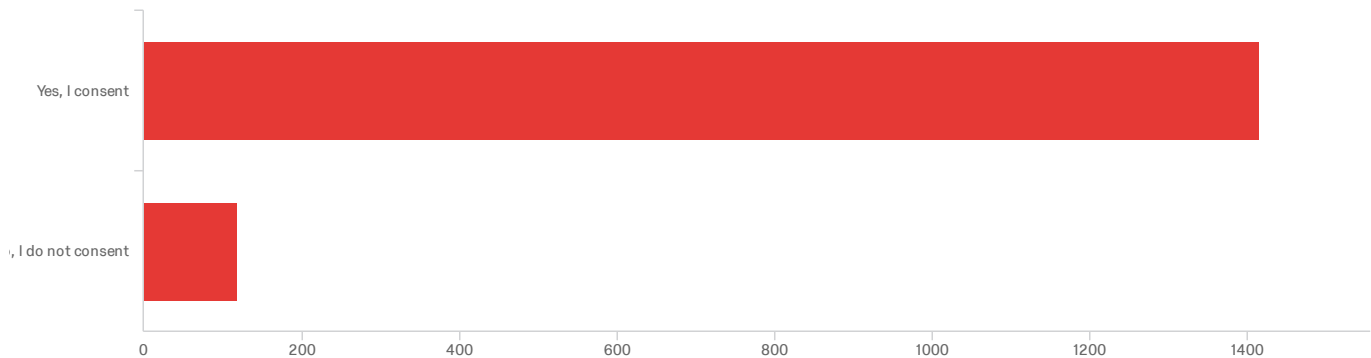


# FBI-UNG Georgia Cyber Threat Survey 2020

A joint effort of the FBI Atlanta Computer Intrusion Squad and the University of North Georgia's Center for Cyber Operations Education October 2019

## Consent



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Click Yes to take the survey. Click no to end the survey.	1.00	2.00	1.08	0.27	0.07	1,533

