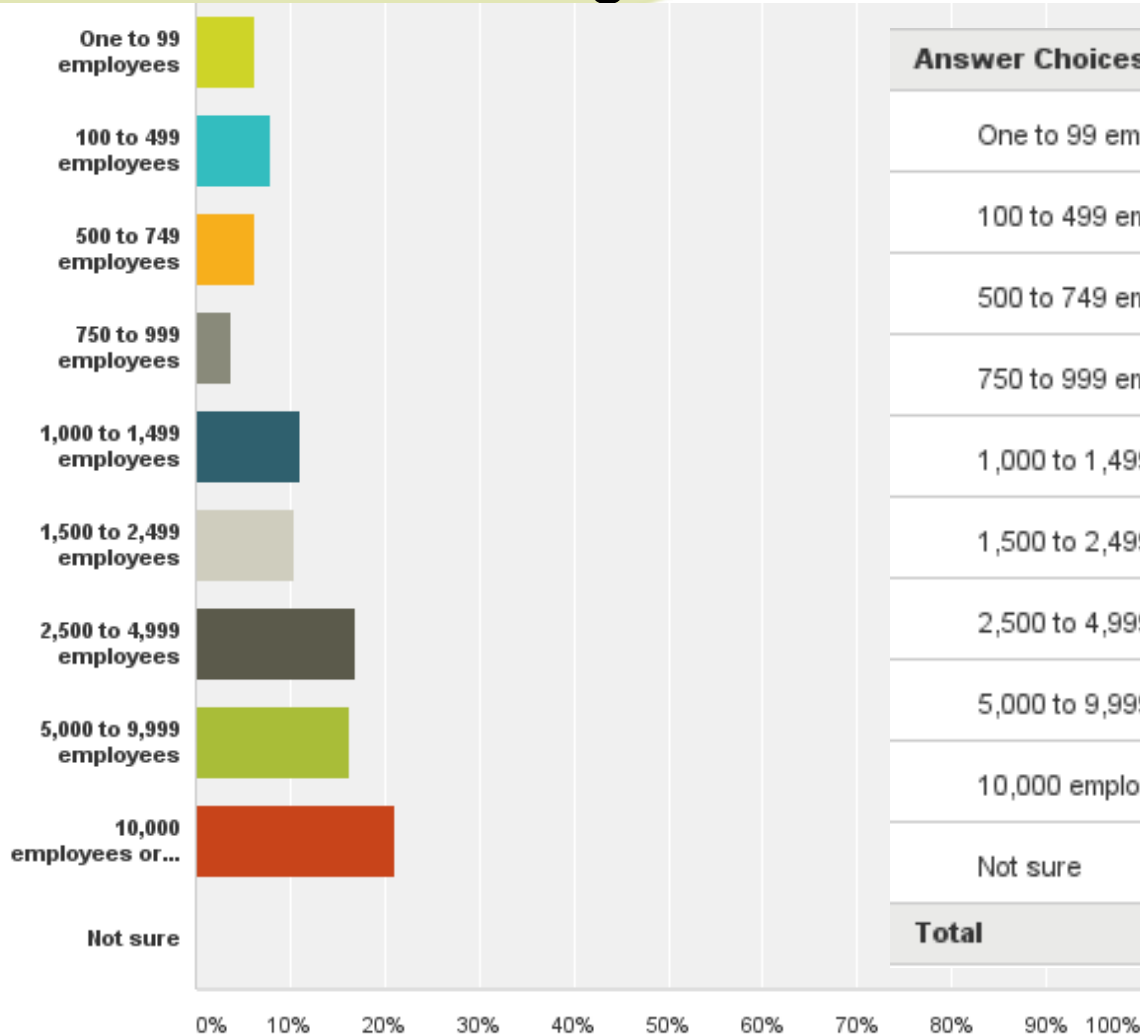
Responses Evaluated by Bed Size

- Less than 100 beds, Other Care Providers w/ Inpatient beds: 36 respondents
- 100 to 399 beds: 48 respondents
- 400 or more beds: 78 respondents
- All respondents: 190

What best describes your organization type?

