

December 19, 2022

*Via Electronic Submission*

Ms. Vanessa A. Countryman  
Secretary  
U.S. Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549-1090

**Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (SEC Rel. Nos. 33-11028; 34-94197; IA-5956; IC-34497; File No. S7-04-22)**

Dear Ms. Countryman:

The Investment Adviser Association (IAA)<sup>1</sup> is writing to supplement our previous comments<sup>2</sup> on the Commission’s proposal that would require investment advisers to adopt and implement written cybersecurity policies and procedures with specified elements, report significant adviser cybersecurity incidents to the Commission, disclose significant adviser cybersecurity risks and incidents to clients, and maintain related books and records.<sup>3</sup> We appreciate the constructive discussions that we have had with Commission staff regarding our Prior Letter and the Proposal’s potential implications for investment advisers.

The IAA believes that the Commission has severely underestimated the quantifiable costs of the Proposal.<sup>4</sup> Following our Prior Letter, and in response to questions raised by staff, the IAA surveyed our members to better determine the Proposal’s impact. The Survey consisted of 10

---

<sup>1</sup> The IAA is the leading organization dedicated to advancing the interests of investment advisers. For more than 85 years, the IAA has been advocating for advisers before Congress and U.S. and global regulators, promoting best practices and providing education and resources to empower advisers to effectively serve their clients, the capital markets, and the U.S. economy. The IAA’s member firms manage more than \$35 trillion in assets for a wide variety of individual and institutional clients, including pension plans, trusts, mutual funds, private funds, endowments, foundations, and corporations. For more information, please visit [www.investmentadviser.org](http://www.investmentadviser.org).

<sup>2</sup> See Letter from Gail C. Bernstein, General Counsel, Investment Adviser Association, to the Commission re: *Cybersecurity Risk Management for Investment Advisers* (Apr. 11, 2022), available at <https://investmentadviser.org/wp-content/uploads/2022/04/IAA-Cybersecurity-Comment-Letter-4.11.22-FINAL.pdf?t=62549ef4aa4dd> (Prior Letter).

<sup>3</sup> *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, 87 Fed. Reg. 13524 (Mar. 9, 2022), available at <https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf> (Proposal).

<sup>4</sup> As we noted in our Prior Letter, we are concerned with the statement in the Proposal that “[a]s we do not currently have reliable data on the extent to which registrants’ existing policies and procedures follow industry best practices, address cybersecurity risks, their ‘reasonableness,’ or the frequency at which they are reviewed, it is not possible for us to quantify the scale of the benefits arising from the proposed requirements.” Proposal at 13551. Without having an appropriate baseline, it is difficult to accurately measure the additional incremental costs.

questions requesting input on several issues, including members' current cybersecurity program costs and cost estimates for implementing the various requirements of the Proposal. We have included the Survey Report as an appendix to this letter.<sup>5</sup>

The IAA received responses from 34 members. These members range from smaller advisers with less than \$500 million in regulatory assets under management (RAUM) and/or fewer than 10 employees to very large firms with over \$1 trillion RAUM and/or more than 1,000 employees. The Survey Report provides responses by both RAUM and employee count. As noted in our Prior Letter, the IAA has long urged the Commission to consider other factors in addition to RAUM (e.g., number of employees) to make a more realistic assessment of the impact of rules on smaller advisers that by their nature have limited staffing.<sup>6</sup>

Below are some key highlights from the Survey:

- The Commission's assumption that firms spend only 0.5% of their revenues on cybersecurity likely significantly underestimates what firms are currently spending. The Survey reflects that:
  - Almost 80% of respondents measured by number of employees and by RAUM currently spend at least 1% of their total revenue on cybersecurity.<sup>7</sup>
  - Approximately 53% of respondents measured by number of employees and by RAUM spent more than \$500,000 on cybersecurity-related costs in 2021.<sup>8</sup>
- The Survey shows that all advisers currently rely heavily on third-party service providers to provide cybersecurity services and we expect that this reflects industry practice.<sup>9</sup> The Commission should acknowledge the need for third-party expertise in this area, and the associated costs, and take this into consideration when finalizing the Proposal, especially as it considers the

---

<sup>5</sup> See Appendix (Survey Report).

<sup>6</sup> See also, e.g., Letter from Karen Barr to SEC Chair Gary Gensler on the Regulation of Registered Investment Advisers (May 17, 2021), available at <https://www.investmentadviser.org/publications/comment-letters/comment-letter-may-17-2021> ("Smaller advisory firms face unique challenges as small businesses. The IAA recommends that the Commission consider the economic impact of regulations on smaller advisory firms more carefully and conduct a more realistic assessment of the cumulative impact of policy and regulatory decisions on these firms' businesses and their ability to serve the investing public.").

<sup>7</sup> Survey Report, Q3.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.* Q6.

impact of the Proposal and the incremental and cumulative impacts of all regulatory requirements on smaller advisers.

- A majority of smaller firms (up to \$10 billion RAUM) estimate that they will spend over \$50,000 in 2022 for external cybersecurity products and services and 37% estimate that they will spend over \$100,000.<sup>10</sup>
- Mid-sized firms (between \$10 billion and \$50 billion RAUM) estimate that they will spend over \$400,000 in 2022 for external cybersecurity products and services.<sup>11</sup>
- Larger firms (between \$50 billion and \$1 trillion RAUM) estimate that they will spend over \$2,000,000 in 2022 for external cybersecurity products and services.<sup>12</sup>
- Two of the three largest firms (more than \$1 trillion RAUM) estimate that they will spend over \$80,000,000 in 2022 for external cybersecurity products and services.<sup>13</sup>
- The Survey reflects that the costs associated with implementing the Proposal will likely be much higher than the Commission's Paperwork Reduction Act (**PRA**) cost estimates. For example:
  - The Commission estimates that firms will have an annual burden of \$16,013 to implement policies and procedures required by the Proposal.<sup>14</sup> The Survey shows that nearly 80% of respondents estimate that the initial costs associated with adopting and implementing the proposed cybersecurity policies and procedures will be at least \$20,000 per adviser, with nearly 50% estimating that these initial costs will be \$100,000 or more.<sup>15</sup> We are also concerned with the ongoing year-over-year impact as nearly 50% of respondents also estimate annual

---

<sup>10</sup> *Id.* Q5 (Up to \$10B RAUM).

<sup>11</sup> *Id.* Q5 (Between \$10B and \$50B RAUM).

<sup>12</sup> *Id.* Q5 (Between \$50B and \$1T RAUM).

<sup>13</sup> *Id.* Q5 (Over \$1T RAUM).

<sup>14</sup> *See* Proposal at 13560, Table 1—Rule 206(4)–9 PRA Estimates. The estimated total new annual burden per adviser of proposed Rule 206(4)–9 is \$12,541 (internal time costs) plus \$3,472 (external cost burden), for a total of \$16,013.

<sup>15</sup> *Id.* Q7.1.

ongoing costs of more than \$100,000.<sup>16</sup> Over a five-year period, this could underestimate the cost by at least \$420,000 per adviser.

- The Commission estimates that firms will have an annual burden of \$340 to implement the recordkeeping obligations required by the Proposal.<sup>17</sup> The Survey shows that 44% of respondents estimate that both the initial and ongoing per-adviser costs will be at least \$10,000.<sup>18</sup>
- The Commission estimates that firms will have an annual burden of \$3,439 to implement the new requirement to report a significant cybersecurity incident.<sup>19</sup> The Survey shows that over 60% of respondents estimate that both initial and ongoing annual per-adviser costs will be at least \$10,000, with 40% estimating that the ongoing annual costs will exceed \$20,000.<sup>20</sup> Over a five-year period, this could underestimate the per-adviser cost by at least \$32,000.
- The Commission estimates that firms will have an annual burden of \$1,598 to implement the new requirement to disclose information on Form ADV Part 2A regarding an adviser's cybersecurity risks and significant cybersecurity incidents that have occurred in the past two years and an annual burden of \$12,919 to implement the requirement that an adviser deliver interim brochure amendments promptly to existing clients if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident.<sup>21</sup> The Survey shows that 66% of respondents estimate that initial per-adviser costs will be at least \$10,000, with 45% estimating that initial costs will be at least

---

<sup>16</sup> *Id.* Q7.2.

<sup>17</sup> See Proposal at 13562-63, Table 3—Rule 204-2 PRA Estimates. The estimated total annual burden per adviser of each of the five aspects of proposed Rule 204-2 is \$68, for a total of \$340. The five aspects are (i) retention of cybersecurity policies and procedures; (ii) retention of written report documenting annual review; (iii) retention of copy of any Form ADV-C filed in last five years; (iv) retention of records documenting a cybersecurity incident; and (v) retention of records documenting an adviser's cybersecurity risk assessment.

<sup>18</sup> Survey Report Q10.1 and Q10.2.

<sup>19</sup> See Proposal at 13563, Table 4—Rule 204-6 PRA Estimates. The estimates for making a determination of significant cybersecurity incident are \$1,059 (internal time costs) plus \$1,488 (external cost burden), plus the estimates for amending Form ADV-C if any of the information previously filed becomes materially inaccurate are \$396 (internal time costs) plus \$496 (external cost burden), for a total of \$3,439.

<sup>20</sup> Survey Report Q9.1 and Q9.2.

<sup>21</sup> See Proposal at 13568, Table 7—Rule 204-3 PRA Estimates. The estimated total new annual burden per adviser is \$12,919.04. See also Proposal at 13566, Table 6—Form ADV PRA Estimates. The estimated revised burden/external cost per adviser is \$1,598.03.

\$50,000.<sup>22</sup> We are also concerned with the ongoing year-over-year impact as 37% of respondents also estimate annual ongoing per-adviser costs of more than \$20,000.<sup>23</sup> Over a five-year period, this could underestimate the per-adviser costs by at least \$40,000.

- Due to the initial and ongoing annual estimated costs reported by respondents to the Survey, the Commission may be underestimating the per-adviser costs to implement the Proposal over a five-year period by over \$500,000 per adviser.

The Survey shows much higher per-adviser costs for IAA members that responded than estimated by the Commission. It also reflects a wide range of estimated per-adviser costs to implement the Proposal, a variation that underscores the IAA's view that there is no "one-size-fits-all" approach to cybersecurity among investment advisers, and reinforces our recommendation that the Commission continue to allow investment advisers to tailor their cybersecurity program to their business model.<sup>24</sup> The IAA requests that the Commission update its cost-benefit analysis to incorporate this data and that it modify the Proposal to reflect these more significant burdens on advisers.

\* \* \*

We appreciate the Commission's consideration of our supplemental comments on this important Proposal. Please do not hesitate to contact the undersigned at (202) 293-4222 if we can be of further assistance.

Respectfully Submitted,

/s/ Gail C. Bernstein

Gail C. Bernstein  
General Counsel

cc: The Honorable Gary Gensler, Chair  
The Honorable Hester M. Peirce, Commissioner  
The Honorable Caroline A. Crenshaw, Commissioner  
The Honorable Mark T. Uyeda, Commissioner  
The Honorable Jaime Lizárraga, Commissioner  
William A. Birdthistle, Director, Division of Investment Management

---

<sup>22</sup> Survey Report Q8.1.

<sup>23</sup> *Id.* Q8.2.

<sup>24</sup> *See* Prior Letter at 6.