#	Field	Choice Count
1	Yes, I consent	92.30% 1415
2	No, I do not consent	7.70% 118

1533

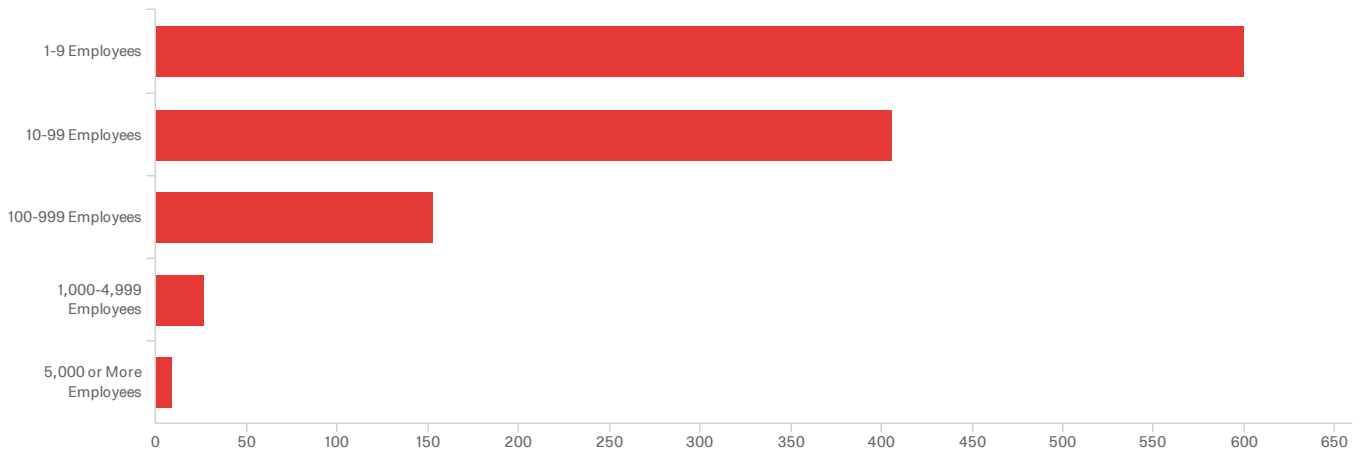
Showing rows 1 - 3 of 3

### Cite as:

Payne, B.R., Robertson, C.L., Reinking, M., Krone, M.E., Abegaz, T.T., Mienie, E.L., Orr, D.A., Hamilton, S. (2020). FBI-UNG Georgia Cyber Threat Survey 2020 [Research white paper]. University of North Georgia. 2020. <http://www.ung.edu/cyber/survey>

If you need this form in an alternate format for accessibility purposes (e.g. Braille, large print, audio, etc.), please contact Kimberly Bruner by email at [kimberly.bruner@ung.edu](mailto:kimberly.bruner@ung.edu) or call 706-867-2189.

Q1 - Choose the answer that best describes the size of your organization.

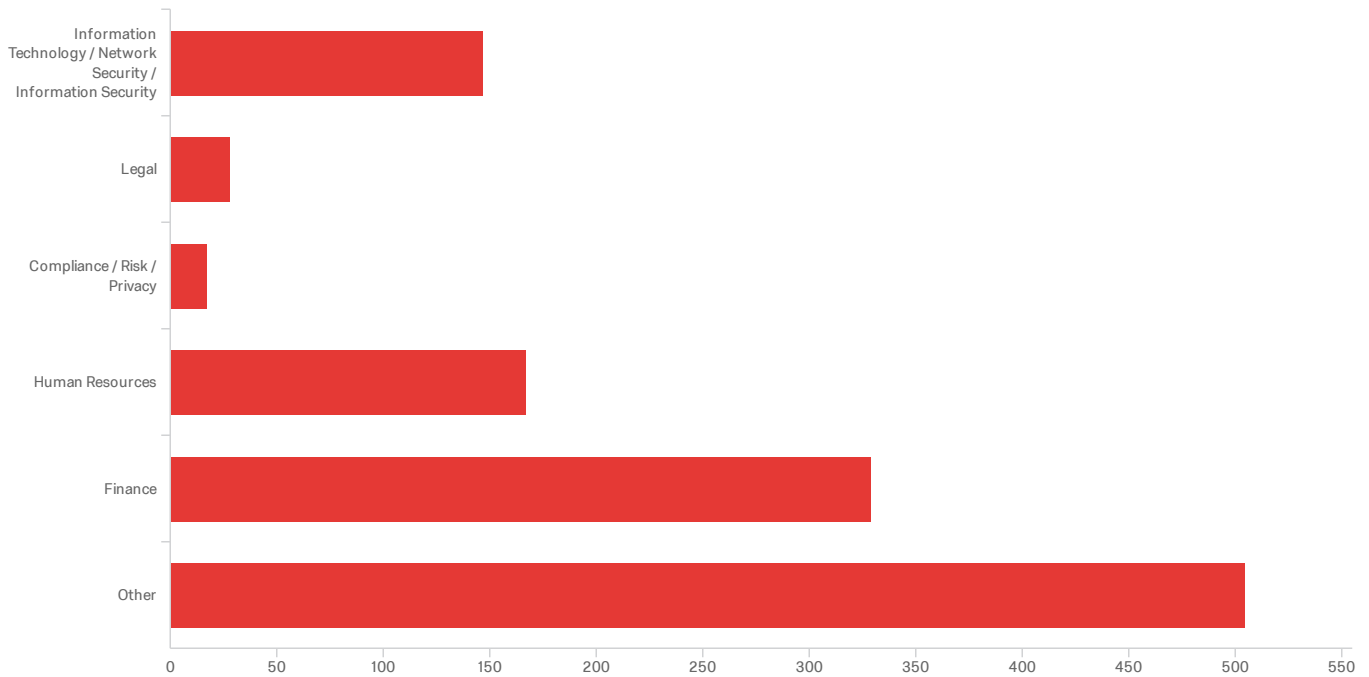


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Choose the answer that best describes the size of your organization.	1.00	5.00	1.69	0.83	0.69	1,195