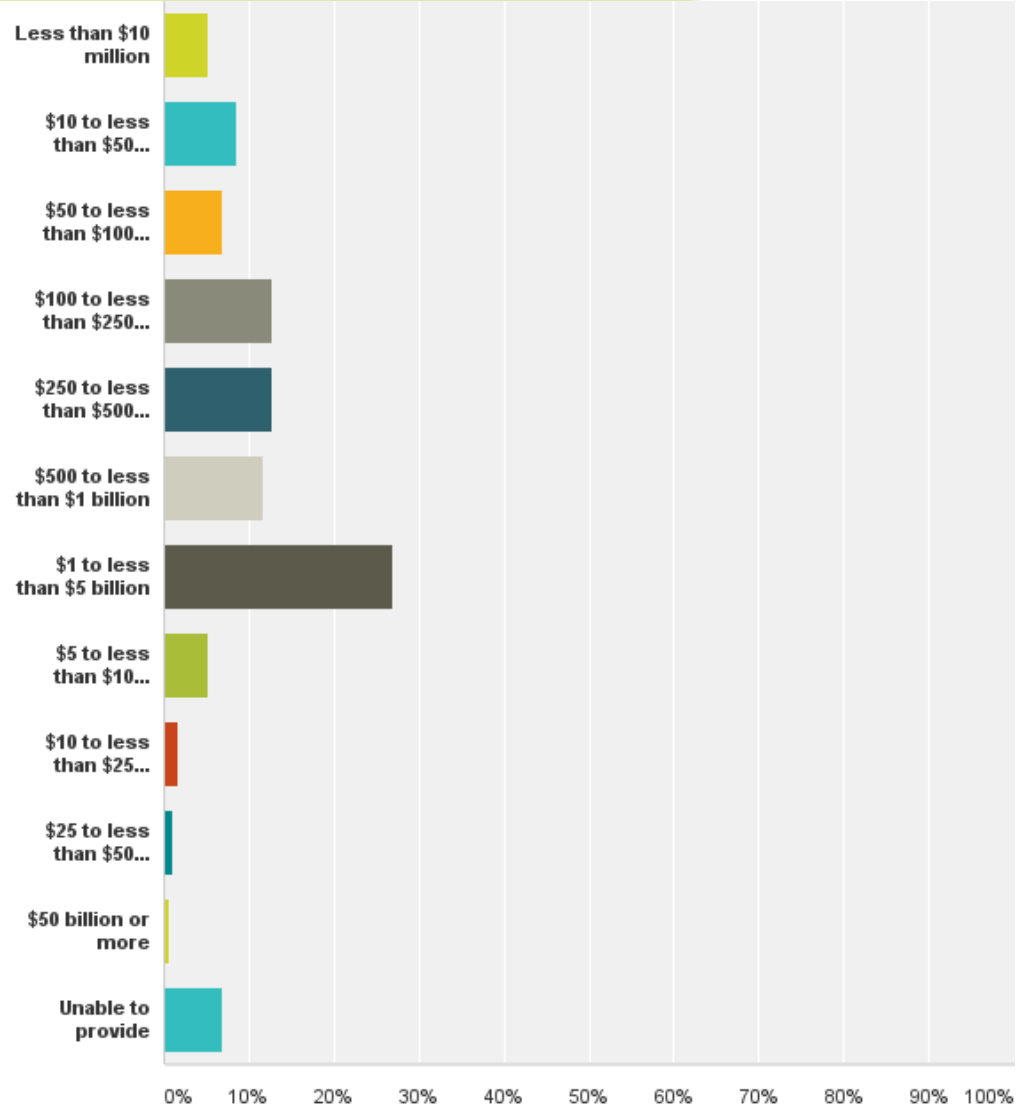
Answer Choices	Responses	
Hospital/Acute Care Facility	35.79%	68
Integrated Delivery Network/System	34.74%	66
Other (please specify)	8.95%	17
Ambulatory Facility/Clinic	3.68%	7
Group Practice/Clinic	3.68%	7
Behavioral Health Care	3.16%	6
Health Insurer/Insurance Organization	3.16%	6
Nursing Home/Long Term Care	2.11%	4
HIE	1.58%	3
MSO	1.05%	2
Rehabilitation	1.05%	2
Home Health Care	0.53%	1
Hospice	0.53%	1
Lab Services	0.00%	0
Managed Care	0.00%	0
Surgical Center	0.00%	0
Total		190

What is the total number of employees across your entire organization, including all of its branches, divisions, and subsidiaries?



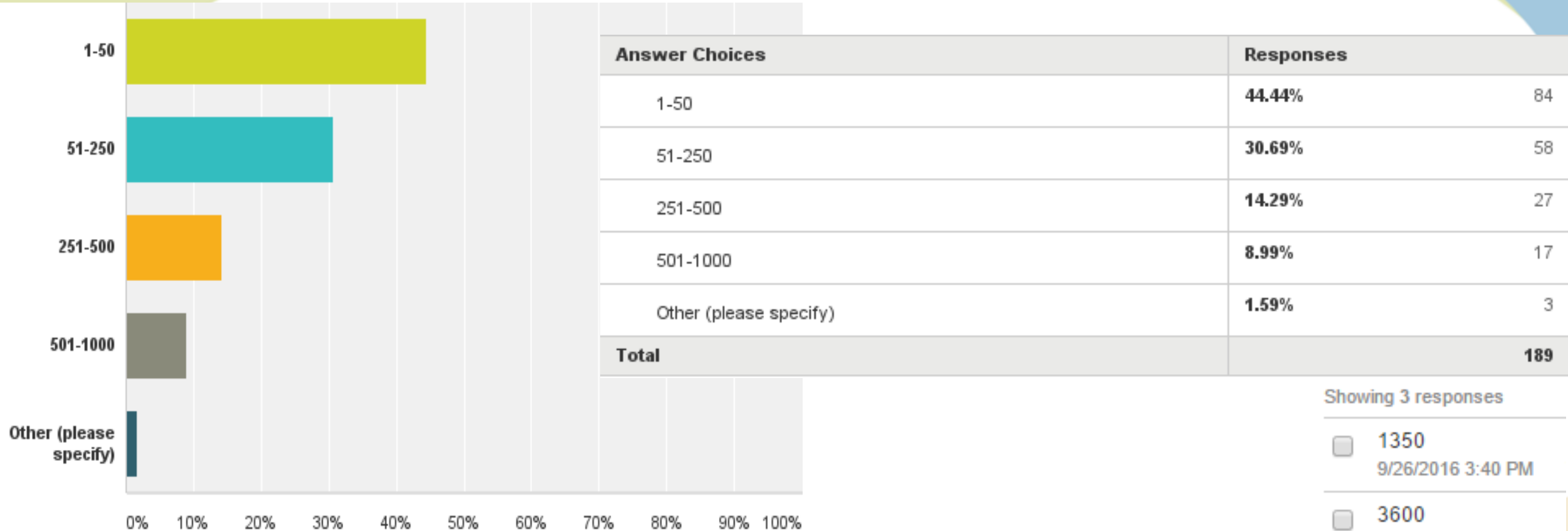
Answer Choices	Responses
One to 99 employees	6.32% 12
100 to 499 employees	7.89% 15
500 to 749 employees	6.32% 12
750 to 999 employees	3.68% 7
1,000 to 1,499 employees	11.05% 21
1,500 to 2,499 employees	10.53% 20
2,500 to 4,999 employees	16.84% 32
5,000 to 9,999 employees	16.32% 31
10,000 employees or more	21.05% 40
Not sure	0.00% 0
Total	190

What is your organization's annual revenue?



Answer Choices	Responses	Count
Less than \$10 million	5.29%	10
\$10 to less than \$50 million	8.47%	16
\$50 to less than \$100 million	6.88%	13
\$100 to less than \$250 million	12.70%	24
\$250 to less than \$500 million	12.70%	24
\$500 to less than \$1 billion	11.64%	22
\$1 to less than \$5 billion	26.98%	51
\$5 to less than \$10 billion	5.29%	10
\$10 to less than \$25 billion	1.59%	3
\$25 to less than \$50 billion	1.06%	2
\$50 billion or more	0.53%	1
Unable to provide	6.88%	13
Total		189

What is your total number of IT staff?