# Appendix



INVESTMENT ADVISER

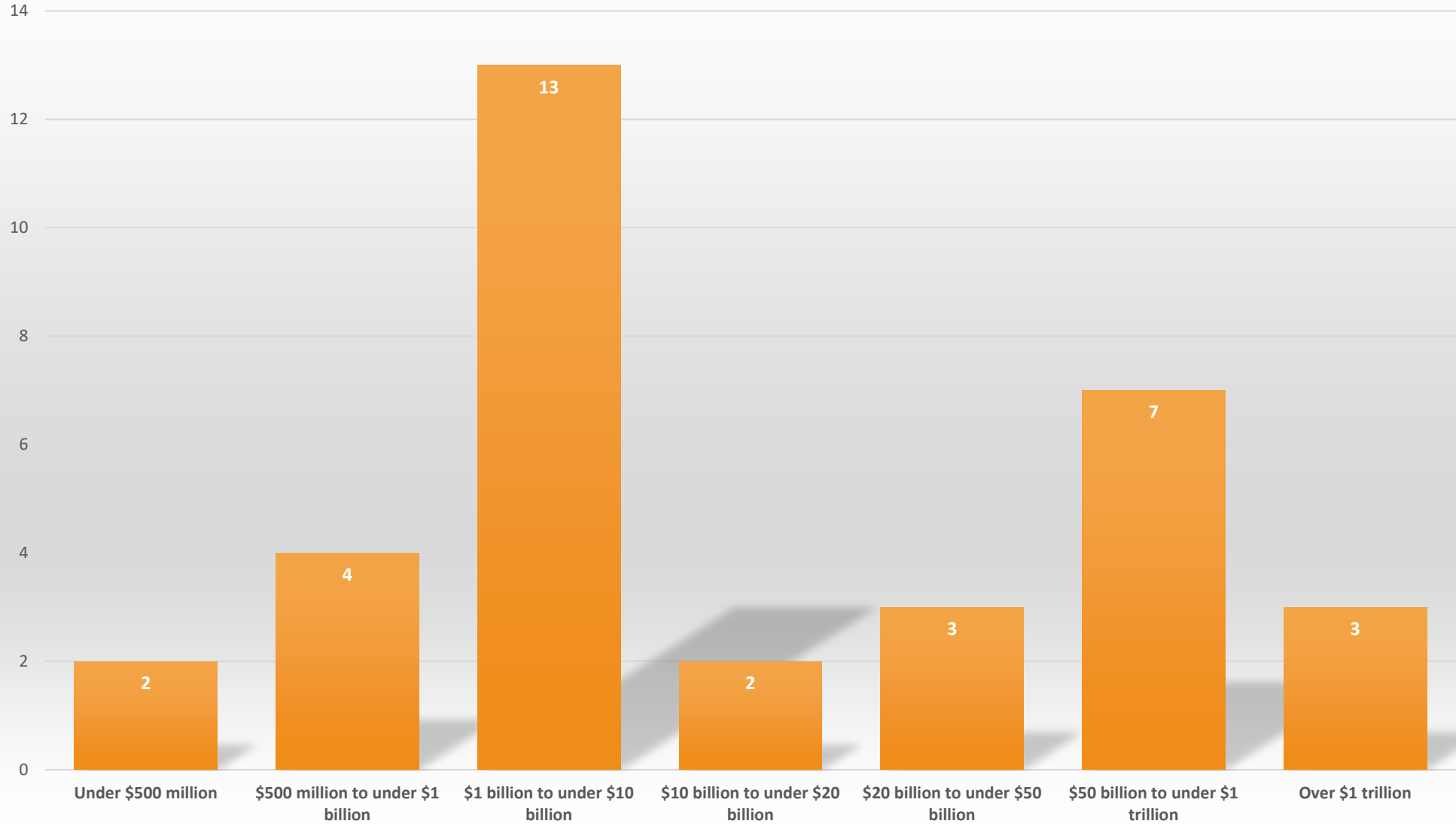
---

A S S O C I A T I O N

*Cybersecurity Survey Results*

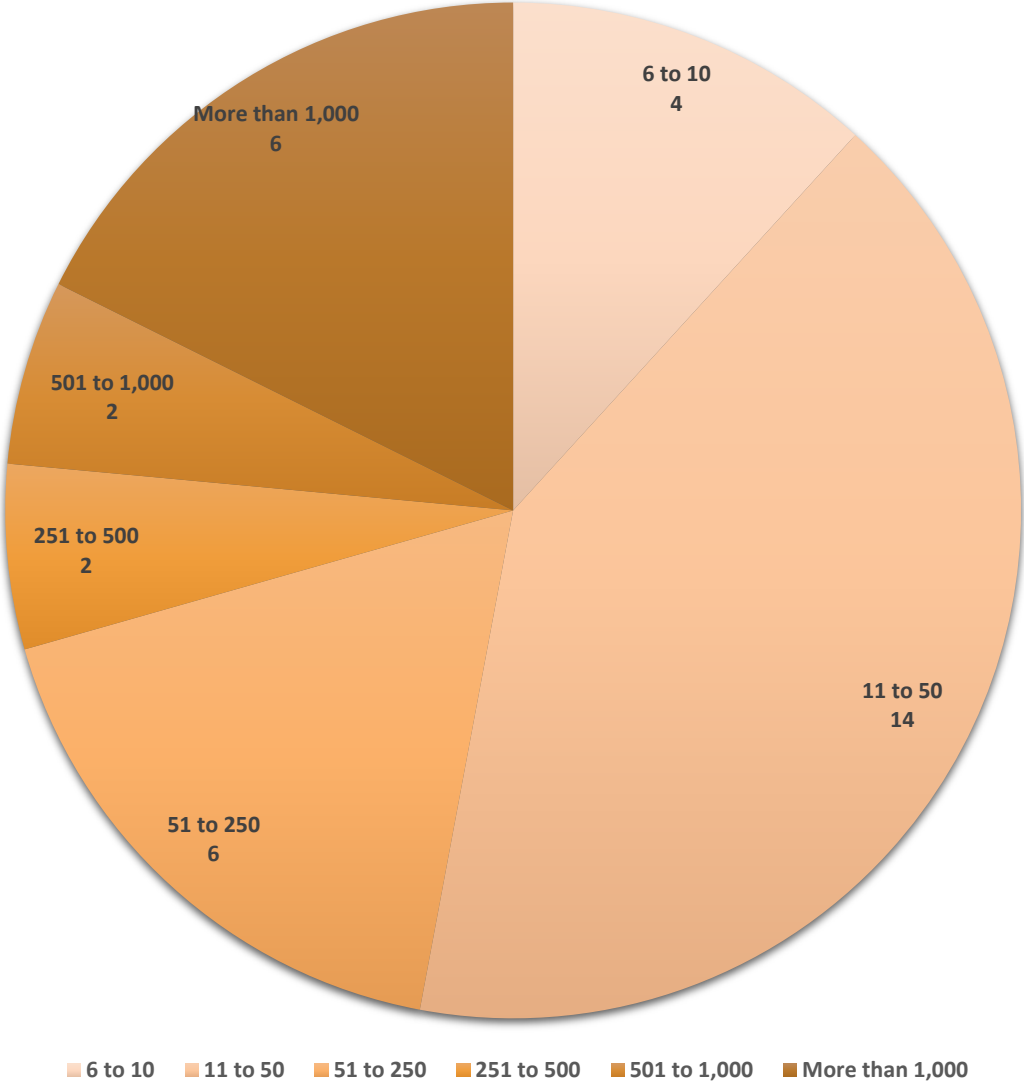
*December 2022*

**Q1. What is your firm's total RAUM (regulatory assets under management)?  
(34 Responses)**

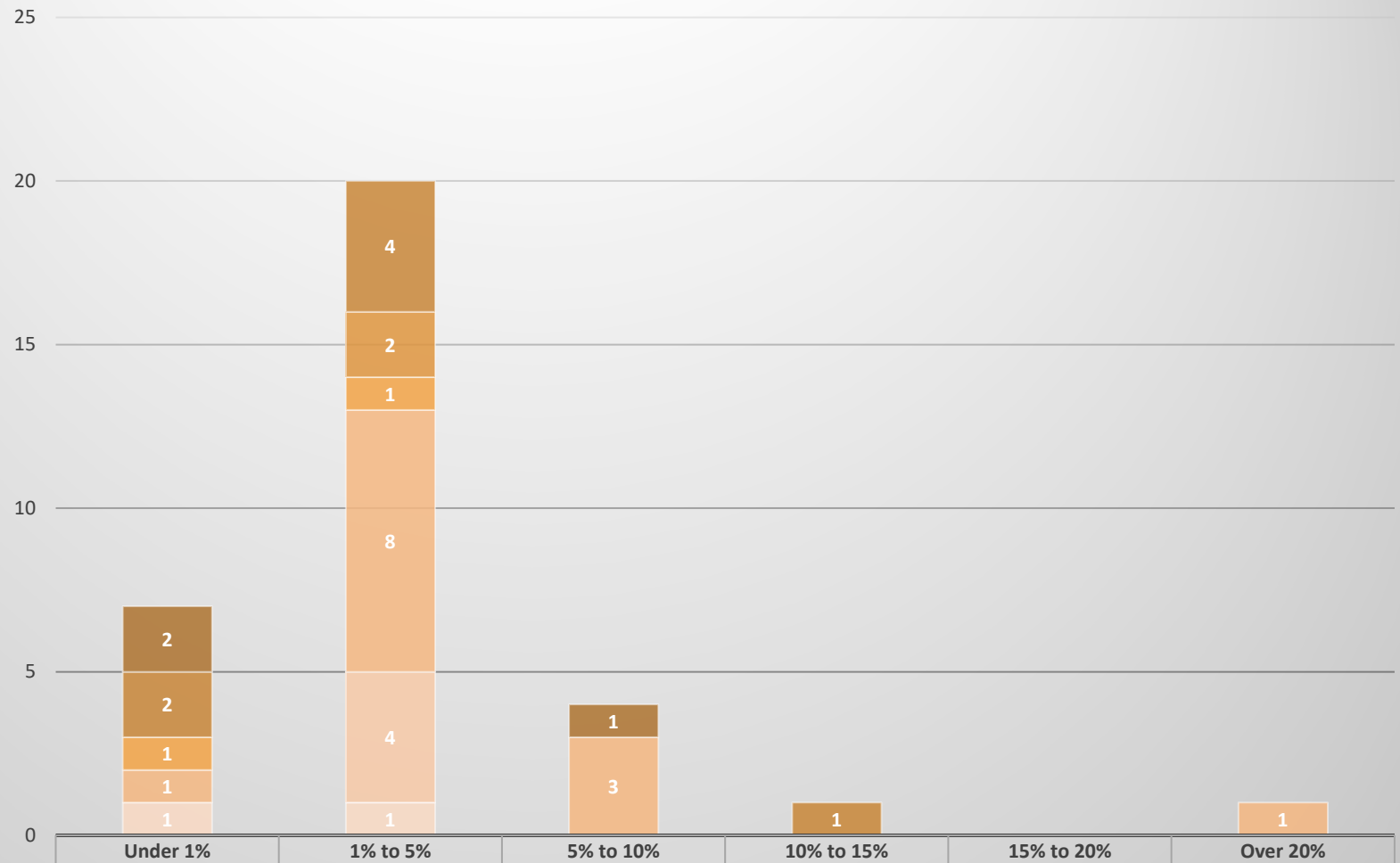




**Q2. How many full and part-time employees does your firm employ?  
(34 Responses)**

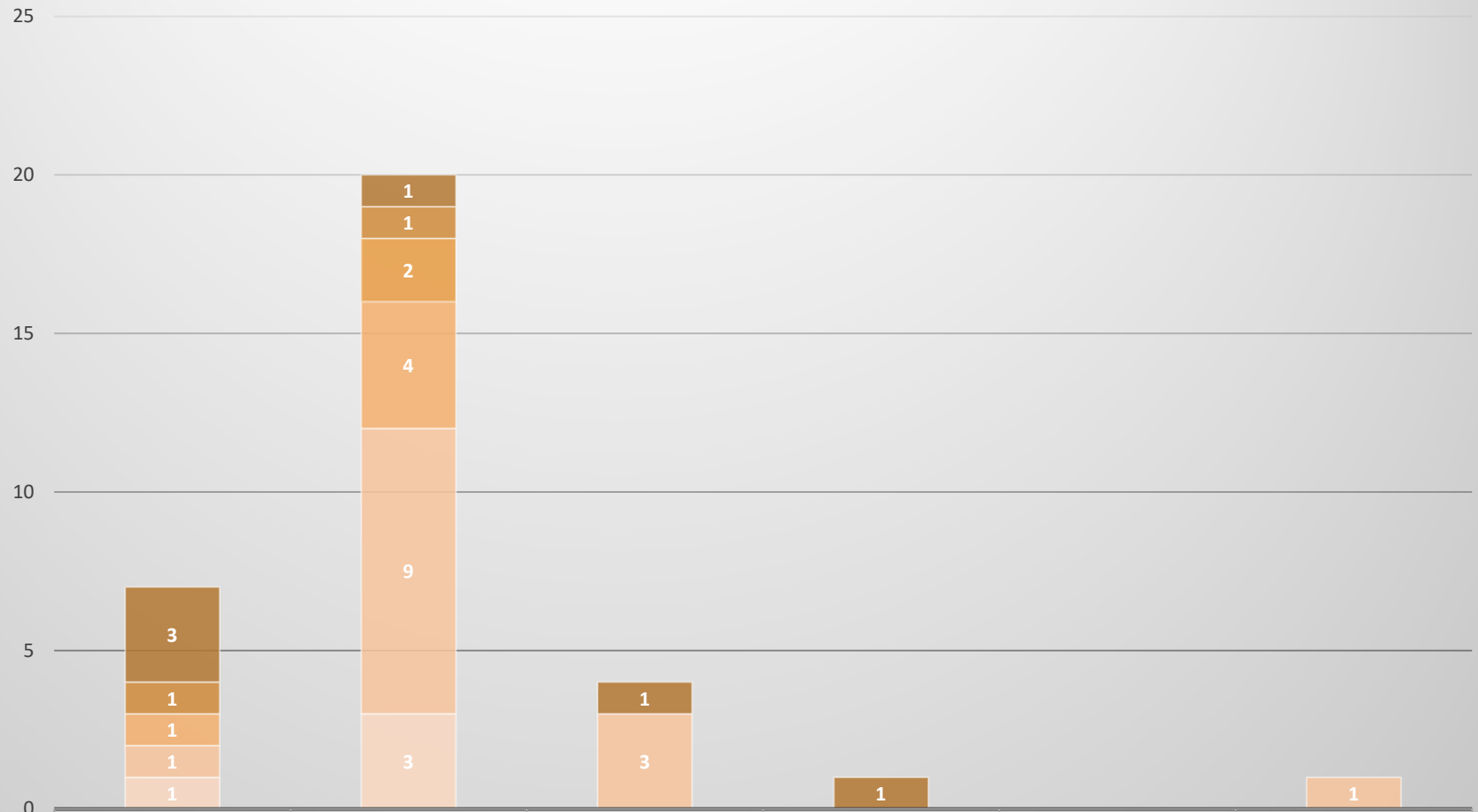


### Q3. What percentage of your firm's total revenue does your cybersecurity program budget represent? (33 Responses)



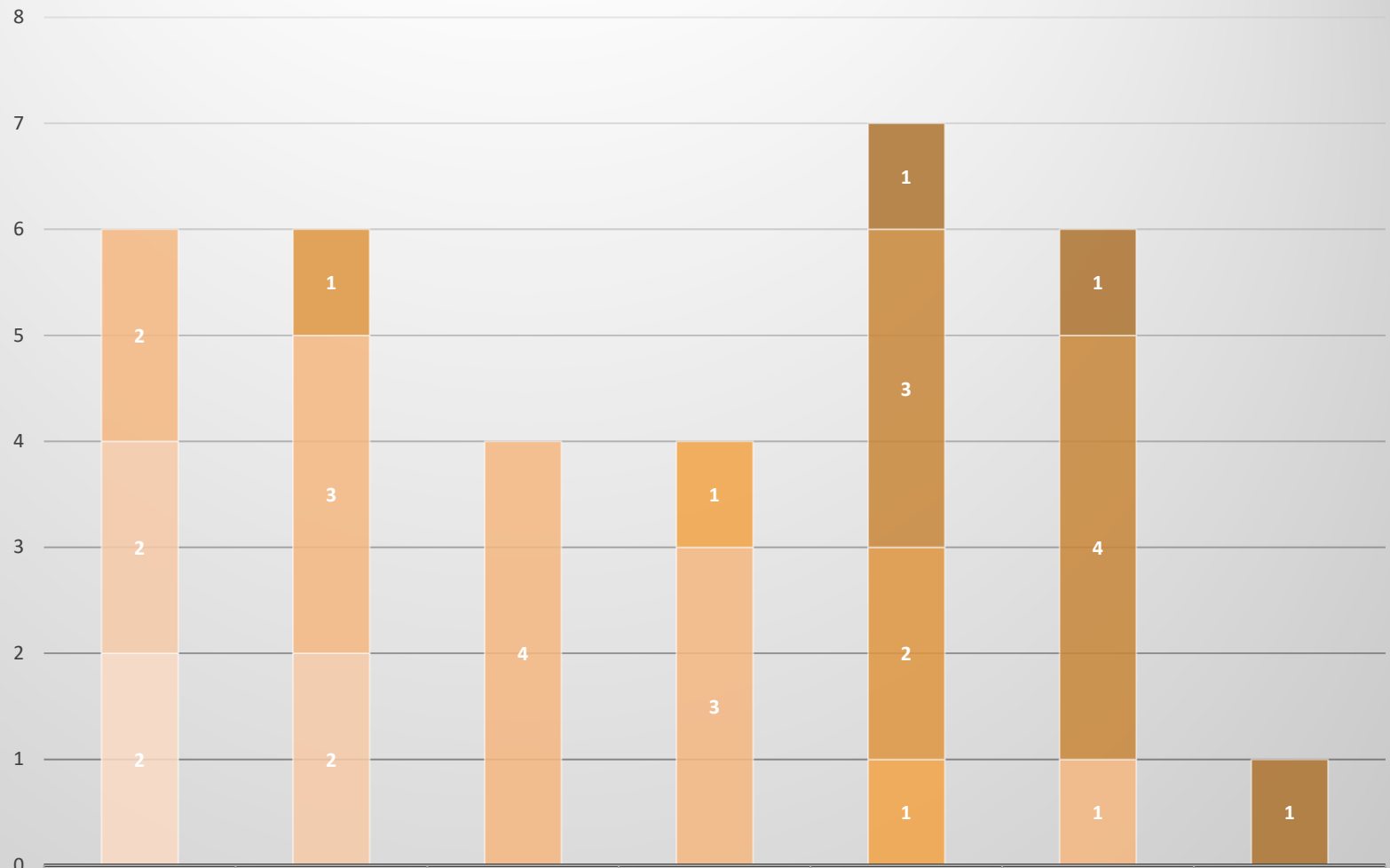
	Under 1%	1% to 5%	5% to 10%	10% to 15%	15% to 20%	Over 20%
Over \$1 trillion RAUM	2		1			
\$50 billion to under \$1 trillion RAUM	2	4		1		
\$20 billion to under \$50 billion RAUM		2				
\$10 billion to under \$20 billion RAUM	1	1				
\$1 billion to under \$10 billion RAUM	1	8	3			1
\$500 million to under \$1 billion RAUM		4				
Under \$500 million RAUM	1	1				