#	Field	Choice Count
1	1-9 Employees	50.21% 600
2	10-99 Employees	33.97% 406
3	100-999 Employees	12.80% 153
4	1,000-4,999 Employees	2.26% 27
5	5,000 or More Employees	0.75% 9
		1195

Showing rows 1 - 6 of 6

# 1a - Which option best describes your role in the organization?



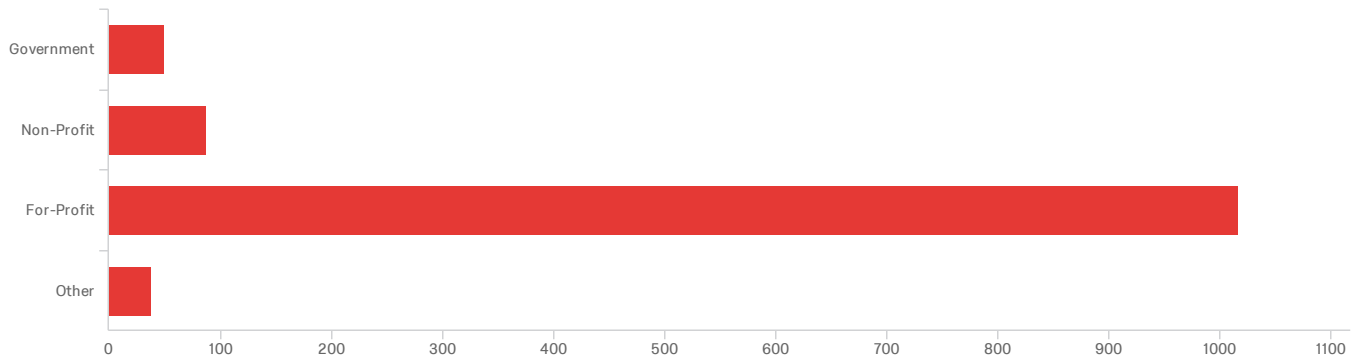
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which option best describes your role in the organization? - Selected Choice	1.00	6.00	4.69	1.65	2.71	1,193

#	Field	Choice Count
1	Information Technology / Network Security / Information Security	12.32% 147
2	Legal	2.35% 28
3	Compliance / Risk / Privacy	1.42% 17
4	Human Resources	14.00% 167
5	Finance	27.58% 329
6	Other	42.33% 505