Showing 3 responses

- 1350
9/26/2016 3:40 PM
- 3600
8/31/2016 10:16 PM
- > 1000
8/30/2016 2:24 PM

Responses on Threats and Vulnerabilities

Q 8. Thinking about your own organization, please rate the following potential security threats on the degree of concern you have for each.

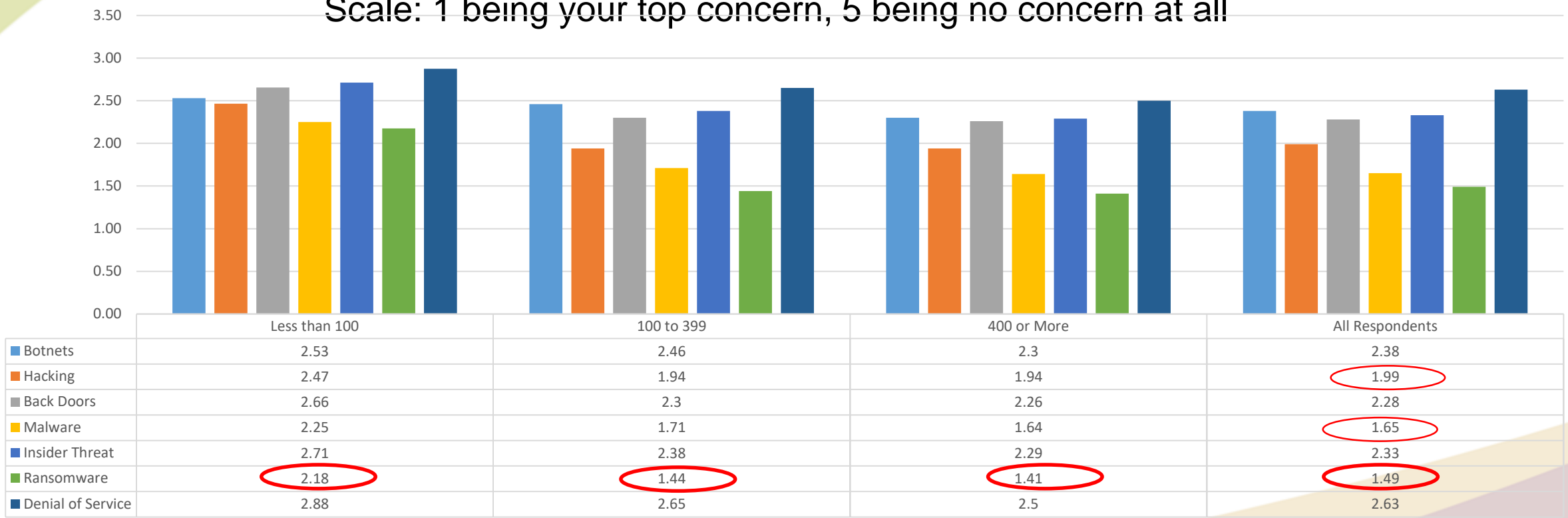
Scale: 1 being your top concern, 5 being no concern at all

Threats



Q 9. Thinking about your own organization, please rate the following potential security exploits on the degree of concern you have for each.

Scale: 1 being your top concern, 5 being no concern at all

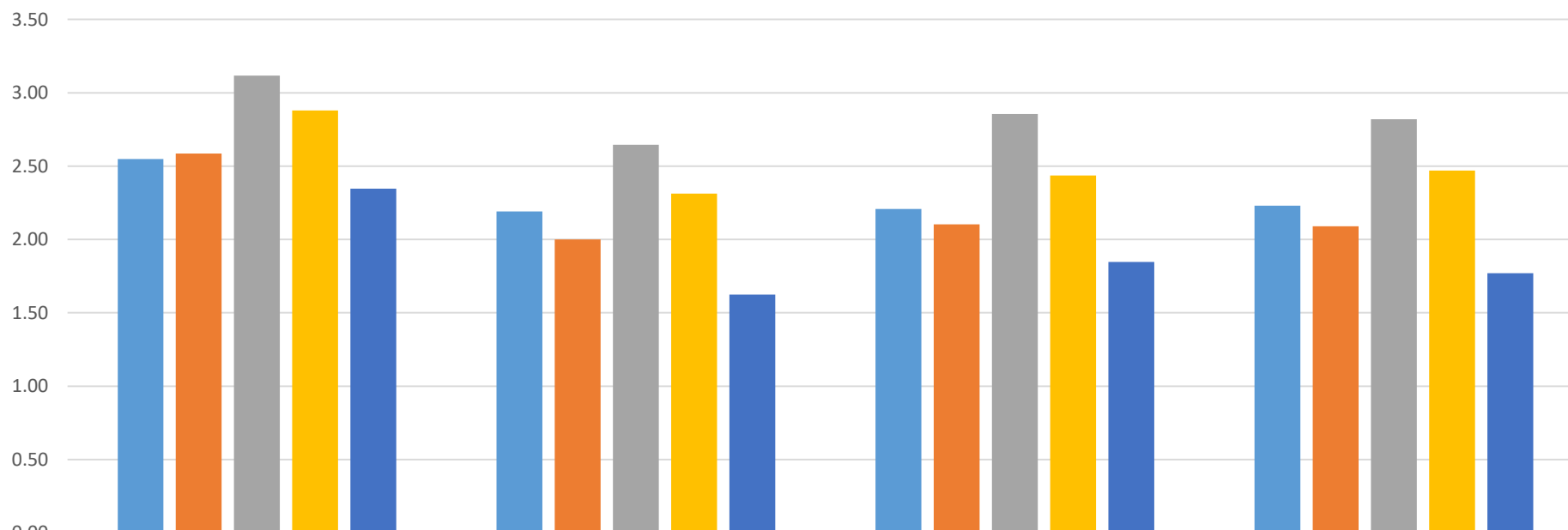


■ Botnets ■ Hacking ■ Back Doors ■ Malware ■ Insider Threat ■ Ransomware ■ Denial of Service

Q 10. Thinking about your own organization, please rate the following potential security vulnerabilities on the degree of concern you have for each.