### Q3. What percentage of your firm's total revenue does your cybersecurity program budget represent? (33 Responses)



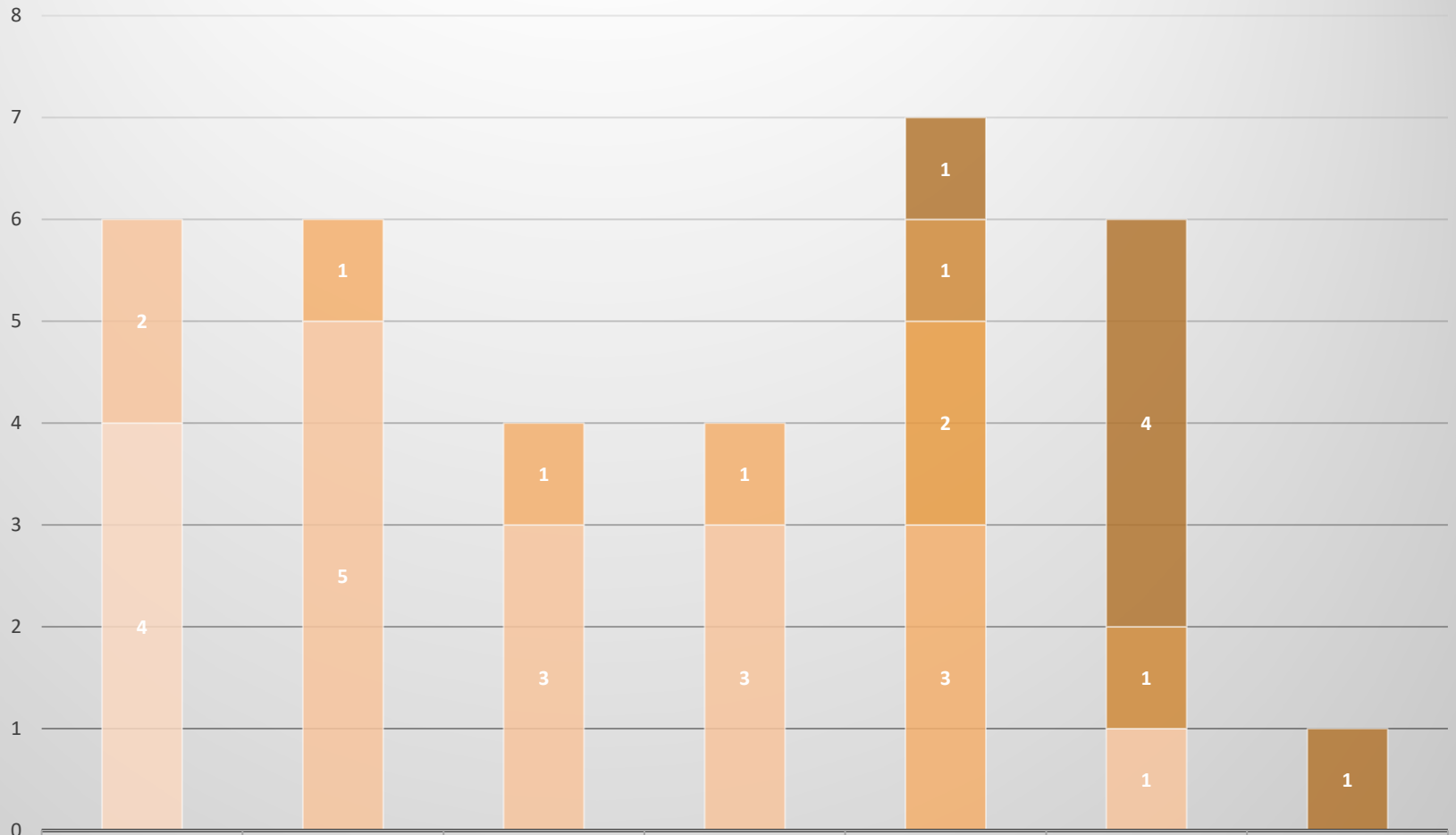
	Under 1%	1% to 5%	5% to 10%	10% to 15%	15% to 20%	Over 20%
More than 1,000 employees	3	1	1	1		
501 to 1,000 employees	1	1				
251 to 500 employees		2				
51 to 250 employees	1	4				
11 to 50 employees	1	9	3			1
6 to 10 employees	1	3				

## Q4. How much did your firm incur in total cybersecurity-related internal and external costs in 2021? (34 Responses)



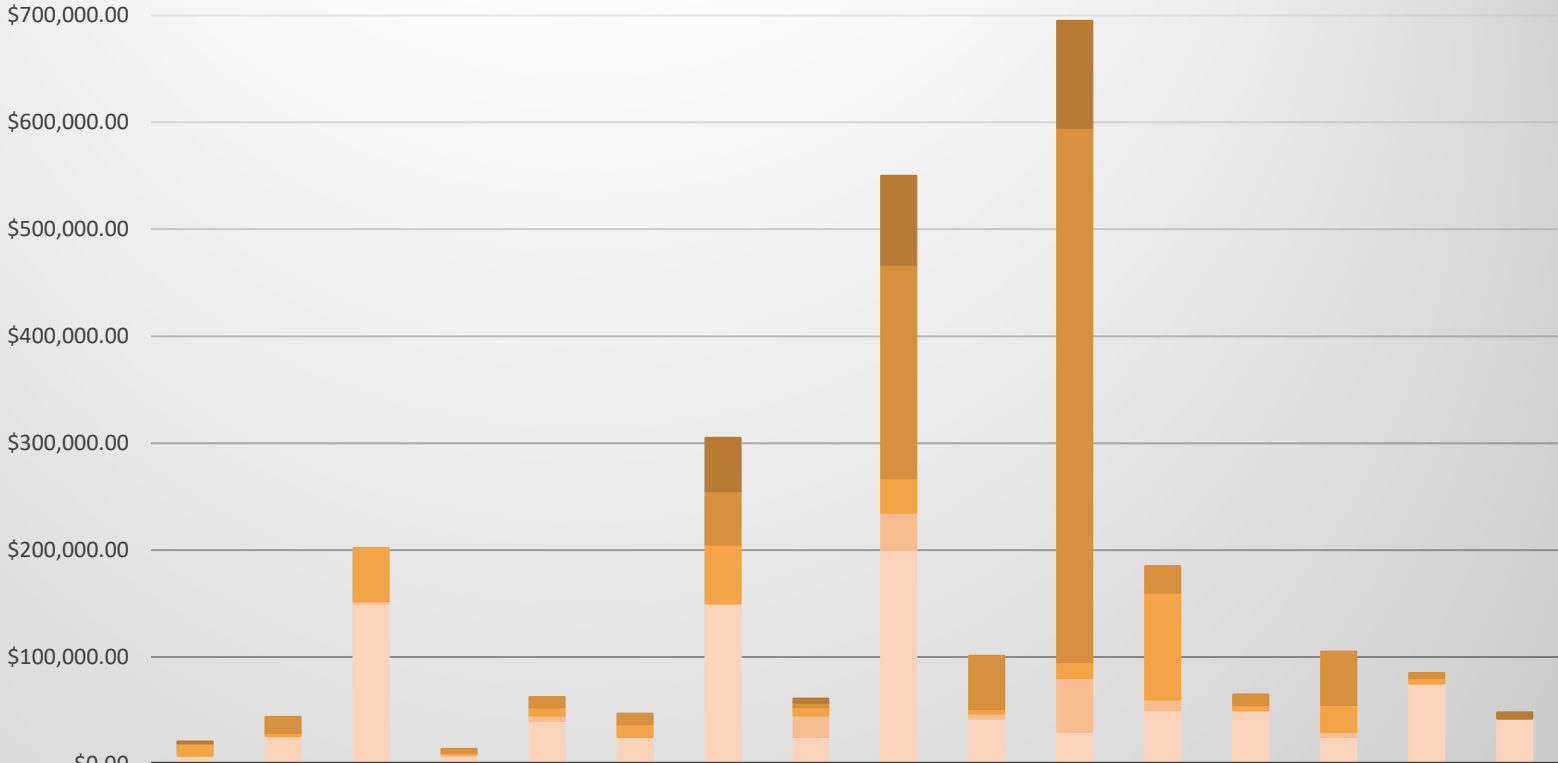
Over \$1 trillion RAUM					1	1	1
\$50 billion to under \$1 trillion RAUM					3	4	
\$20 billion to under \$50 billion RAUM		1			2		
\$10 billion to under \$20 billion RAUM				1	1		
\$1 billion to under \$10 billion RAUM	2	3	4	3		1	
\$500 million to under \$1 billion RAUM	2	2					
Under \$500 million RAUM	2						

## Q4. How much did your firm incur in total cybersecurity-related internal and external costs in 2021? (34 Responses)



	Under \$100,000	\$100,001 to \$250,000	\$251,000 to \$500,000	\$500,001 to \$1 million	\$1 million to \$5 million	\$5 million to \$500 million	Over \$500 million
More than 1,000 employees					1	4	1
501 to 1,000 employees					1	1	
251 to 500 employees					2		
51 to 250 employees		1	1	1	3		
11 to 50 employees	2	5	3	3		1	
6 to 10 employees	4						

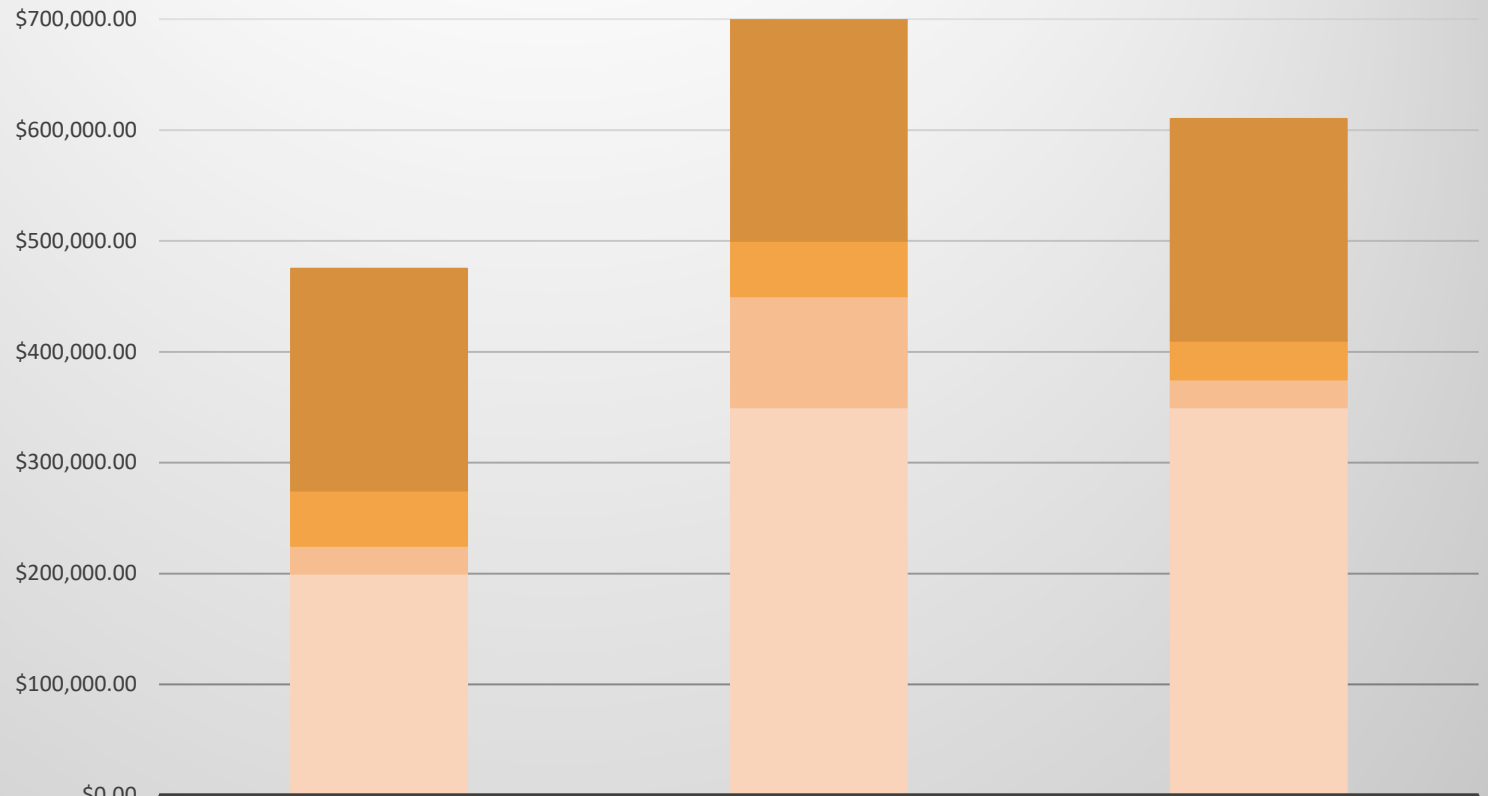
### Q5. Approximately how much will your firm pay in 2022 for external cybersecurity products and services? (Up to \$10B RAUM) (19 Firms)



	Under \$500 million	Under \$500 million	\$500 million to under \$1 billion	\$500 million to under \$1 billion	\$500 million to under \$1 billion	\$500 million to under \$1 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion	\$1 billion to under \$10 billion
Other	\$2,000						\$50,000	\$4,000	\$83,000		\$100,000				\$6,000
Procurement and Maintenance of Technology		\$15,000		\$3,500	\$10,000	\$10,000	\$50,000	\$4,000	\$200,000	\$50,000	\$500,000	\$25,000	\$10,000	\$50,000	\$5,000
Insurance	\$11,500	\$3,000	\$50,000	\$1,500	\$7,500	\$12,000	\$55,000	\$8,000	\$32,000	\$4,100	\$15,000	\$100,000	\$5,000	\$25,000	\$5,000
Legal			\$2,000	\$1,500	\$5,000			\$20,000	\$35,000	\$5,000	\$50,000	\$10,000		\$5,000	
Third-Party Consultants or Other Service Providers	\$7,500	\$26,000	\$150,000	\$7,500	\$40,000	\$25,000	\$150,000	\$25,000	\$200,000	\$42,000	\$30,000	\$50,000	\$50,000	\$25,000	\$75,000

■ Third-Party Consultants or Other Service Providers
 ■ Legal
 ■ Insurance
 ■ Procurement and Maintenance of Technology
 ■ Other

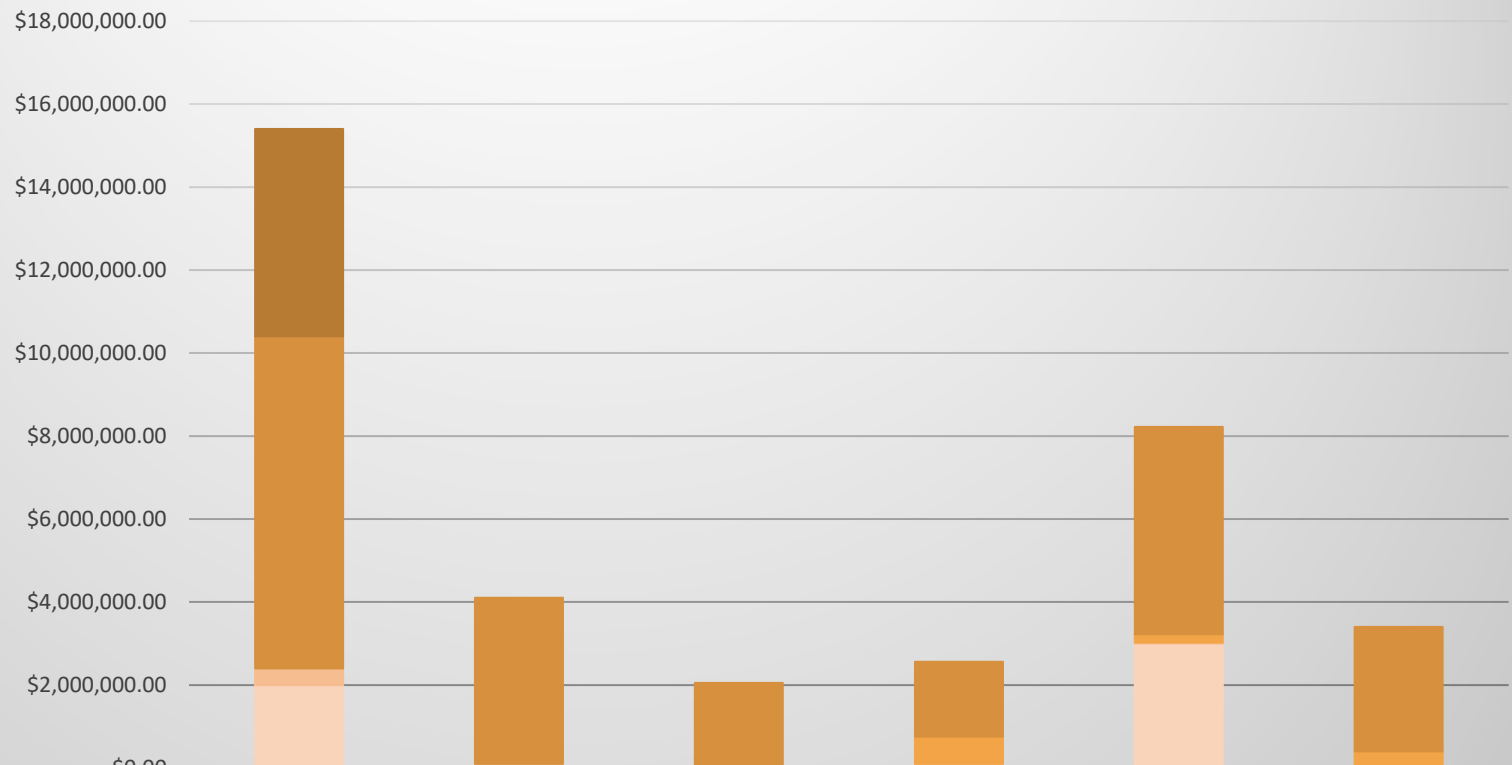
**Q5. Approximately how much will your firm pay in 2022 for external cybersecurity products and services? (Between \$10B and \$50B RAUM)  
(3 Firms)**



	\$10 billion to under \$20 billion	\$10 billion to under \$20 billion	\$20 billion to under \$50 billion
Other			
Procurement and Maintenance of Technology	200000	300000	200000
Insurance	50000	50000	35000
Legal	25000	100000	25000
Third-Party Consultants or Other Service Providers	200000	350000	350000