1193

Showing rows 1 - 7 of 7

## 1b - Which term best describes your organization?



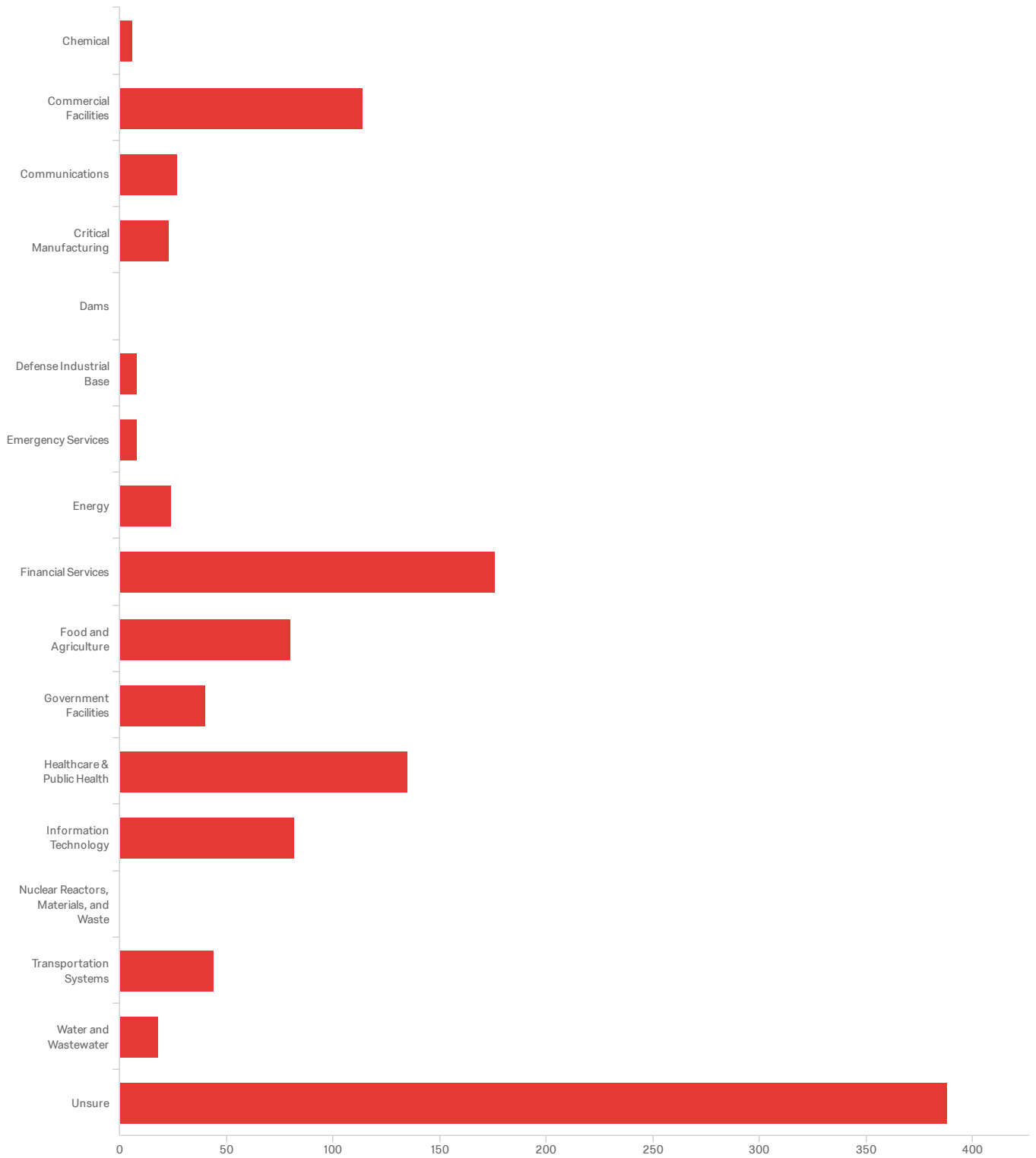
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which term best describes your organization? - Selected Choice	1.00	4.00	2.87	0.51	0.26	1,192

#	Field	Choice Count
1	Government	4.19% 50
2	Non-Profit	7.38% 88
3	For-Profit	85.23% 1016
4	Other	3.19% 38

1192

Showing rows 1 - 5 of 5

## Q2 - Which critical infrastructure sector best describes your organization?



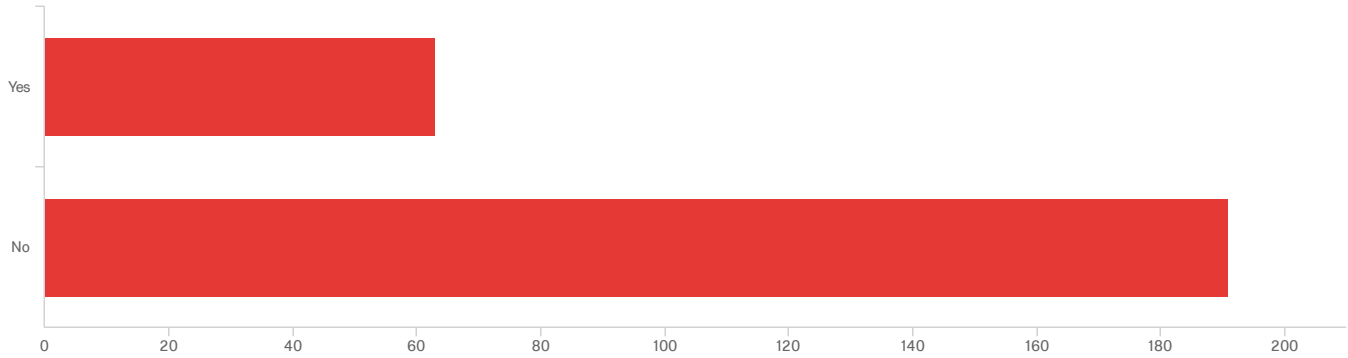
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
---	-------	---------	---------	------	---------------	----------	-------