Scale: 1 being your top concern, 5 being no concern at all

Vulnerabilities

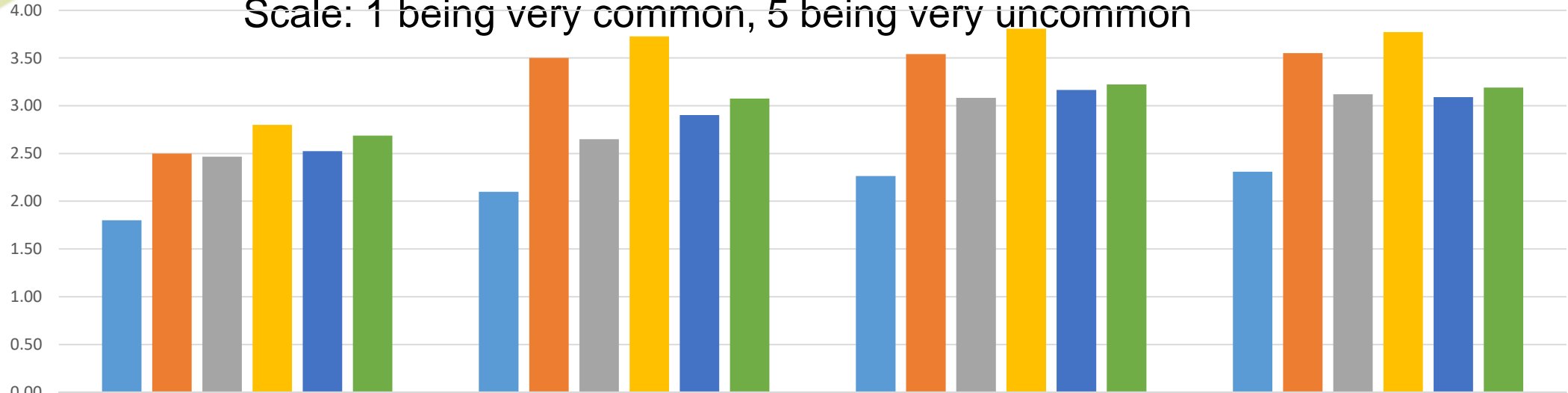


	Less than 100 beds	100 to 399 beds	400 or more beds	All Respondents
Poor Authentication & Session Management	2.55	2.19	2.21	2.23
Security Misconfiguration	2.59	2.00	2.10	2.09
Buffer Overflows	3.12	2.65	2.86	2.82
Injection Vulnerabilities	2.88	2.31	2.44	2.47
Data Exposure	2.35	1.63	1.85	1.77

■ Poor Authentication & Session Management
 ■ Security Misconfiguration
 ■ Buffer Overflows
 ■ Injection Vulnerabilities
 ■ Data Exposure

Q 11. Please indicate how common each of the security threats listed below are for your organization

Scale: 1 being very common, 5 being very uncommon

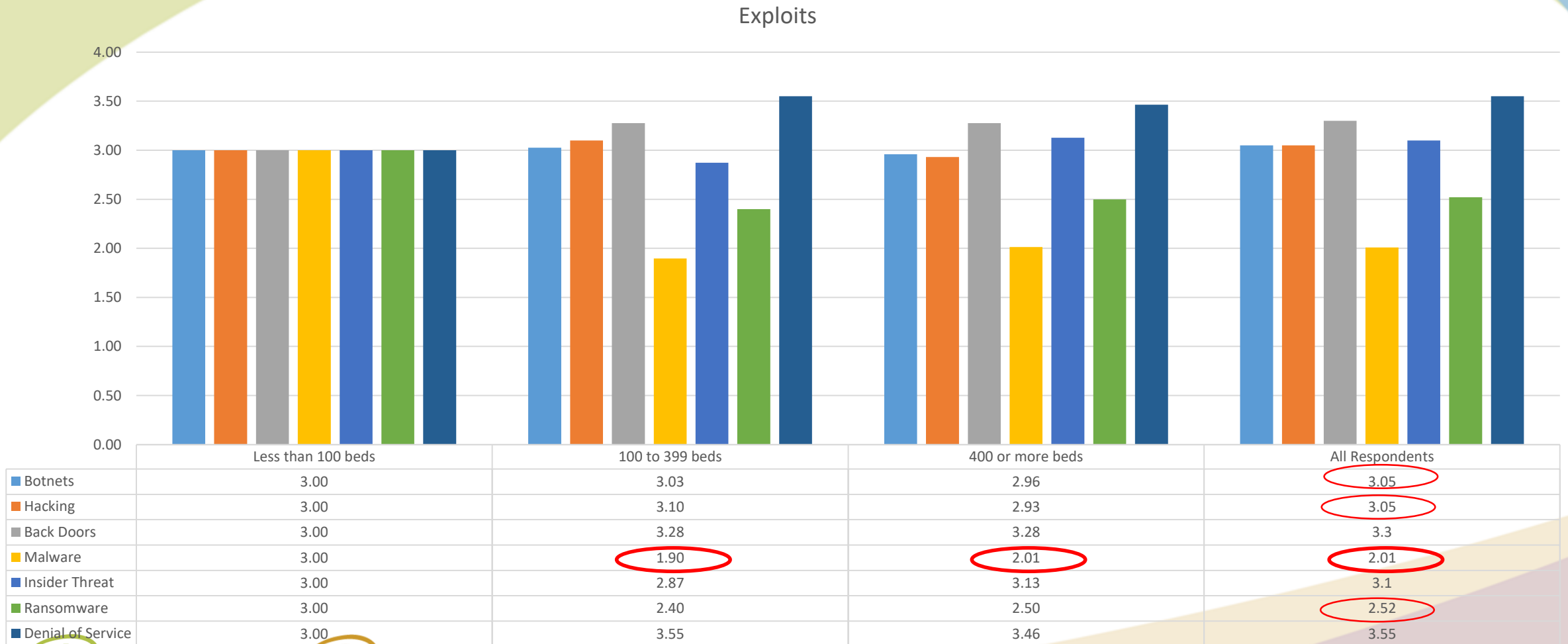


	Less than 100 Beds	100 to 399 beds	400 or more beds	All Respondents
Social Engineering	1.80	2.10	2.26	2.31
Cyber Terrorism	2.50	3.50	3.54	3.55
IoT	2.47	2.65	3.08	3.12
Organized Crime	2.80	3.73	3.81	3.77
Insider Threat	2.52	2.90	3.16	3.09
Data Theft	2.69	3.08	3.22	3.19