Third-Party Consultants or Other Service Providers    Legal    Insurance    Procurement and Maintenance of Technology    Other

## Q5. Approximately how much will your firm pay in 2022 for external cybersecurity products and services? (Between \$50B and \$1T RAUM) (6 Firms)

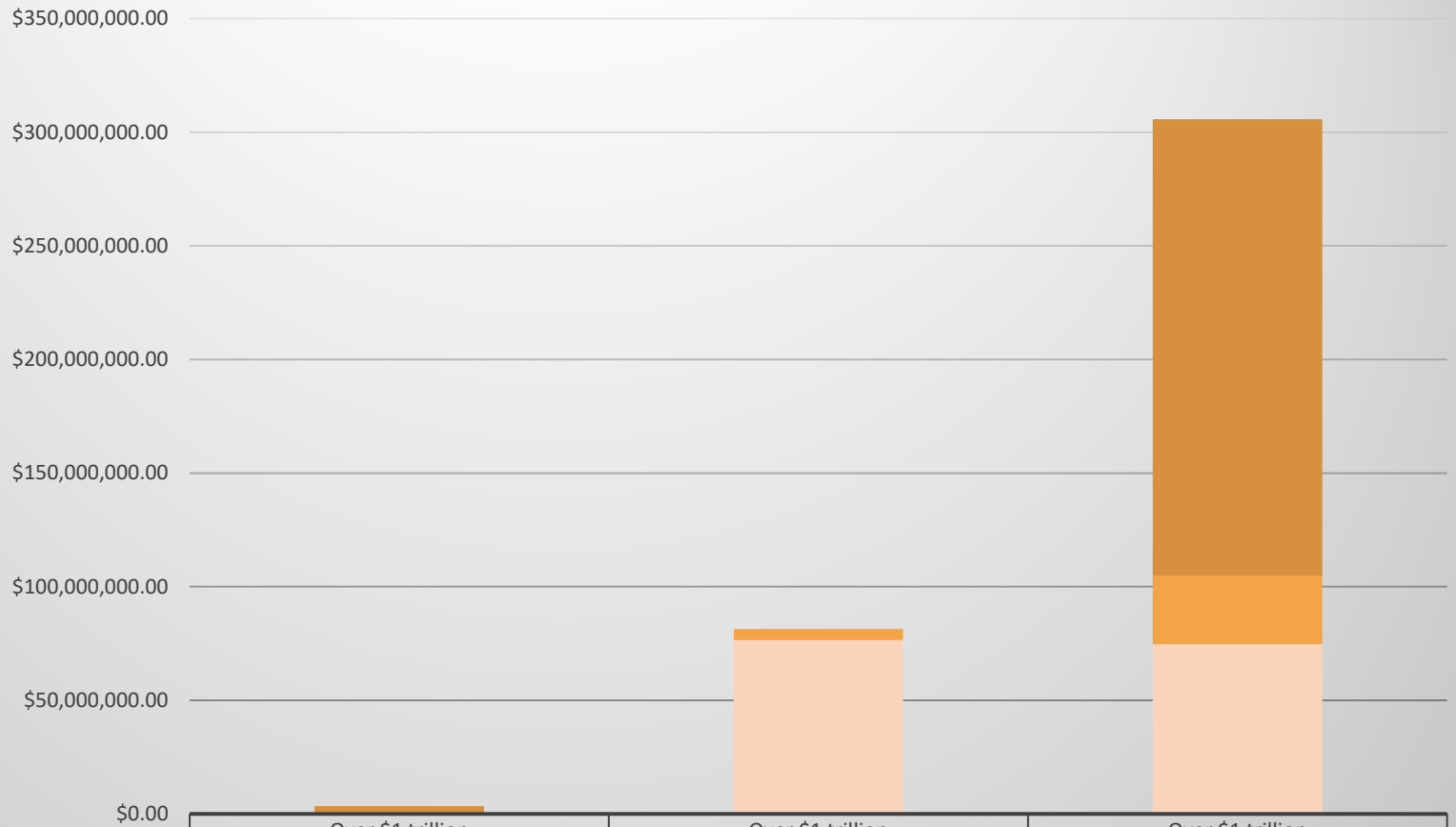


	\$50 billion to under \$1 trillion	\$50 billion to under \$1 trillion	\$50 billion to under \$1 trillion	\$50 billion to under \$1 trillion	\$50 billion to under \$1 trillion	\$50 billion to under \$1 trillion
Other	\$5,000,000					
Procurement and Maintenance of Technology	\$8,000,000	\$4,000,000	\$2,000,000	\$1,800,000	\$5,000,000	\$3,000,000
Insurance			\$50,000	\$657,000	\$200,000	\$400,000
Legal	\$400,000	\$100,000		\$100,000	\$25,000	
Third-Party Consultants or Other Service Providers	\$2,000,000				\$3,000,000	

■ Third-Party Consultants or Other Service Providers
 ■ Legal
 ■ Insurance
 ■ Procurement and Maintenance of Technology
 ■ Other



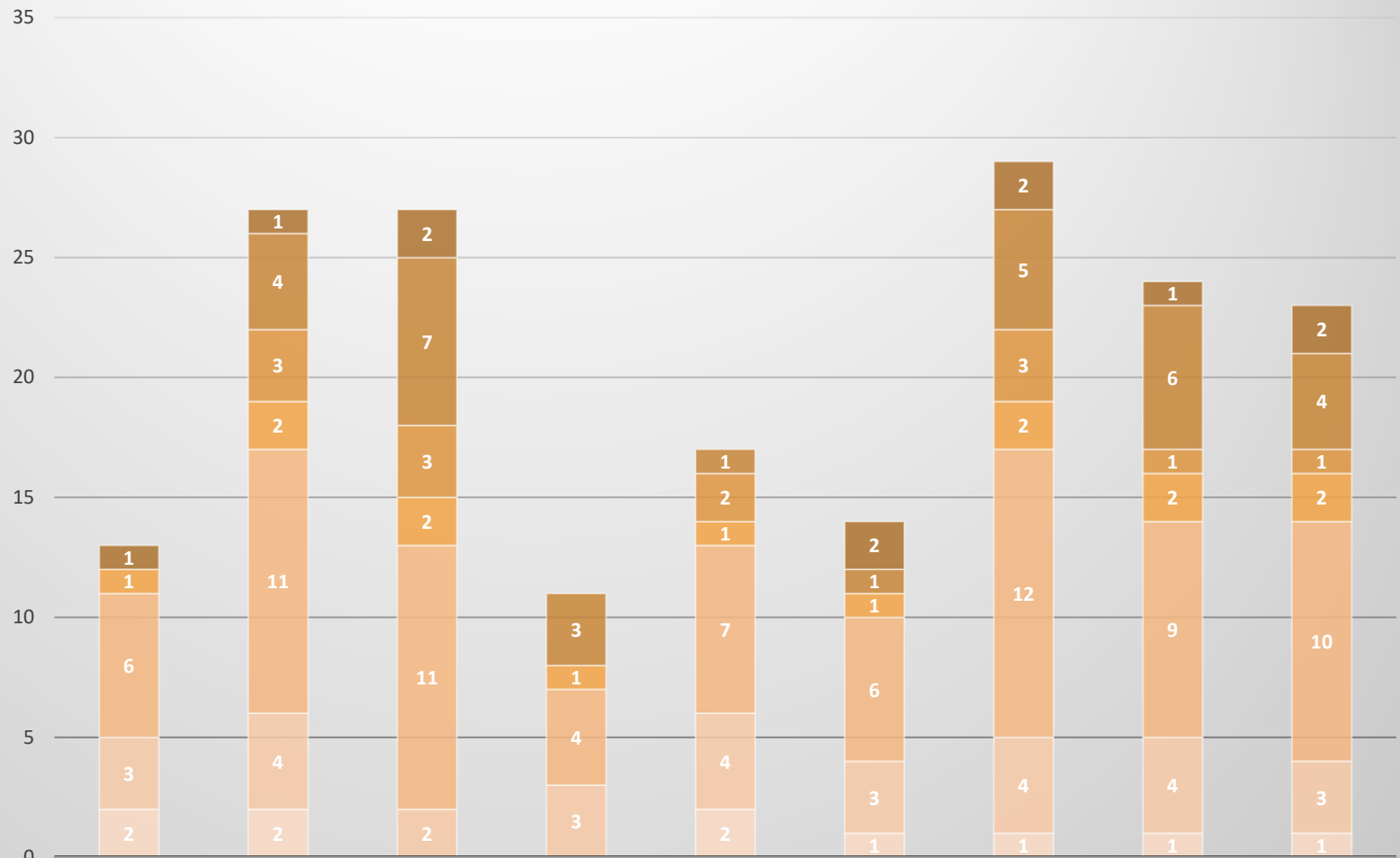
## Q5. Approximately how much will your firm pay in 2022 for external cybersecurity products and services? (Over \$1T RAUM) (3 Firms)



	Over \$1 trillion	Over \$1 trillion	Over \$1 trillion
Other			
Procurement and Maintenance of Technology	\$2,000,000		\$200,000,000
Insurance		\$4,000,000	\$30,000,000
Legal			\$250,000
Third-Party Consultants or Other Service Providers	\$1,000,000	\$77,000,000	\$75,000,000

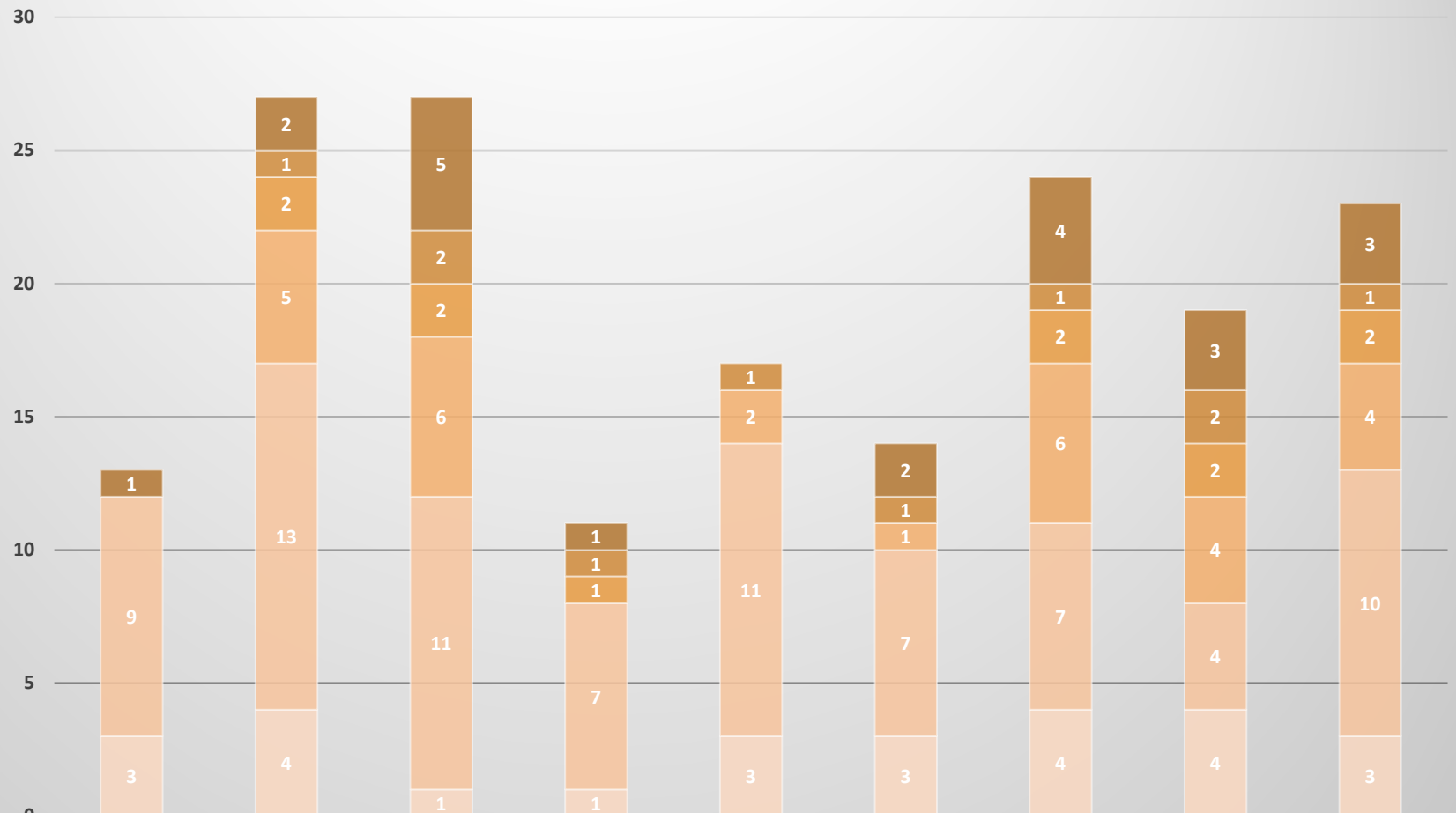
■ Third-Party Consultants or Other Service Providers
 ■ Legal
 ■ Insurance
 ■ Procurement and Maintenance of Technology
 ■ Other

## Q6. If you engage third-party consultants or other service providers, which of the following services do they provide for your firm? (34 Responses)



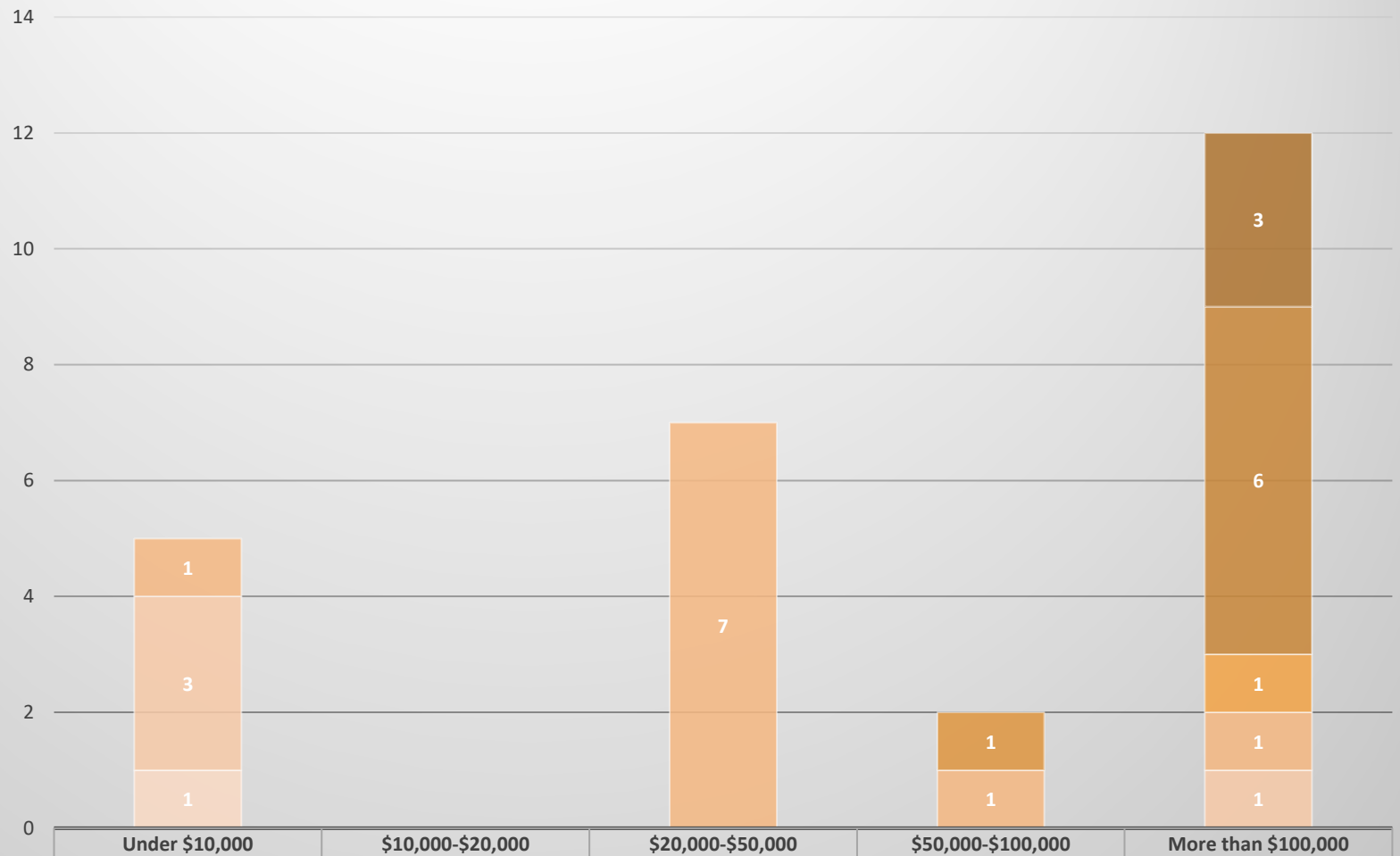
	Creation of Cybersecurity Strategy	Vulnerability Assessments	Penetration Testing	Web Application Assessments	Security Architecture Review	Security Program Development	Threat Monitoring	Incident Response and Management	Training
Over \$1 trillion RAUM	1	1	2			2	2	1	2
\$50 billion to under \$1 trillion RAUM		4	7	3	1	1	5	6	4
\$20 billion to under \$50 billion RAUM		3	3		2		3	1	1
\$10 billion to under \$20 billion RAUM	1	2	2	1	1	1	2	2	2
\$1 billion to under \$10 billion RAUM	6	11	11	4	7	6	12	9	10
\$500 million to under \$1 billion RAUM	3	4	2	3	4	3	4	4	3
Under \$500 million RAUM	2	2			2	1	1	1	1