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which critical infrastructure sector best describes your organization?	17.00	34.00	28.06	5.33	28.42	1,173

#	Field	Choice Count
1	Chemical	0.51% 6
2	Commercial Facilities	9.72% 114
3	Communications	2.30% 27
4	Critical Manufacturing	1.96% 23
5	Dams	0.00% 0
6	Defense Industrial Base	0.68% 8
7	Emergency Services	0.68% 8
8	Energy	2.05% 24
9	Financial Services	15.00% 176
10	Food and Agriculture	6.82% 80
11	Government Facilities	3.41% 40
12	Healthcare & Public Health	11.51% 135
13	Information Technology	6.99% 82
14	Nuclear Reactors, Materials, and Waste	0.00% 0
15	Transportation Systems	3.75% 44
16	Water and Wastewater	1.53% 18
17	Unsure	33.08% 388
		1173

Showing rows 1 - 18 of 18

2c - If your organization uses ICS/SCADA (industrial control systems), can users remotely access your organization's ICS/SCADA systems & network?



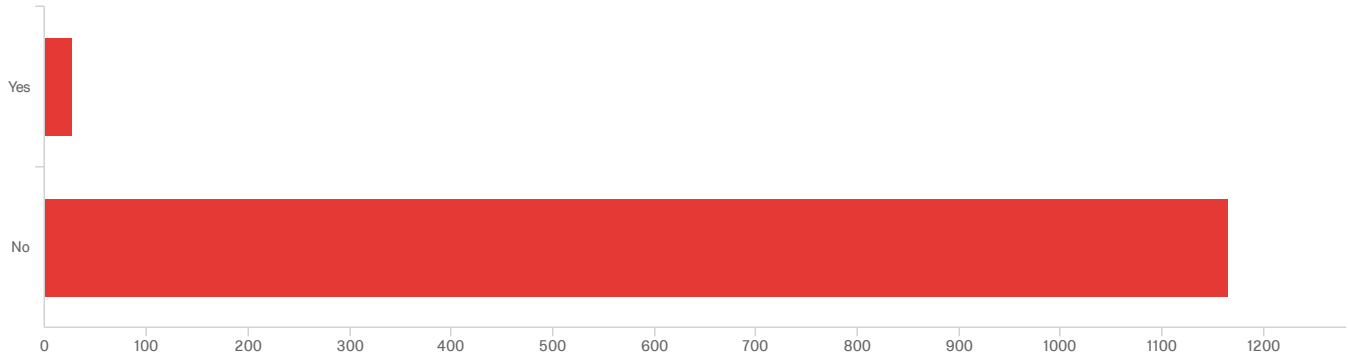
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	If your organization uses ICS/SCADA (industrial control systems), can users remotely access your organization's ICS/SCADA systems & network?	1.00	2.00	1.75	0.43	0.19	254

#	Field	Choice Count
1	Yes	24.80% 63
2	No	75.20% 191

254

Showing rows 1 - 3 of 3

2f - Does your organization have any joint partnerships with foreign companies or laboratories?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Does your organization have any joint partnerships with foreign companies or laboratories?	1.00	2.00	1.98	0.15	0.02	1,193