■ Social Engineering ■ Cyber Terrorism ■ IoT ■ Organized Crime ■ Insider Threat ■ Data Theft

Q 12. Please indicate how common each of the security exploits listed below are for your organization

Scale: 1 being very common, 5 being very uncommon



Q 13. Please indicate how common each of the security vulnerabilities listed below are for your organization

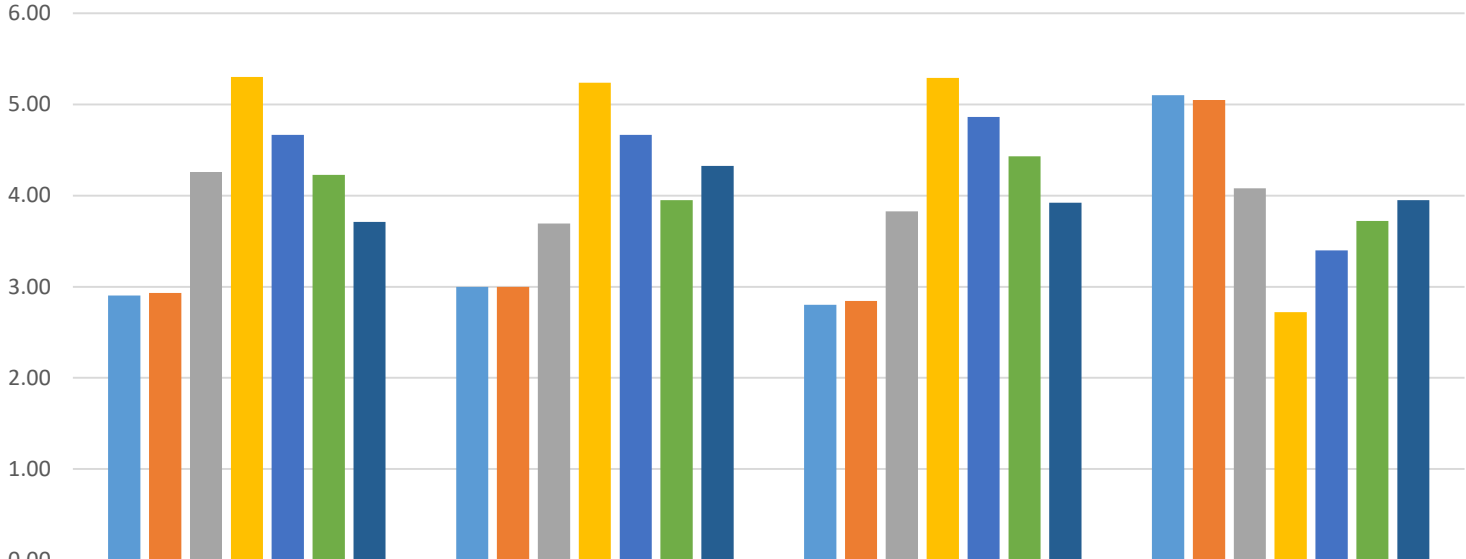
Scale: 1 being very common, 5 being very uncommon



Q 14. Please rank: In your opinion, why does the business strategy not drive the security strategy?