## Q6. If you engage third-party consultants or other service providers, which of the following services do they provide for your firm? (34 Responses)



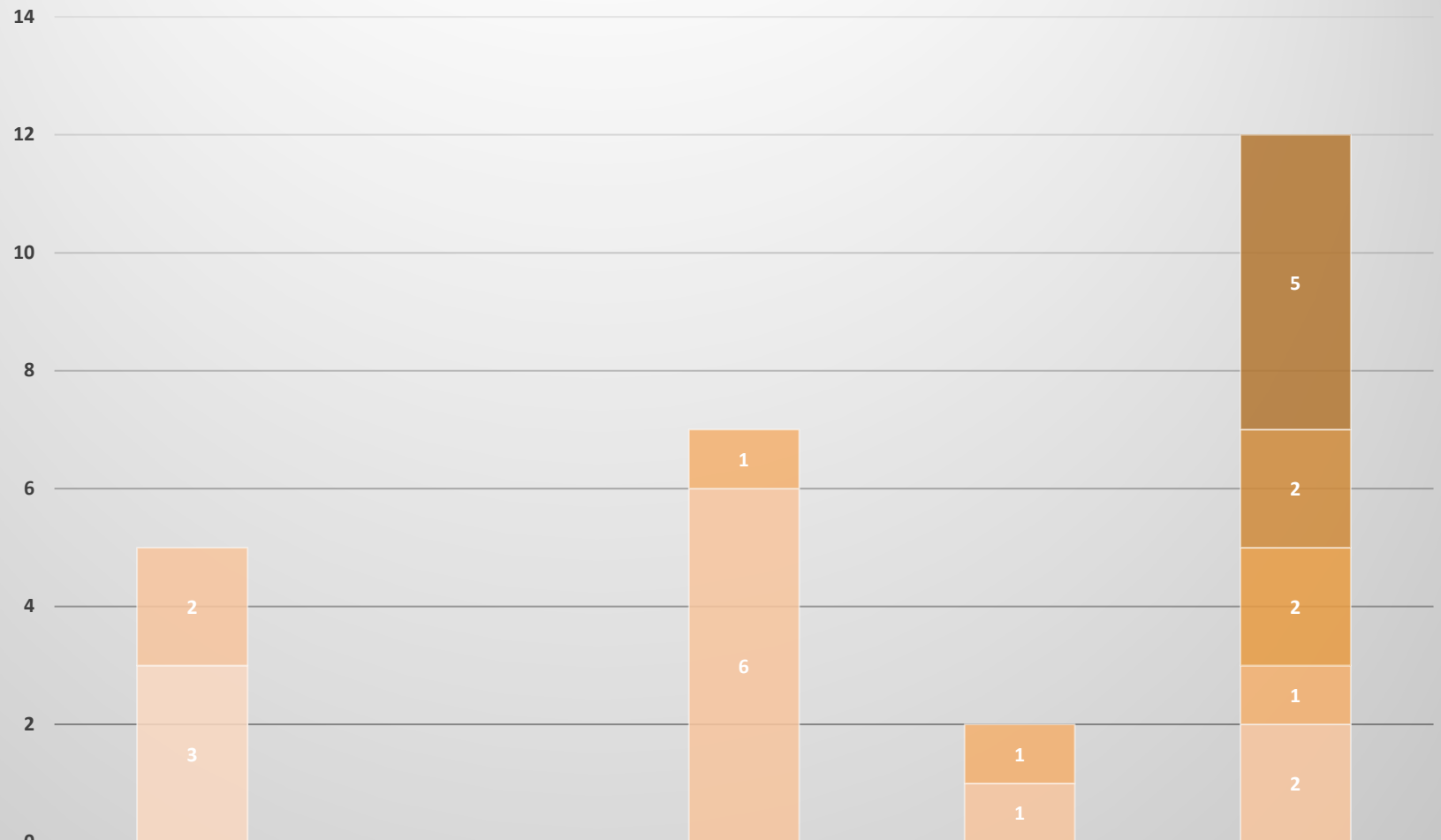
	Creation of Cybersecurity Strategy	Vulnerability Assessments	Penetration Testing	Web Application Assessments	Security Architecture Review	Security Program Development	Threat Monitoring	Incident Response and Management	Training
More than 1,000 employees	1	2	5	1		2	4	3	3
501 to 1,000 employees		1	2	1	1	1	1	2	1
251 to 500 employees		2	2	1			2	2	2
51 to 250 employees		5	6		2	1	6	4	4
11 to 50 employees	9	13	11	7	11	7	7	4	10
6 to 10 employees	3	4	1	1	3	3	4	4	3

## Q7.1 What would be the initial costs associated with adopting and implementing the proposed cybersecurity policies and procedures for your firm? (26 Responses)



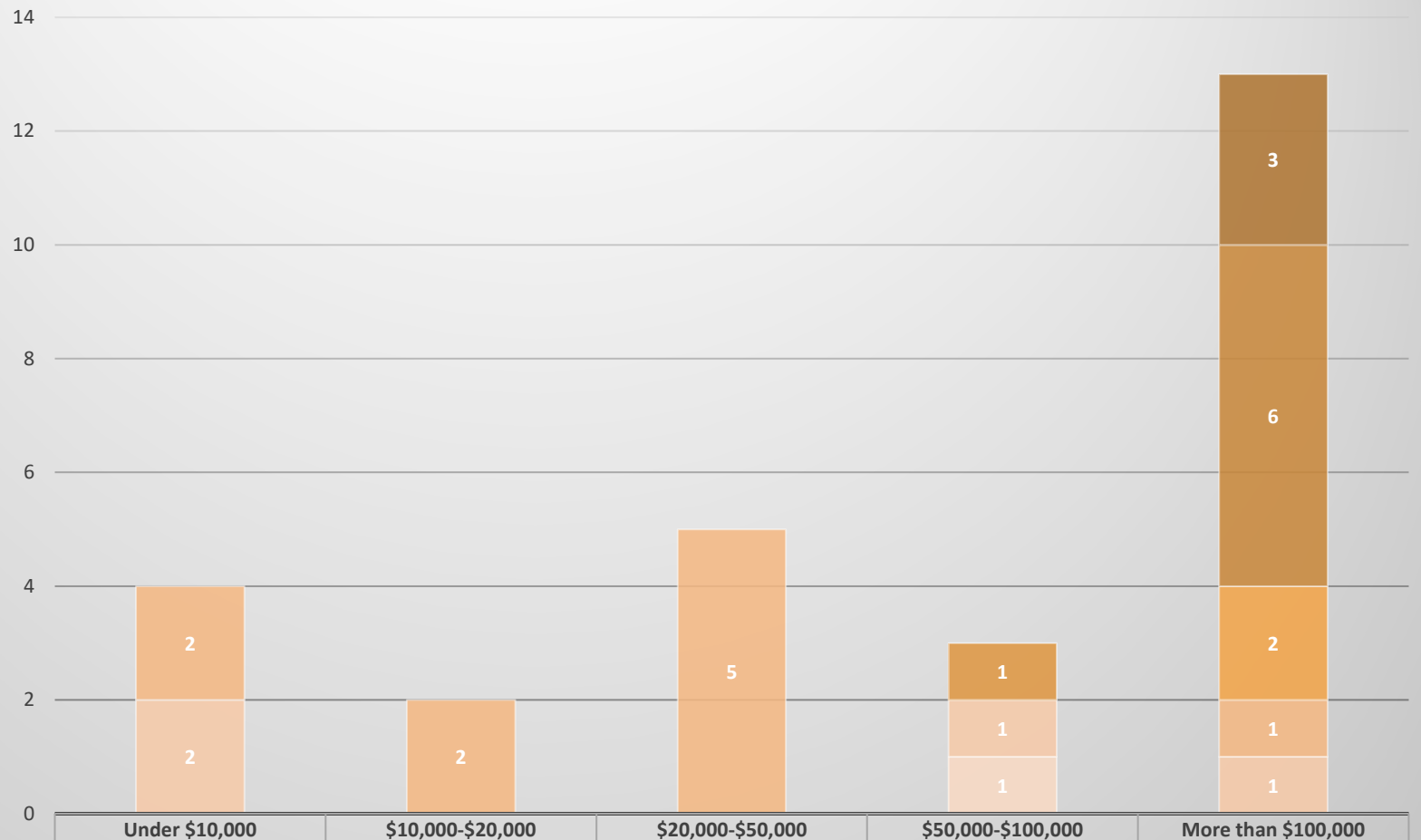
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM					3
\$50 billion to under \$1 trillion RAUM					6
\$20 billion to under \$50 billion RAUM				1	1
\$10 billion to under \$20 billion RAUM					1
\$1 billion to under \$10 billion RAUM	1		7	1	1
\$500 million to under \$1 billion RAUM	3				1
Under \$500 million RAUM	1				

## Q7.1 What would be the initial costs associated with adopting and implementing the proposed cybersecurity policies and procedures for your firm? (26 Responses)



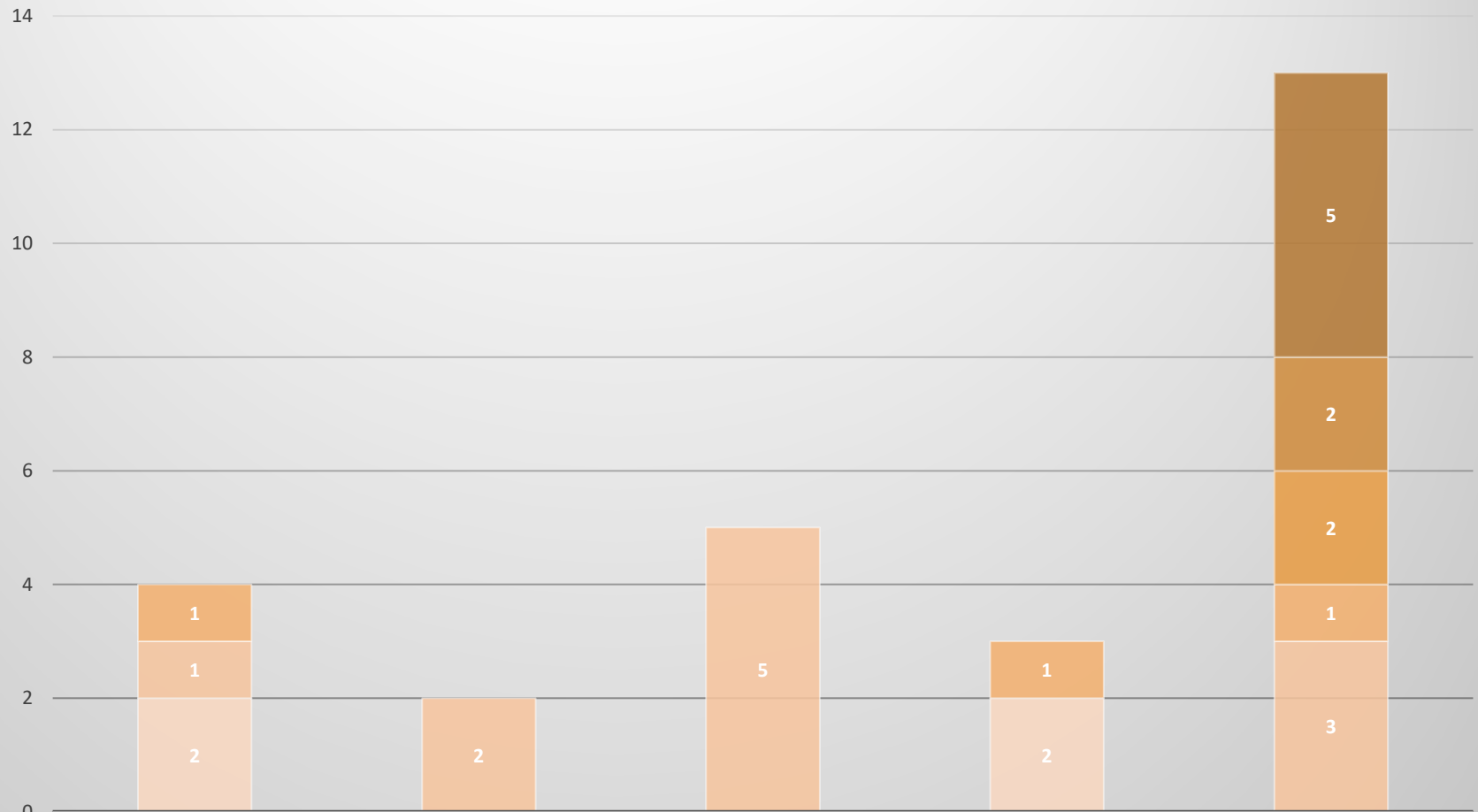
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees					5
501 to 1000 employees					2
251 to 500 employees					2
51 to 250 employees			1	1	1
11 to 50 employees	2		6	1	2
6 to 10 employees	3				

## Q7.2 What would be the annual ongoing costs associated with adopting and implementing the proposed cybersecurity policies and procedures for your firm? (27 Responses)