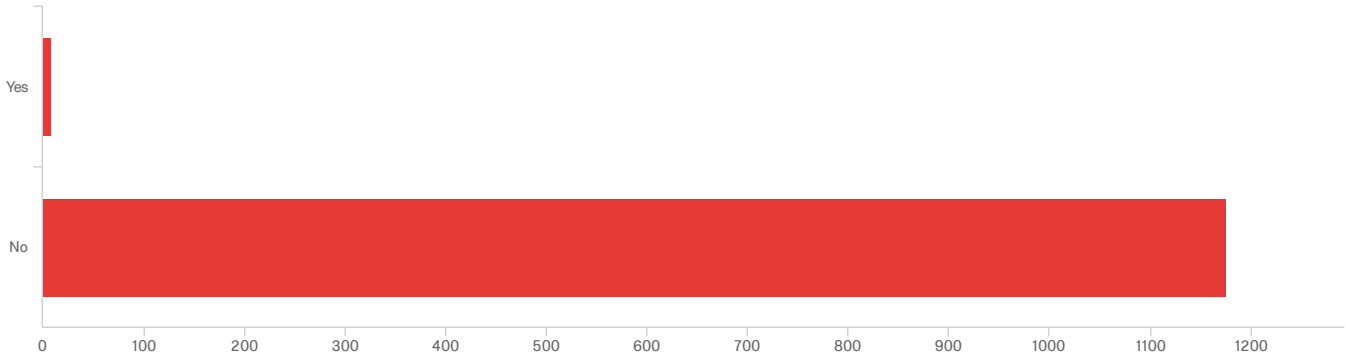
#	Field	Choice Count
1	Yes	2.26% 27
2	No	97.74% 1166

1193

Showing rows 1 - 3 of 3



## 2g - Does your organization have any joint partnerships with educational institutions overseas?



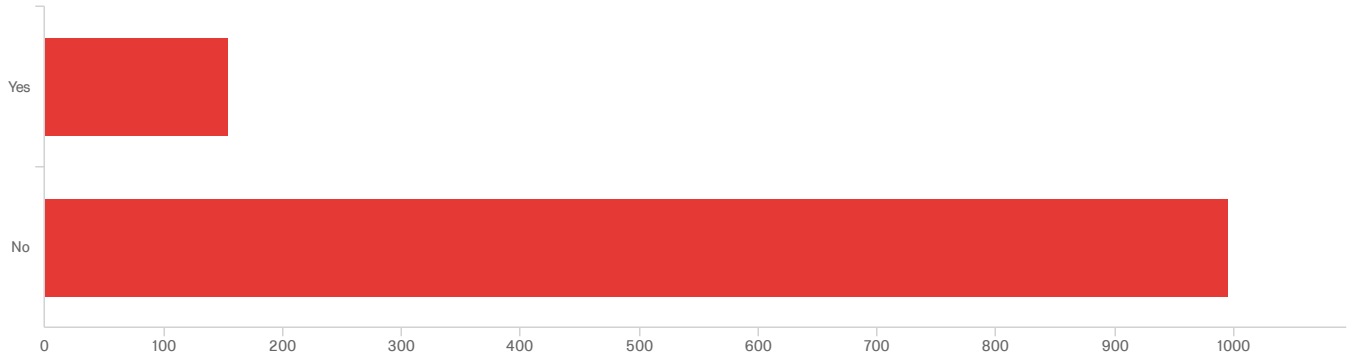
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Does your organization have any joint partnerships with educational institutions overseas?	1.00	2.00	1.99	0.08	0.01	1,184