1 = Top Reason, 7 = Very Little Reason

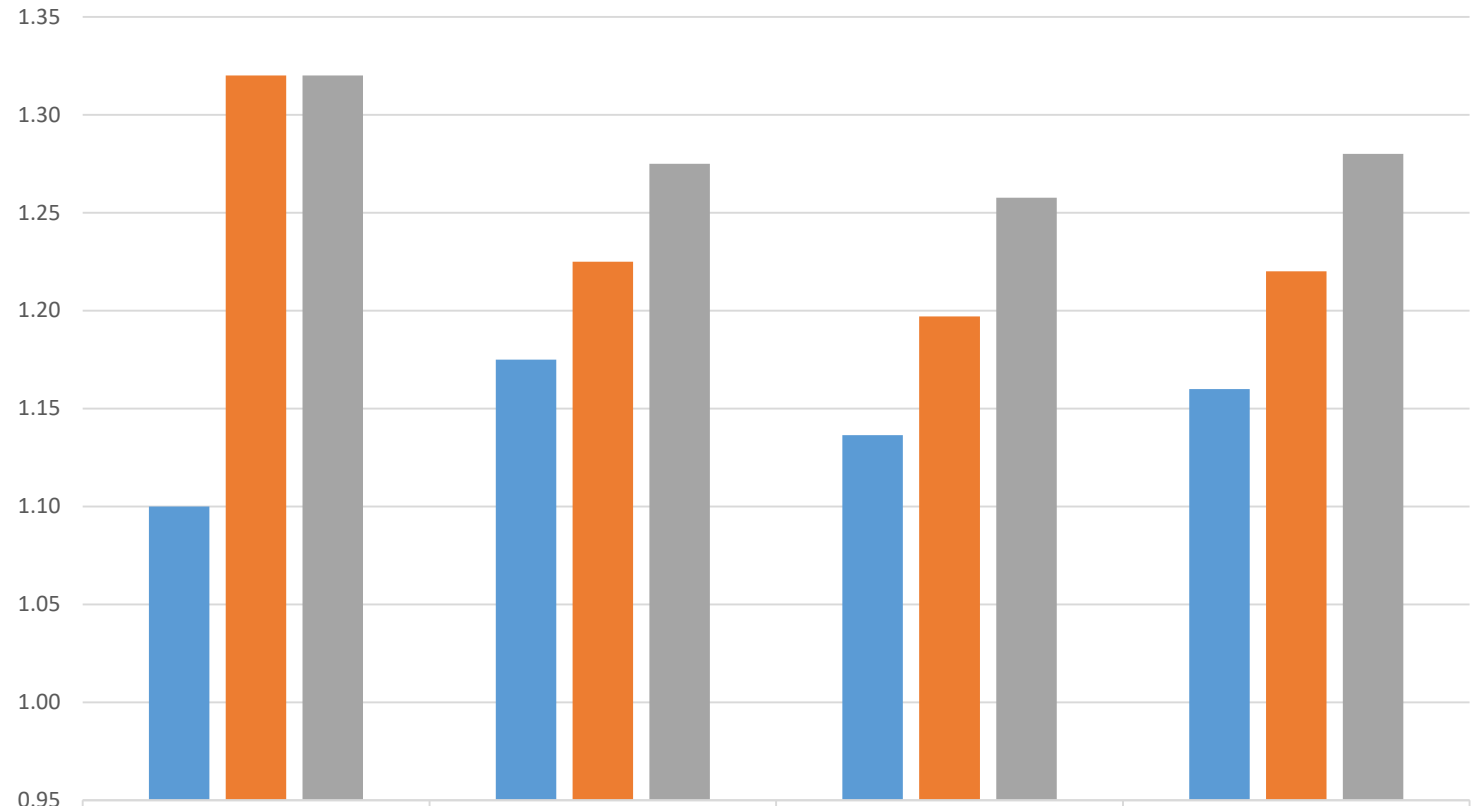
Business Strategy vs. Security Strategy



	Less than 100 beds	100 to 399 beds	400 or more beds	All Respondents
Budgets or Staffing	2.90	3.00	2.80	5.1
Pace of change for the business (Too Many other Initiatives)	2.93	3.00	2.84	5.05
Security is not considered a patient care or quality of care issue	4.26	3.69	3.83	4.08
BYOD/BYOA	5.30	5.24	5.29	2.72
Regulatory Landscape is too complex	4.67	4.67	4.86	3.4
Threat landscape changes too quickly	4.23	3.95	4.43	3.72
Changing delivery of care models and workflows don't address security until after the fact	3.71	4.33	3.92	3.95

Q 15. Compared to a year ago, please indicate how your organization would perform if its systems or data were compromised by a targeted attack?
 Scale: 1 = Better, 3= Worse

Organization's Performance vs. One Year Ago

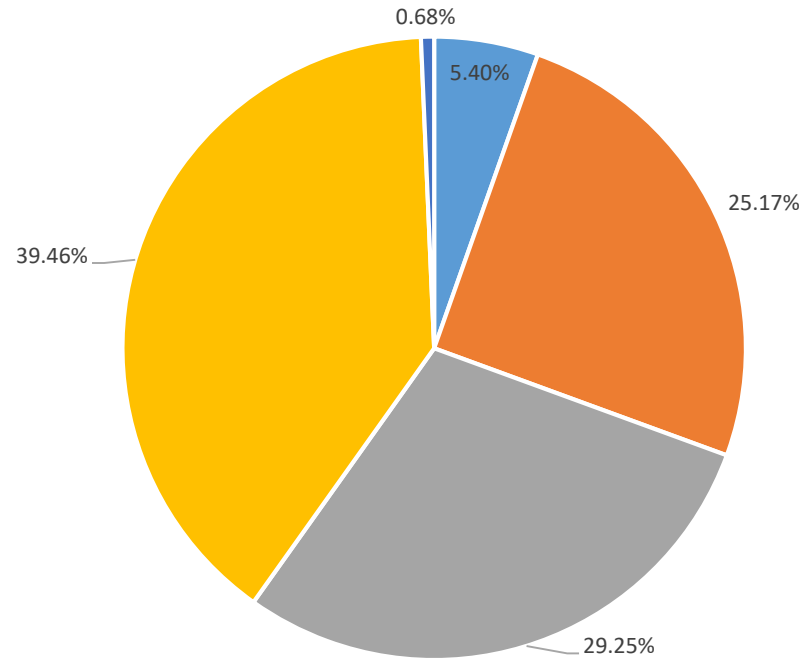


	Less than 100 beds	100 to 399 beds	400 or more beds	All Respondents
Having systems in place to prepare for a security incident	1.10	1.18	1.14	1.16
Discovering a security incident	1.32	1.23	1.20	1.22
Recovering from a security incident	1.32	1.28	1.26	1.28

■ Having systems in place to prepare for a security incident ■ Discovering a security incident ■ Recovering from a security incident

Q 16. How confident are you that Federal legislators understand the importance of security enough to support your key information security initiatives?