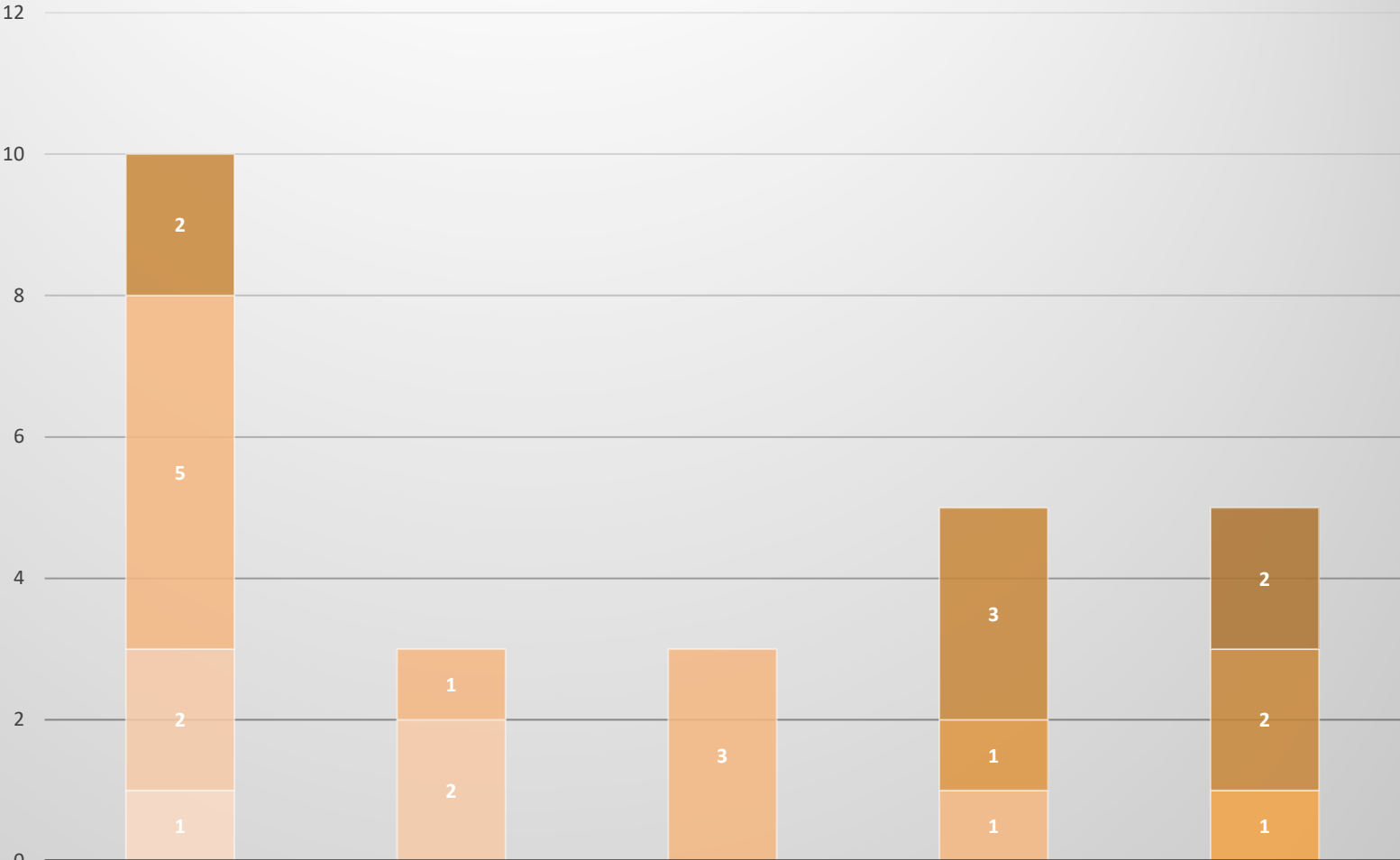
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM					3
\$50 billion to under \$1 trillion RAUM					6
\$20 billion to under \$50 billion RAUM				1	2
\$10 billion to under \$20 billion RAUM			5		1
\$1 billion to under \$10 billion RAUM	2	2			1
\$500 million to under \$1 billion RAUM	2			1	1
Under \$500 million RAUM				1	

## Q7.2 What would be the annual ongoing costs associated with adopting and implementing the proposed cybersecurity policies and procedures for your firm? (27 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees					5
501 to 1000 employees					2
251 to 500 employees					2
51 to 250 employees	1			1	1
11 to 50 employees	1	2	5		3
6 to 10 employees	2			2	

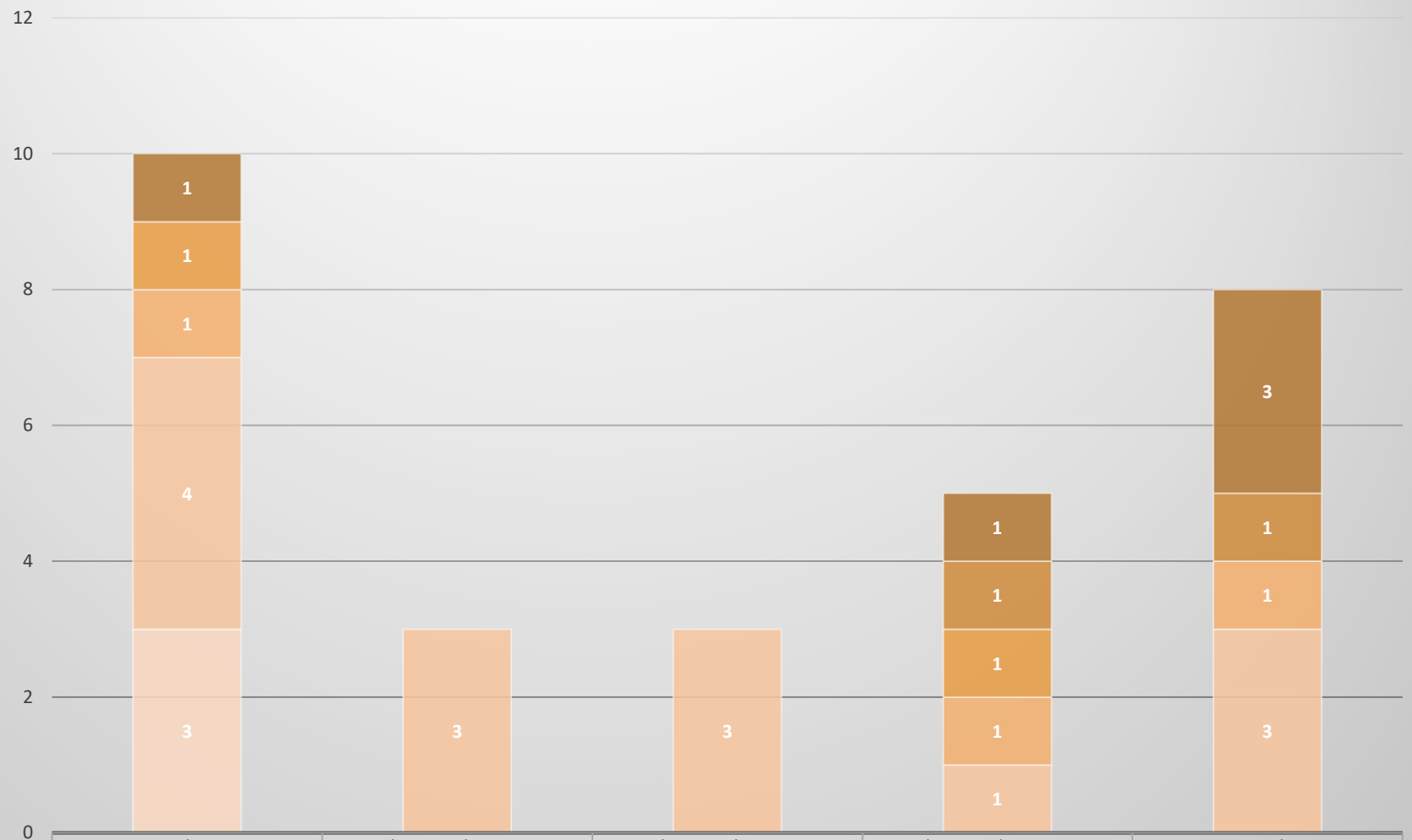
# Q8.1 What would be the initial costs associated with implementing the proposed disclosure requirements of cybersecurity risks and incidents? (26 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM					2
\$50 billion to under \$1 trillion RAUM	2			3	2
\$20 billion to under \$50 billion RAUM				1	
\$10 billion to under \$20 billion RAUM					1
\$1 billion to under \$10 billion RAUM	5	1	3	1	
\$500 million to under \$1 billion RAUM	2	2			
Under \$500 million RAUM	1				

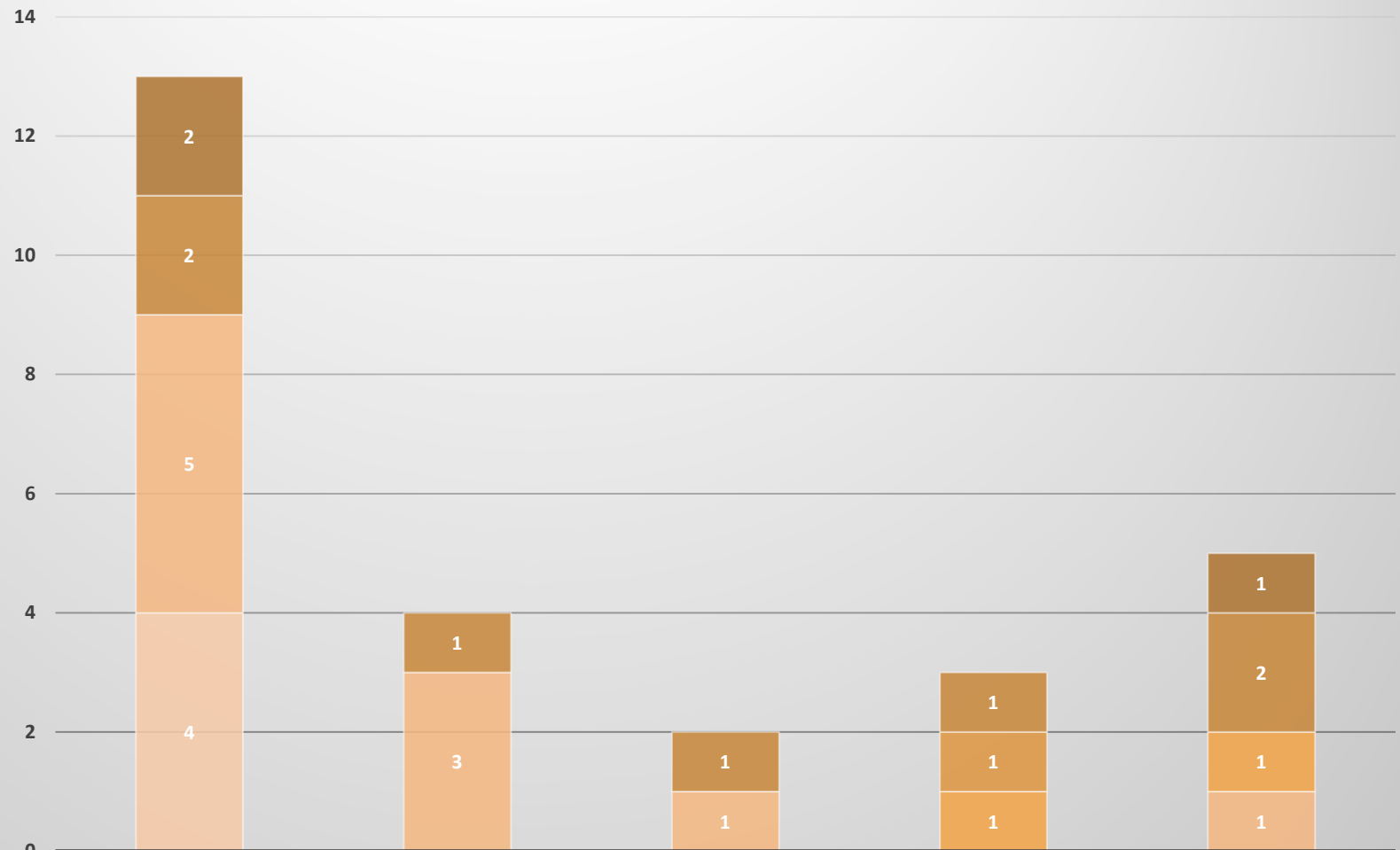


## Q8.1 What would be the initial costs associated with implementing the proposed disclosure requirements of cybersecurity risks and incidents? (26 Responses)



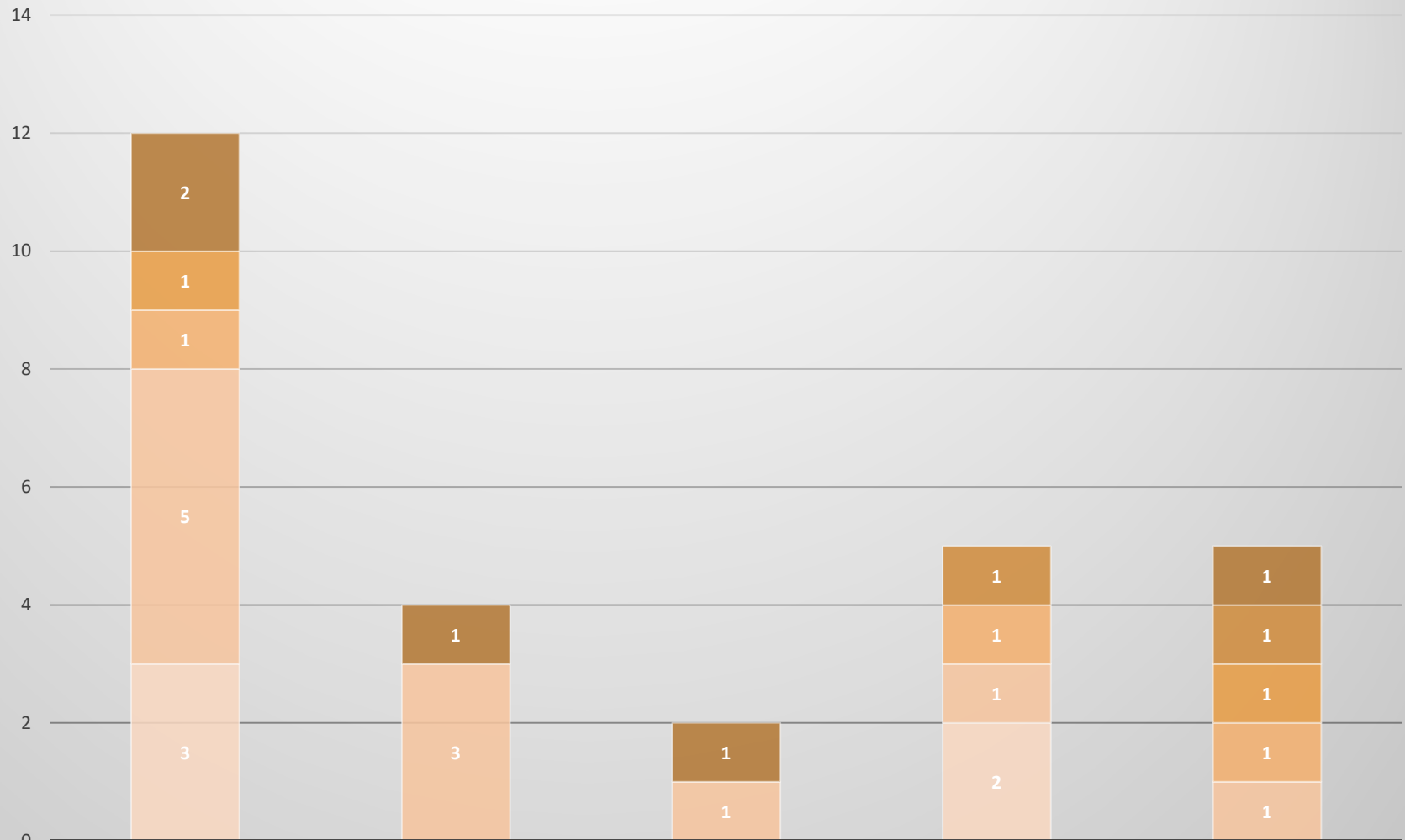
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	1			1	3
501 to 1000 employees				1	1
251 to 500 employees	1			1	
51 to 250 employees	1			1	1
11 to 50 employees	4	3	3	1	3
6 to 10 employees	3				

## Q8.2 What would be the ongoing annual costs associated with implementing the proposed disclosure requirements of cybersecurity risks and incidents? (27 Responses)



