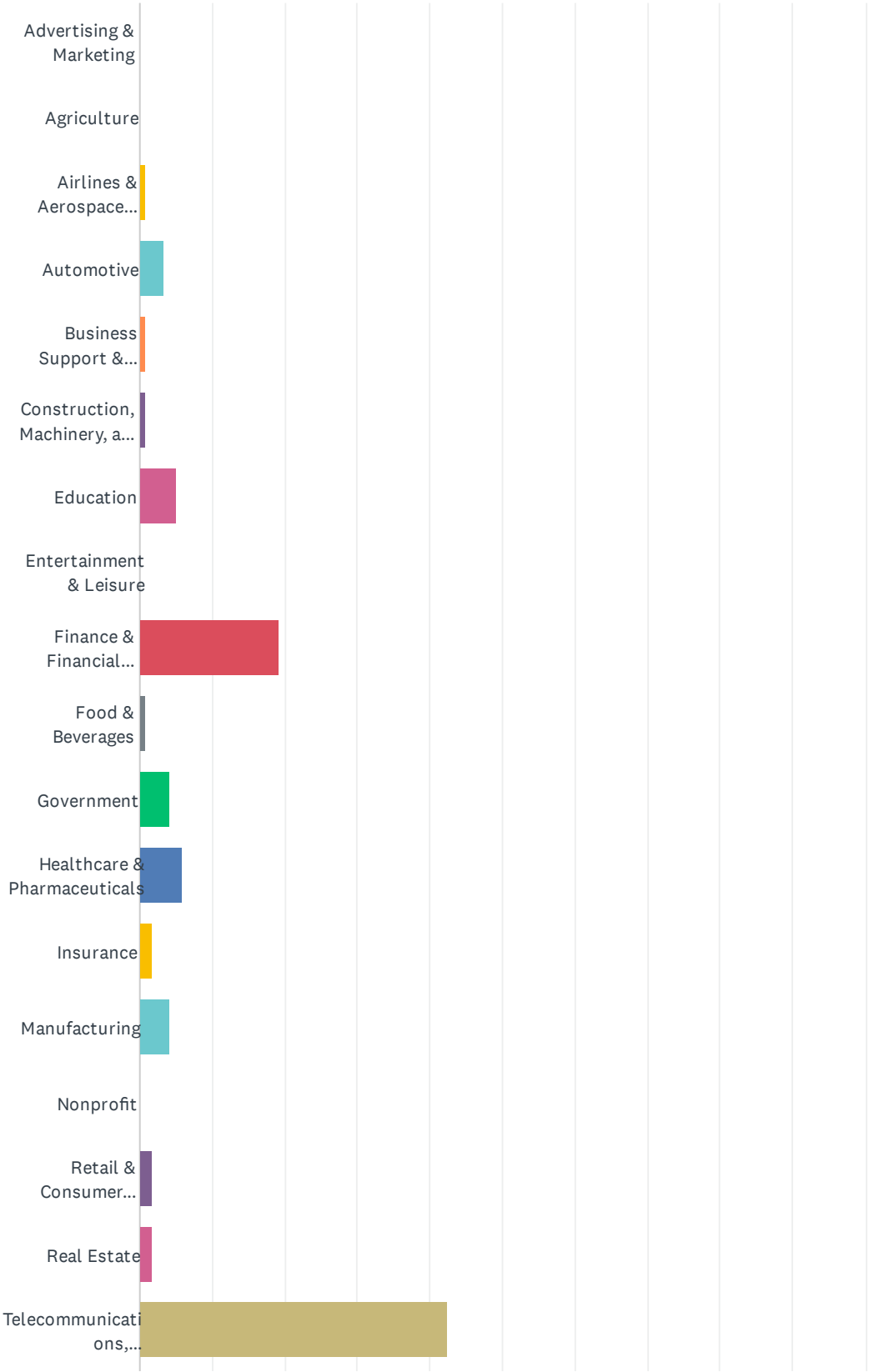
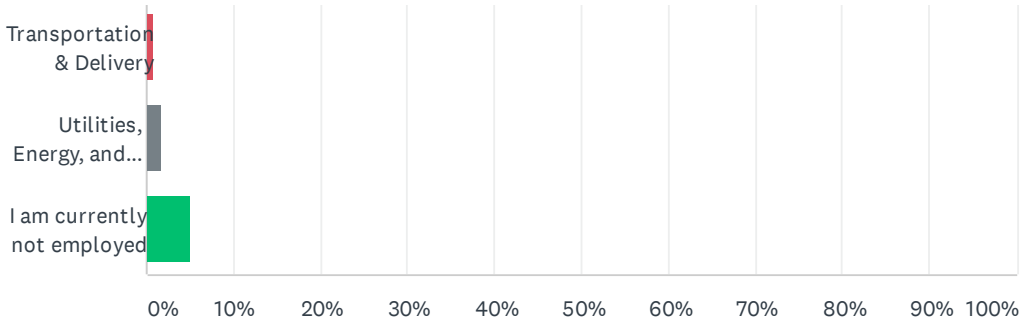
Q1 Which of the following best describes the principal industry of your organization?