Confidence in Federal Legislators to Understand Security Initiatives

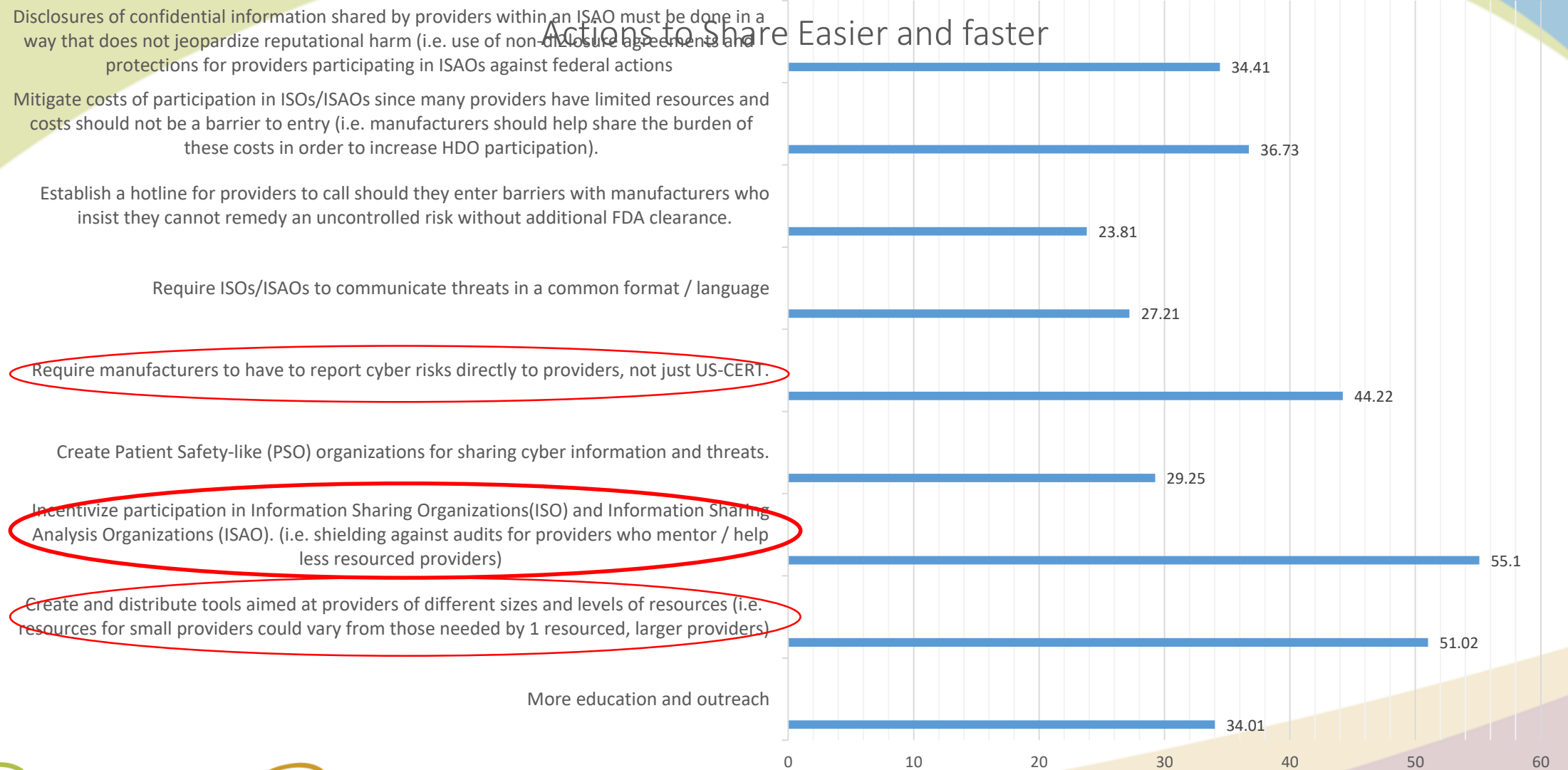


- Very Confident
- Somewhat Confident
- Neither Confident nor Unconfident
- Don't know
- Not Confident at All

Q 17. What do you think the Federal Government could do to help you share cybersecurity information more easily and faster? Pick your top 3.

Percentage of overall respondents.

Actions to Share Easier and faster



Q 17. What do you think the Federal Government could do to help you share cybersecurity information more easily and faster? Pick your top 3.

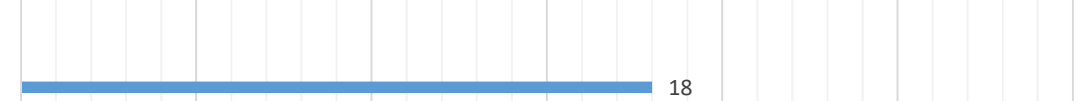
100 or less beds

Actions to Share Easier and faster

Disclosures of confidential information shared by providers within an ISAO must be done in a way that does not jeopardize reputational harm (i.e. use of non-disclosure agreements and protections for providers participating in ISAOs against federal actions)



Mitigate costs of participation in ISOs/ISAOs since many providers have limited resources and costs should not be a barrier to entry (i.e. manufacturers should help share the burden of these costs in order to increase HDO participation).



Establish a hotline for providers to call should they enter barriers with manufacturers who insist they cannot remedy an uncontrolled risk without additional FDA clearance.



Require ISOs/ISAOs to communicate threats in a common format / language



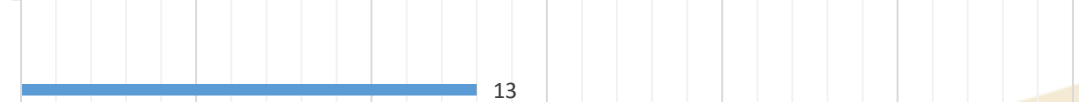
Require manufacturers to have to report cyber risks directly to providers, not just US-CERT.



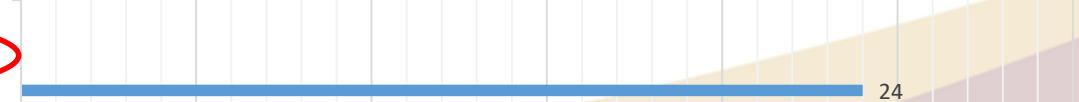
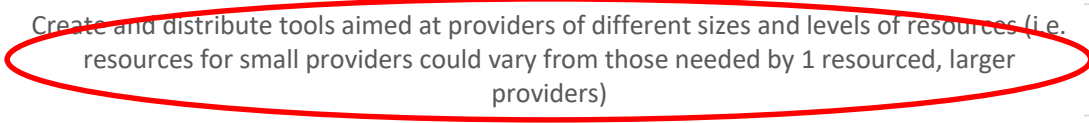
Create Patient Safety-like (PSO) organizations for sharing cyber information and threats.



Incentivize participation in Information Sharing Organizations(ISO) and Information Sharing Analysis Organizations (ISAO). (i.e. shielding against audits for providers who mentor / help less resourced providers)



Create and distribute tools aimed at providers of different sizes and levels of resources (i.e. resources for small providers could vary from those needed by 1 resourced, larger providers)



More education and outreach



0.00 5.00 10.00 15.00 20.00 25.00 30.00

Q 17. What do you think the Federal Government could do to help you share cybersecurity information more easily and faster?