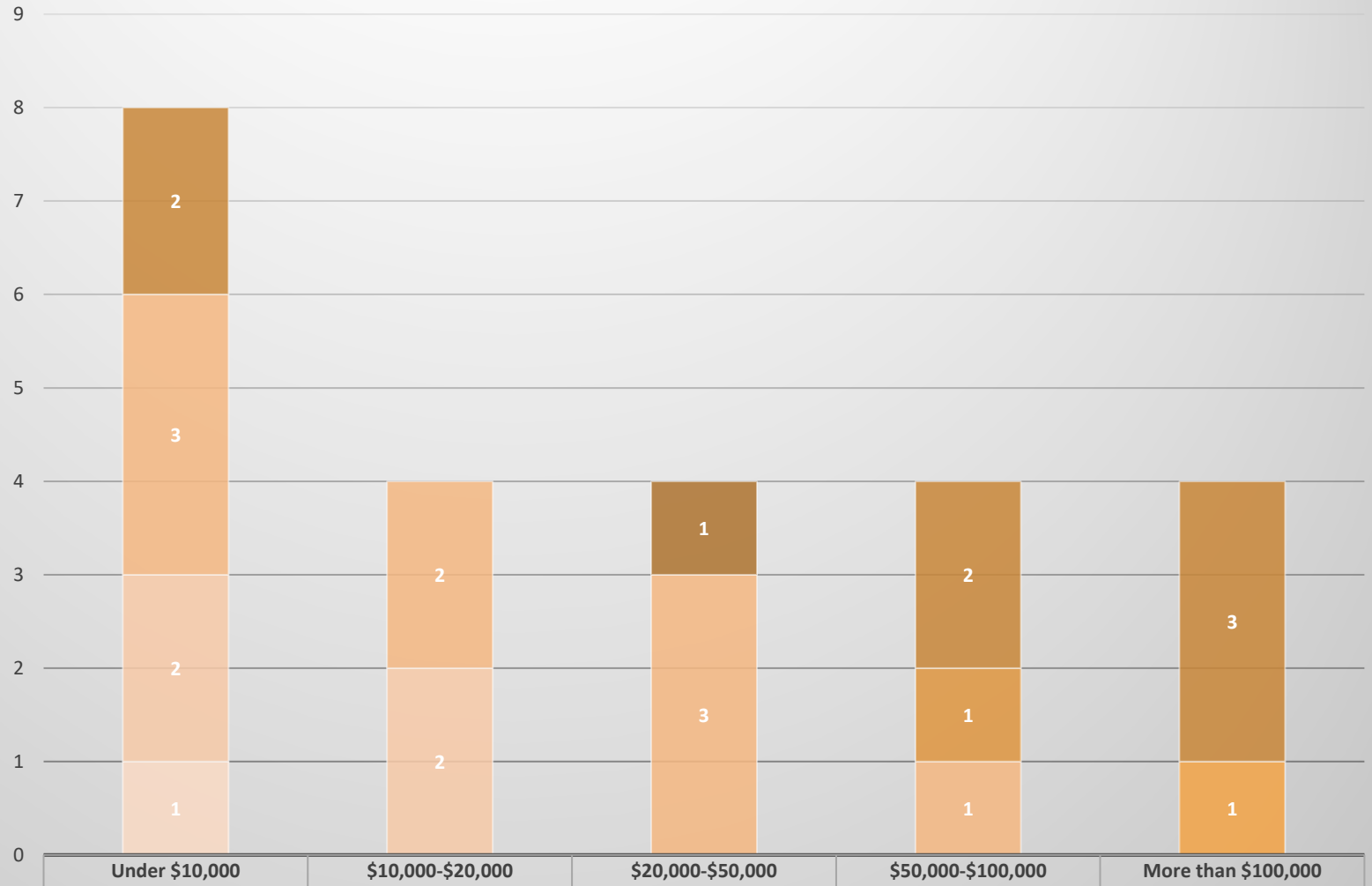
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM	2				1
\$50 billion to under \$1 trillion RAUM	2	1	1	1	2
\$20 billion to under \$50 billion RAUM				1	
\$10 billion to under \$20 billion RAUM				1	1
\$1 billion to under \$10 billion RAUM	5	3	1		1
\$500 million to under \$1 billion RAUM	4				
Under \$500 million RAUM					

## Q8.2 What would be the ongoing annual costs associated with implementing the proposed disclosure requirements of cybersecurity risks and incidents? (27 Responses)



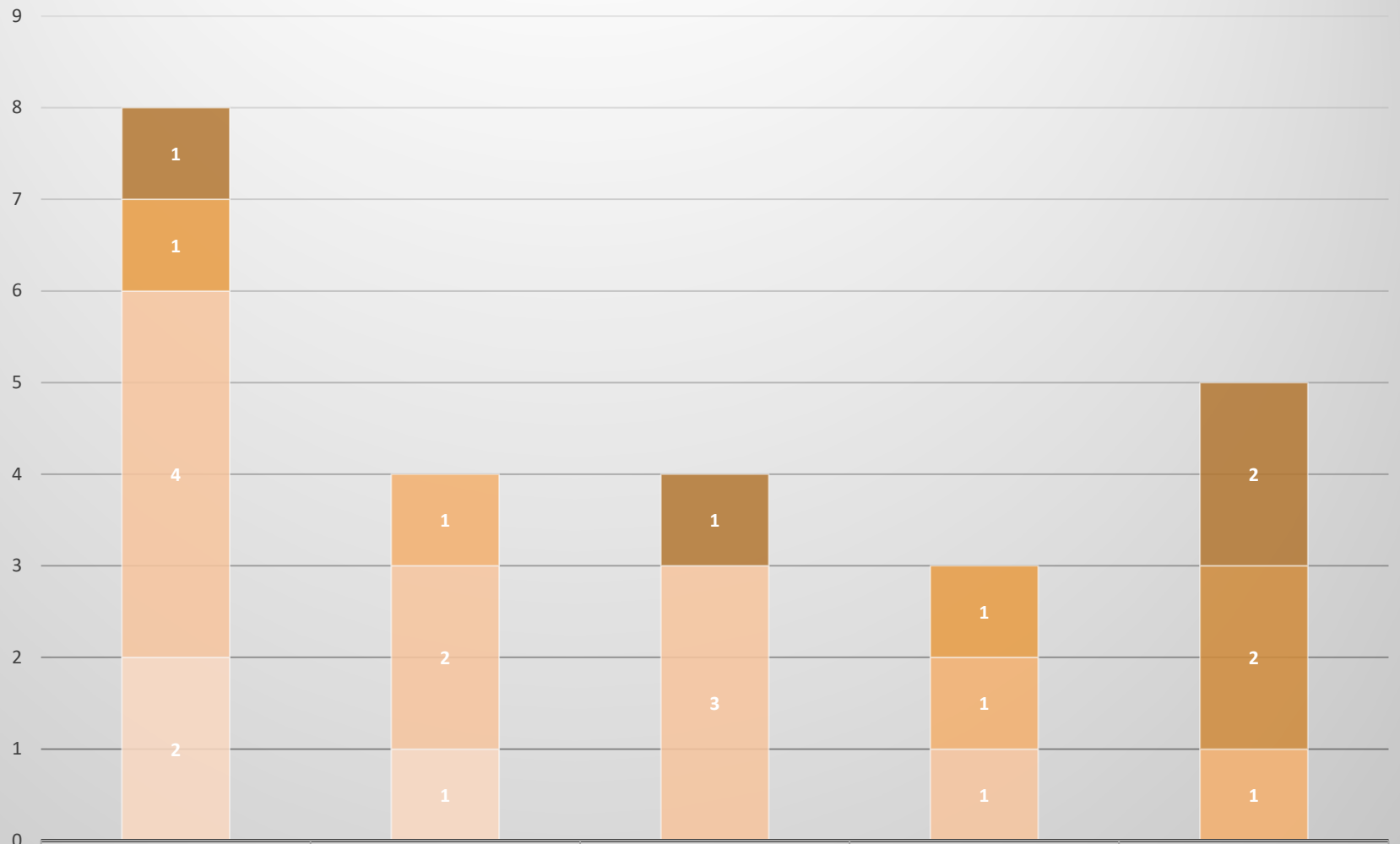
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	2	1	1		1
501 to 1000 employees				1	1
251 to 500 employees	1				1
51 to 250 employees	1		1	1	1
11 to 50 employees	5	3	1	1	1
6 to 10 employees	3			2	

## Q9.1 What would be the initial costs associated with implementing the proposed requirements of regulatory reporting of cybersecurity incidents? (24 Responses)



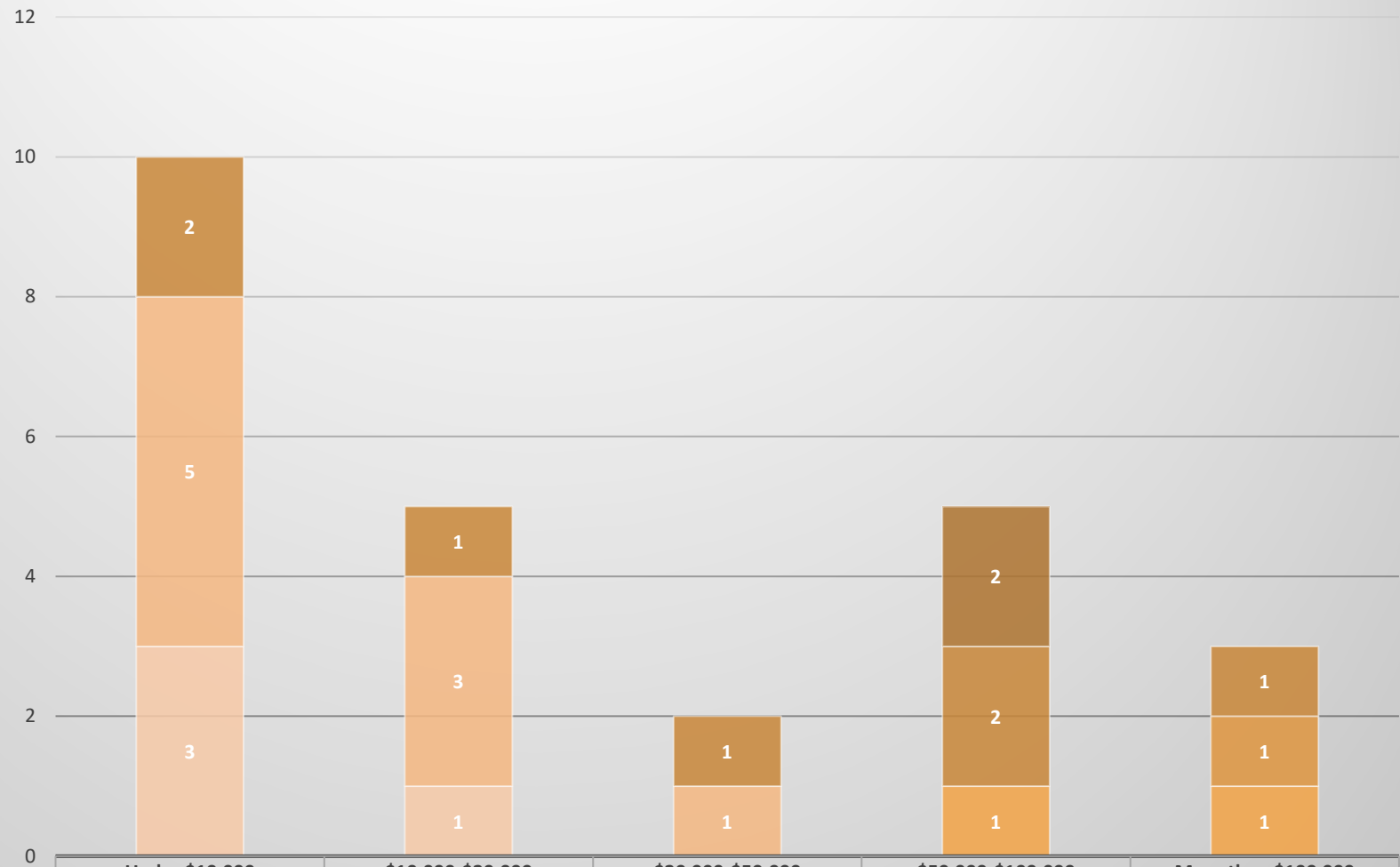
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM			1		
\$50 billion to under \$1 trillion RAUM	2			2	3
\$20 billion to under \$50 billion RAUM				1	
\$10 billion to under \$20 billion RAUM					1
\$1 billion to under \$10 billion RAUM	3	2	3	1	
\$500 million to under \$1 billion RAUM	2	2			
Under \$500 million RAUM	1				

## Q9.1 What would be the initial costs associated with implementing the proposed requirements of regulatory reporting of cybersecurity incidents? (24 Responses)



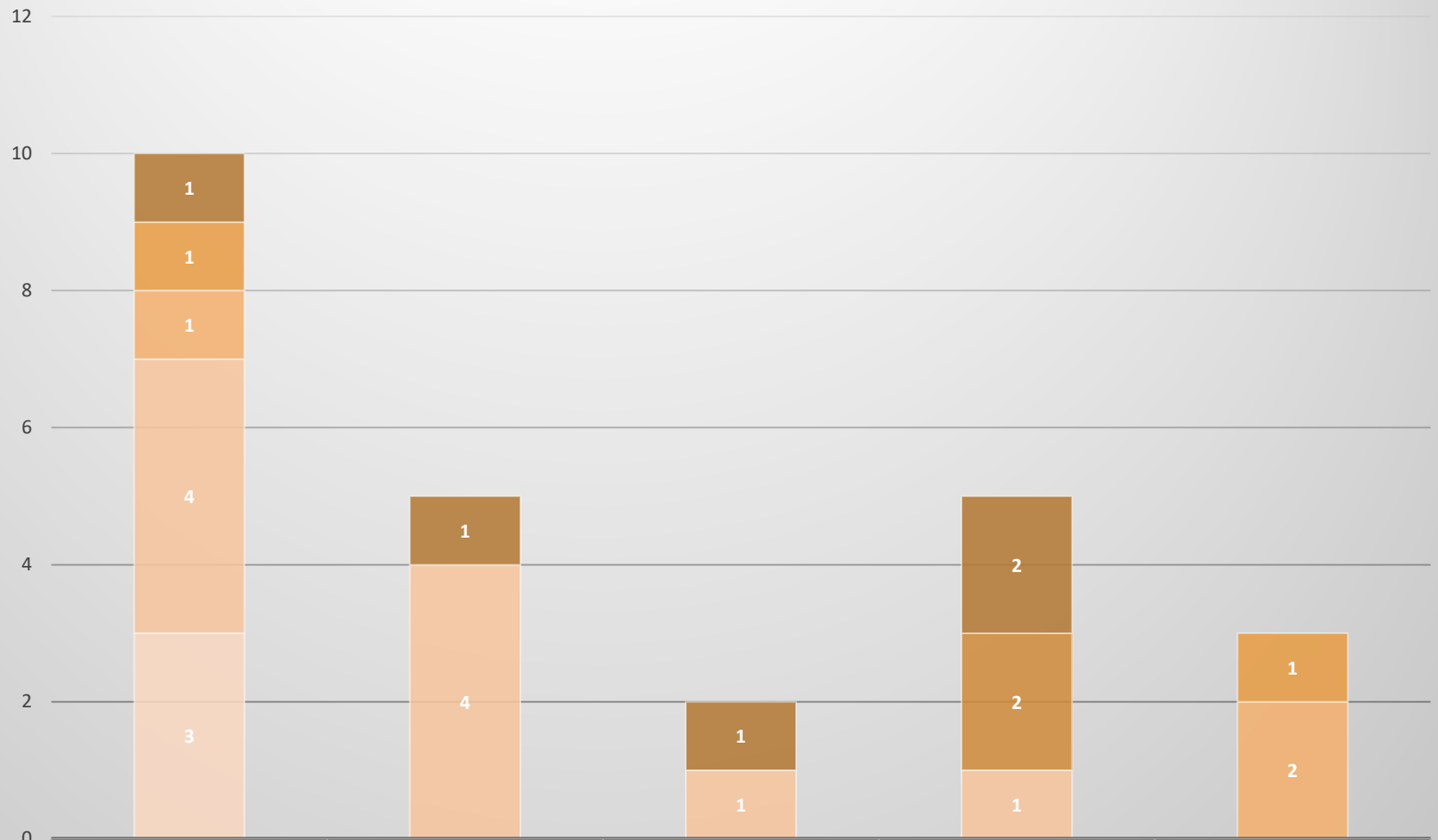
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	1		1		2
501 to 1000 employees					2
251 to 500 employees	1			1	
51 to 250 employees		1		1	1
11 to 50 employees	4	2	3	1	
6 to 10 employees	2	1			

## Q9.2 What would be the ongoing annual costs associated with implementing the proposed requirements of regulatory reporting of cybersecurity incidents? (25 Responses)