Answered: 120 Skipped: 0

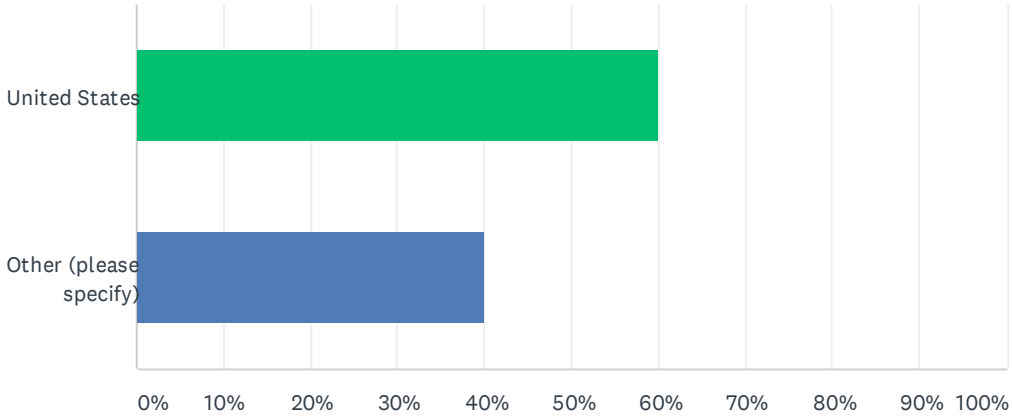




ANSWER CHOICES	RESPONSES	
Advertising & Marketing	0.00%	0
Agriculture	0.00%	0
Airlines & Aerospace (including Defense)	0.83%	1
Automotive	3.33%	4
Business Support & Logistics	0.83%	1
Construction, Machinery, and Homes	0.83%	1
Education	5.00%	6
Entertainment & Leisure	0.00%	0
Finance & Financial Services	19.17%	23
Food & Beverages	0.83%	1
Government	4.17%	5
Healthcare & Pharmaceuticals	5.83%	7
Insurance	1.67%	2
Manufacturing	4.17%	5
Nonprofit	0.00%	0
Retail & Consumer Durables	1.67%	2
Real Estate	1.67%	2
Telecommunications, Technology, Internet & Electronics	42.50%	51
Transportation & Delivery	0.83%	1
Utilities, Energy, and Extraction	1.67%	2
I am currently not employed	5.00%	6
TOTAL		120

Q2 In what country do you currently reside?