Pick your top 3.

100 to 399 beds

Actions to Share Easier and faster

Disclosures of confidential information shared by providers within an ISAO must be done in a way that does not jeopardize reputational harm (i.e. use of non-disclosure agreements and protections for providers participating in ISAOs against federal actions)

Mitigate costs of participation in ISOs/ISAOs since many providers have limited resources and costs should not be a barrier to entry (i.e. manufacturers should help share the burden of these costs in order to increase HDO participation).

Establish a hotline for providers to call should they enter barriers with manufacturers who insist they cannot remedy an uncontrolled risk without additional FDA clearance.

Require ISOs/ISAOs to communicate threats in a common format / language

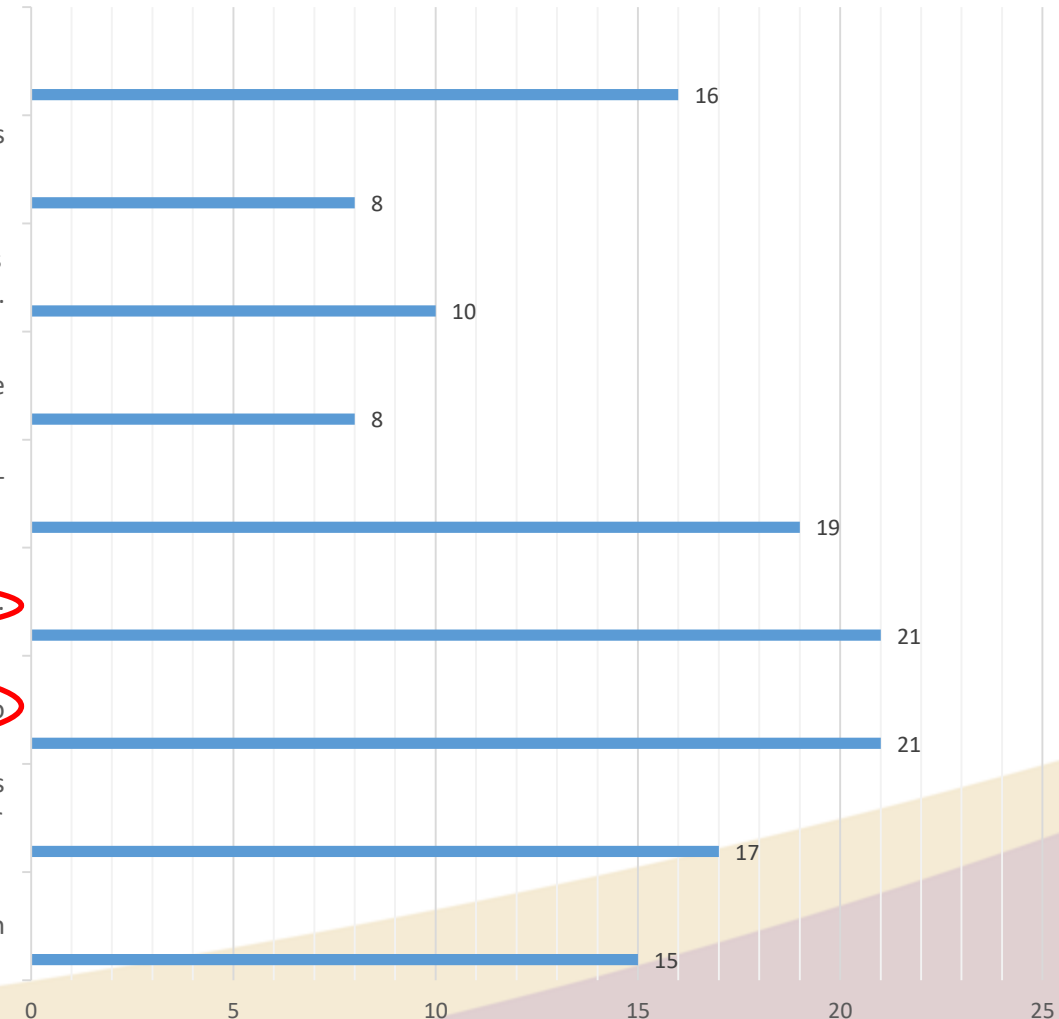
Require manufacturers to have to report cyber risks directly to providers, not just US-CERT.

Create Patient Safety-like (PSO) organizations for sharing cyber information and threats.

Incentivize participation in Information Sharing Organizations (ISO) and Information Sharing Analysis Organizations (ISAO). (i.e. shielding against audits for providers who mentor / help less resourced providers)

Create and distribute tools aimed at providers of different sizes and levels of resources (i.e. resources for small providers could vary from those needed by 1 resourced, larger providers)

More education and outreach



Q 17. What do you think the Federal Government could do to help you share cybersecurity information more easily and faster?

Pick your top 3.
400 or more beds

Actions to Share Easier and faster

Disclosures of confidential information shared by providers within an ISAO must be done in a way that does not jeopardize reputational harm (i.e. use of non-disclosure agreements and protections for providers participating in ISAOs against federal actions)

Mitigate costs of participation in ISOs/ISAOs since many providers have limited resources and costs should not be a barrier to entry (i.e. manufacturers should help share the burden of these costs in order to increase HDO participation).

Establish a hotline for providers to call should they enter barriers with manufacturers who insist they cannot remedy an uncontrolled risk without additional FDA clearance.

Require ISOs/ISAOs to communicate threats in a common format / language

Require manufacturers to have to report cyber risks directly to providers, not just US-CERT.

Create Patient Safety-like (PSO) organizations for sharing cyber information and threats.

Incentivize participation in Information Sharing Organizations (ISO) and Information Sharing Analysis Organizations (ISAO). (i.e. shielding against audits for providers who mentor / help less resourced providers)

Create and distribute tools aimed at providers of different sizes and levels of resources (i.e. resources for small providers could vary from those needed by 1 resourced, larger providers)

More education and outreach