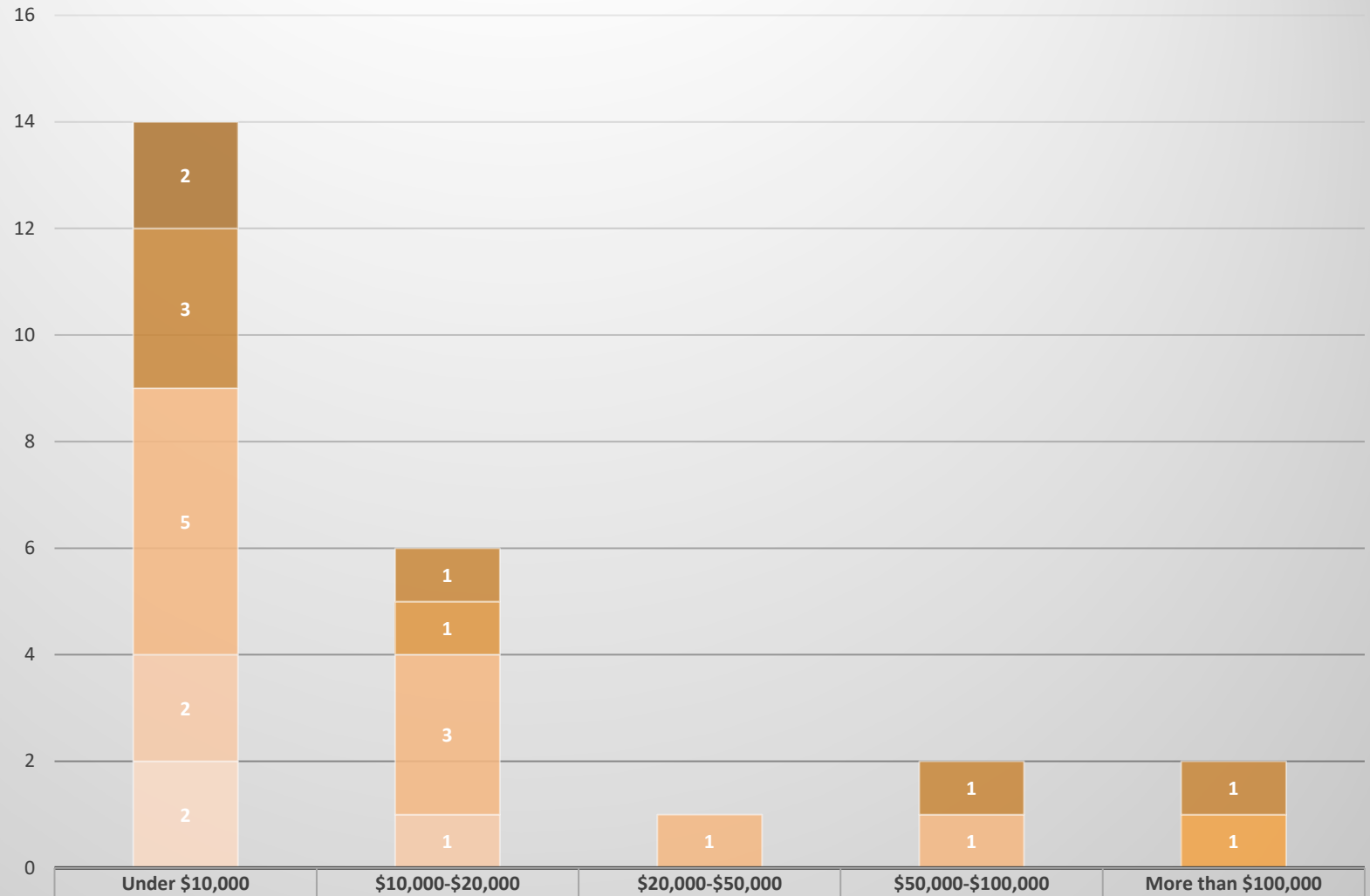
Over \$1 trillion RAUM				2	
\$50 billion to under \$1 trillion RAUM	2	1	1	2	1
\$20 billion to under \$50 billion RAUM					1
\$10 billion to under \$20 billion RAUM				1	1
\$1 billion to under \$10 billion RAUM	5	3	1		
\$500 million to under \$1 billion RAUM	3	1			
Under \$500 million RAUM					

## Q9.2 What would be the ongoing annual costs associated with implementing the proposed requirements of regulatory reporting of cybersecurity incidents? (25 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	1	1	1	2	
501 to 1000 employees				2	
251 to 500 employees	1				1
51 to 250 employees	1				2
11 to 50 employees	4	4	1	1	
6 to 10 employees	3				

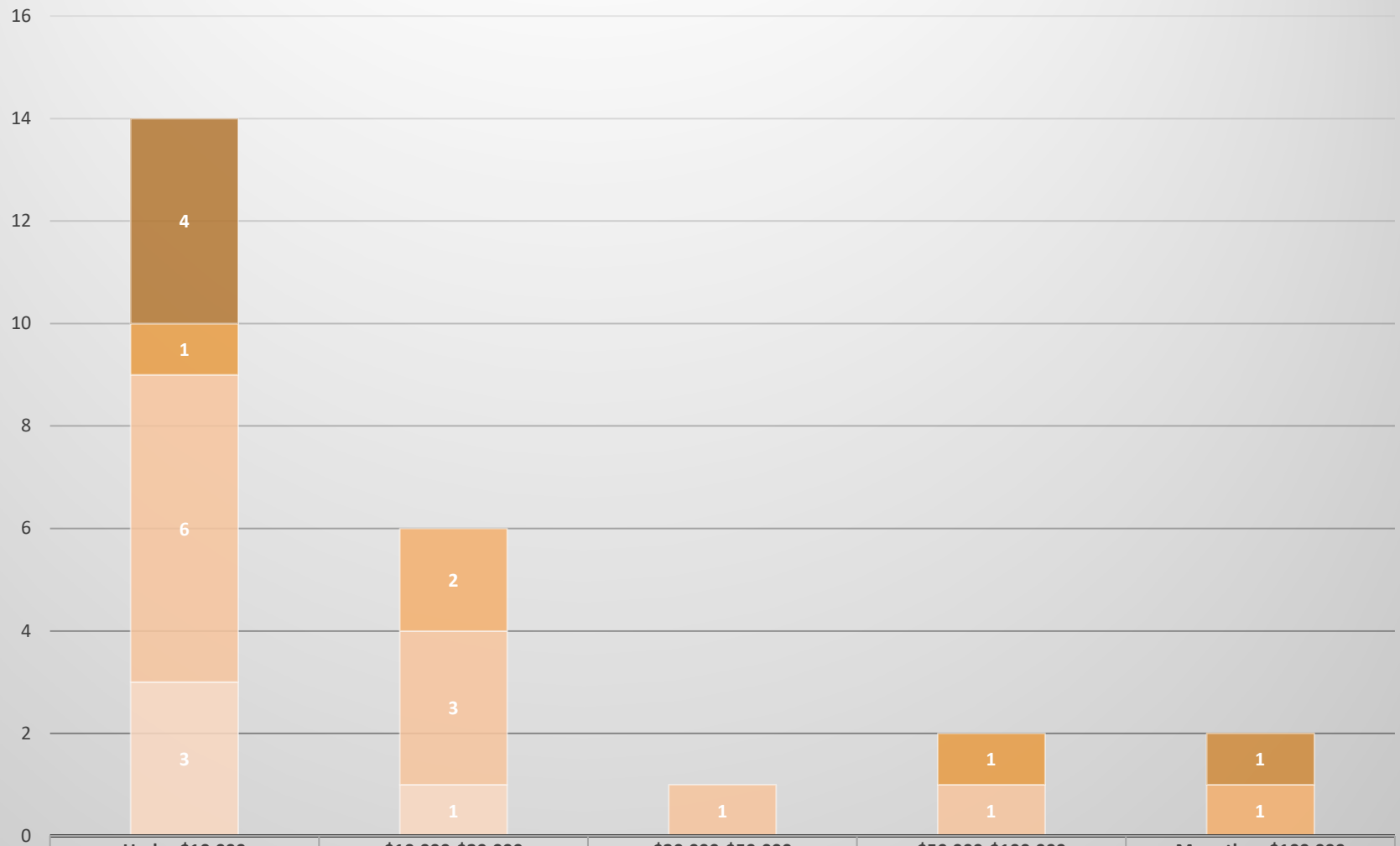
## Q10.1 What would be the initial costs associated with implementing the proposed recordkeeping requirements? (25 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM	2				
\$50 billion to under \$1 trillion RAUM	3	1		1	1
\$20 billion to under \$50 billion RAUM		1			1
\$10 billion to under \$20 billion RAUM		3	1	1	
\$1 billion to under \$10 billion RAUM	5	3	1	1	
\$500 million to under \$1 billion RAUM	2	1			
Under \$500 million RAUM	2				

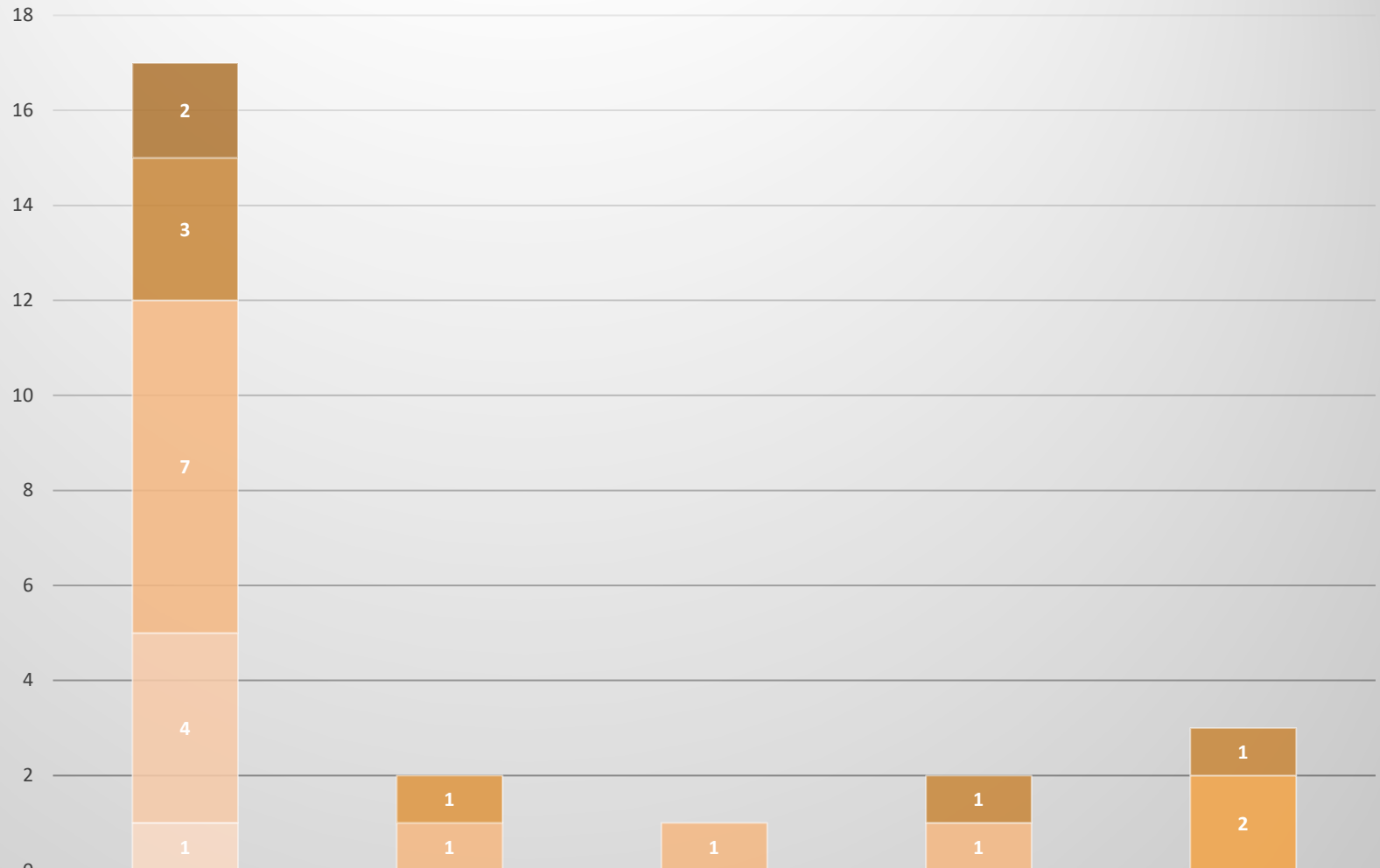


## Q10.1 What would be the ongoing annual costs associated with implementing the proposed requirements of regulatory reporting of cybersecurity incidents? (25 Responses)



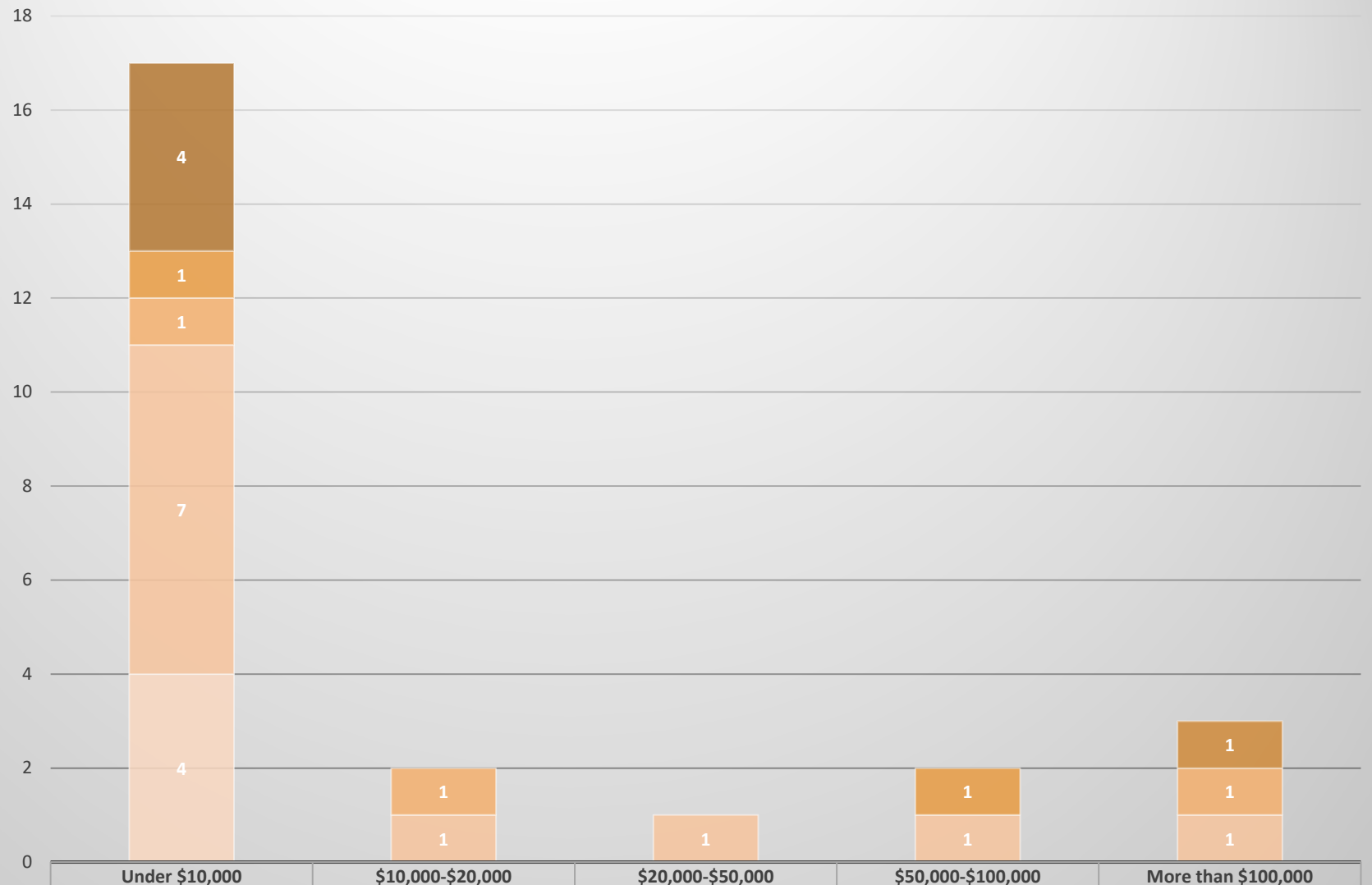
	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	4				
501 to 1000 employees					1
251 to 500 employees	1			1	
51 to 250 employees		2			1
11 to 50 employees	6	3	1	1	
6 to 10 employees	3	1			

## Q10.2 What would be the ongoing annual costs associated with implementing the proposed recordkeeping requirements? (25 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
Over \$1 trillion RAUM	2				
\$50 billion to under \$1 trillion RAUM	3			1	1
\$20 billion to under \$50 billion RAUM		1			
\$10 billion to under \$20 billion RAUM					2
\$1 billion to under \$10 billion RAUM	7	1	1	1	
\$500 million to under \$1 billion RAUM	4				
Under \$500 million RAUM	1				

## Q10.2 What would be the ongoing annual costs associated with implementing the proposed recordkeeping requirements? (25 Responses)



	Under \$10,000	\$10,000-\$20,000	\$20,000-\$50,000	\$50,000-\$100,000	More than \$100,000
More than 1,000 employees	4				
501 to 1000 employees					1
251 to 500 employees	1			1	
51 to 250 employees	1	1			1
11 to 50 employees	7	1	1	1	1
6 to 10 employees	4				