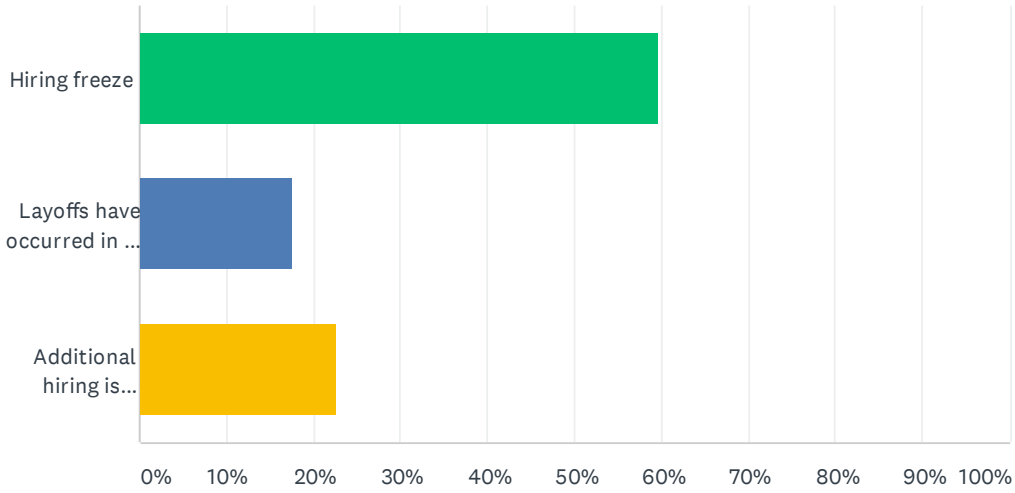
Answered: 120 Skipped: 0



ANSWER CHOICES	RESPONSES	
United States	60.00%	72
Other (please specify)	40.00%	48
TOTAL		120

Q3 What is the impact on your company's cybersecurity staffing as a result of COVID-19?

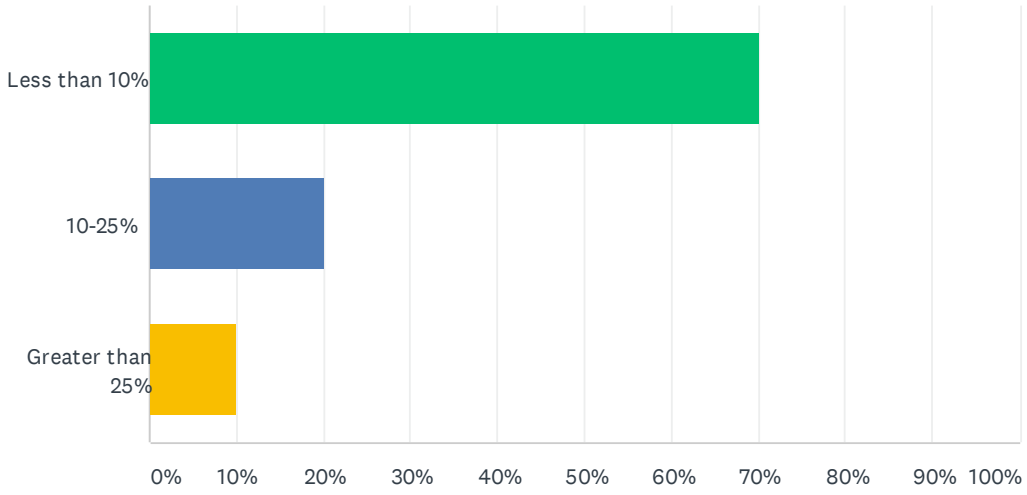
Answered: 119 Skipped: 1



ANSWER CHOICES	RESPONSES	
Hiring freeze	59.66%	71
Layoffs have occurred in the cybersecurity department	17.65%	21
Additional hiring is happening in the cybersecurity department	22.69%	27
TOTAL		119

Q4 If you reported layoffs in the previous question, what is the approximate percentage of the cybersecurity staff that was laid off?

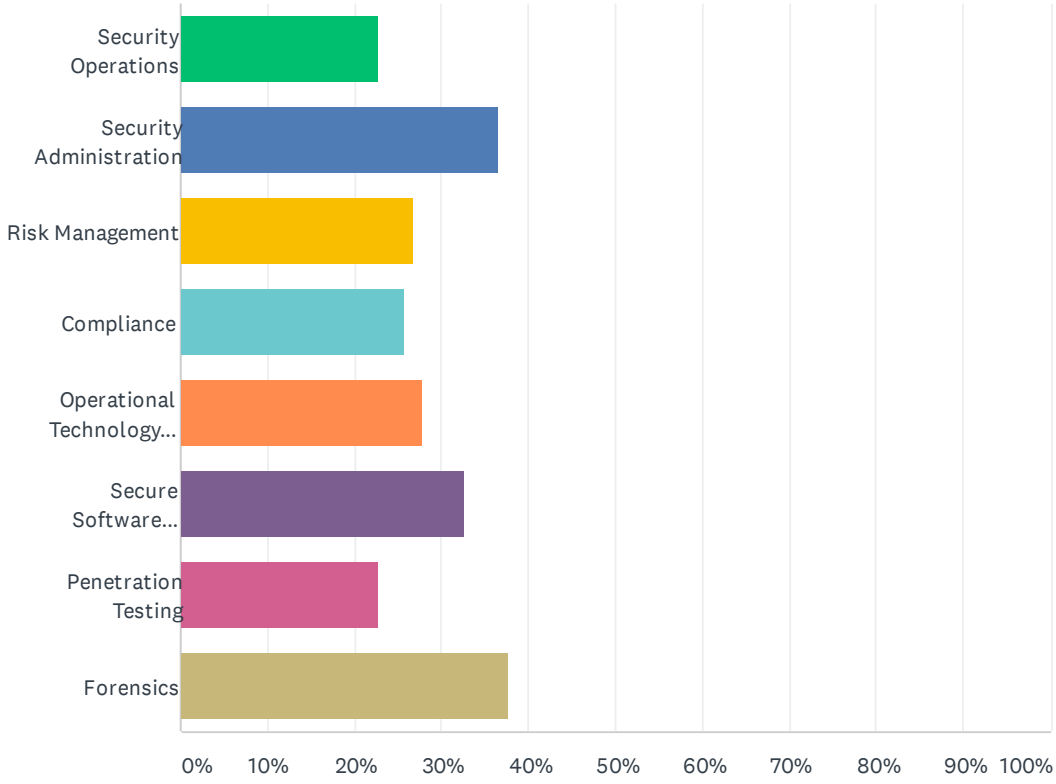
Answered: 60 Skipped: 60



ANSWER CHOICES	RESPONSES	
Less than 10%	70.00%	42
10-25%	20.00%	12
Greater than 25%	10.00%	6
TOTAL		60

Q5 In the event of a prolonged economic downturn, which cybersecurity roles do you anticipate are most likely to be reduced in your organization? Select up to 3 maximum (roles source ISC2 2019 Workforce Study)

Answered: 101 Skipped: 19



ANSWER CHOICES	RESPONSES	
Security Operations	22.77%	23
Security Administration	36.63%	37
Risk Management	26.73%	27
Compliance	25.74%	26
Operational Technology Security	27.72%	28
Secure Software Development	32.67%	33
Penetration Testing	22.77%	23
Forensics	37.62%	38
Total Respondents: 101		

Q6 For cybersecurity staff not impacted directly by layoffs, what do you anticipate the biggest challenges will be for the remainder of 2020 as a result of budget reductions of freezes?

Answered: 102 Skipped: 18

Accelerated work by third party vendors and consultants who have no clue about our company's policies and procedures. And increasing concentration of knowledge with vendors instead of our own staff.

Organization will opt to reduce CyberSec budget as they are towards more to Productivity due to financial pressure.

I believe that layoffs are coming, just later in the year.

Retention of best people- we've had salary cuts so some are already seeking other opportunities; cuts in funding for key projects; aggressive cost cutting up to and including having to fight for foundational security controls and cyber hygiene now considered optional.

Home office will be permanent and we will need increase security with the same budget.

Gov/Mil hiring continues unabated, as does federal contractors with contract awards that need hiring needs met. However, new-start projects are slowed or halted which could affect mid-term staffing decisions. Mil service members transitioning to the private sector are finding their choices limited during hiring freezes, although recruiters/HR appear to maintain a healthy interest in finding suitable candidates for an anticipated re-opening.

Increased work load without an increase in staffing.

With the Pandemic distractions and the increase in malicious activity, it seems there will be more incidents and preventing them is our primary focus now...

Evaluating and implementing open source alternatives for commercial software tools in our security stack.

1). Attackers using COVID as an opportunity to craft nifty social engineering attacks 2). Budget freeze may inhibit future cybersecurity investments 3). Potential resource capacity issues with cloud service providers.

1) Double whammy of IR35 legislation in the UK. 2) budgets for security will be cut more than other functions as CxO still think security is non essential 3) skills will denature or go offshore providing a perfect target rich environment for crime.

Dramatic increases in attacks from all quarters. "Never let a crisis go to waste", cyber criminals.

Budget cuts, longer work hours.