#	Field	Choice Count
1	Yes	0.68% 8
2	No	99.32% 1176

1184

Showing rows 1 - 3 of 3

## 2h - Does your organization have Internet of Things (IoT) devices integrated into your environment?



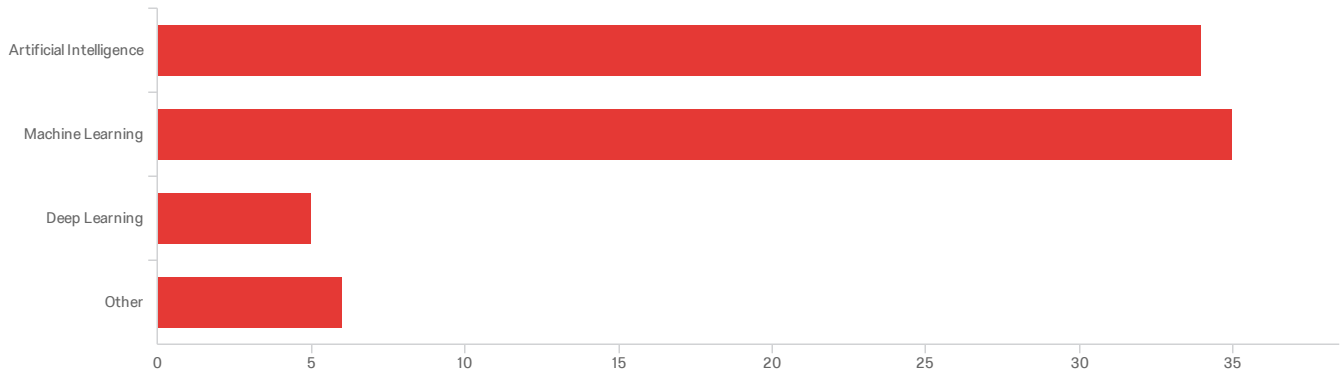
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Does your organization have Internet of Things (IoT) devices integrated into your environment?	1.00	2.00	1.87	0.34	0.12	1,150

#	Field	Choice Count
1	Yes	13.39% 154
2	No	86.61% 996

1150

Showing rows 1 - 3 of 3

2i - Does your organization utilize any of the following automation techniques? (Choose all that apply)

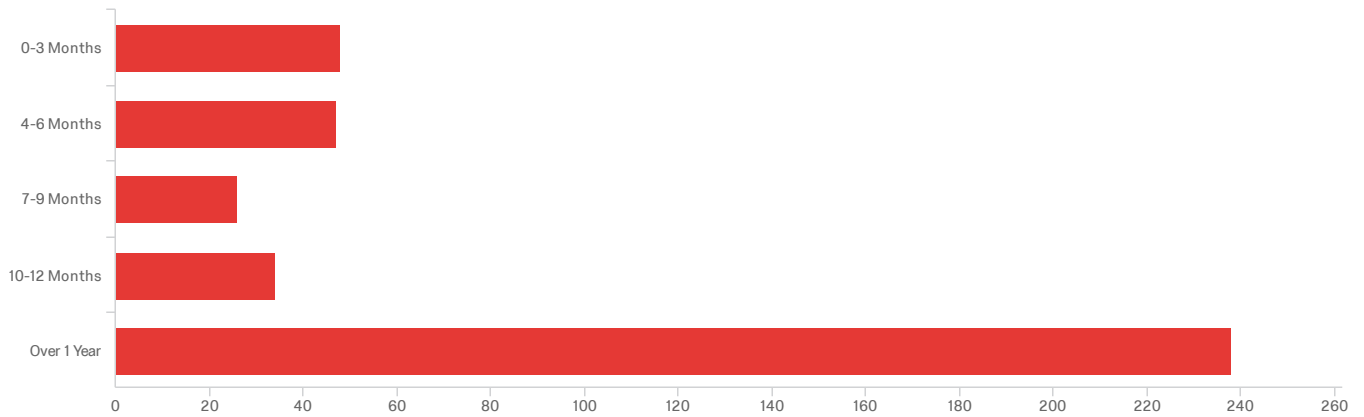


#	Field	Choice Count
1	Artificial Intelligence	42.50% 34
2	Machine Learning	43.75% 35
3	Deep Learning	6.25% 5
4	Other	7.50% 6

80

Showing rows 1 - 5 of 5

## Q5 - How recent was your last computer compromise?



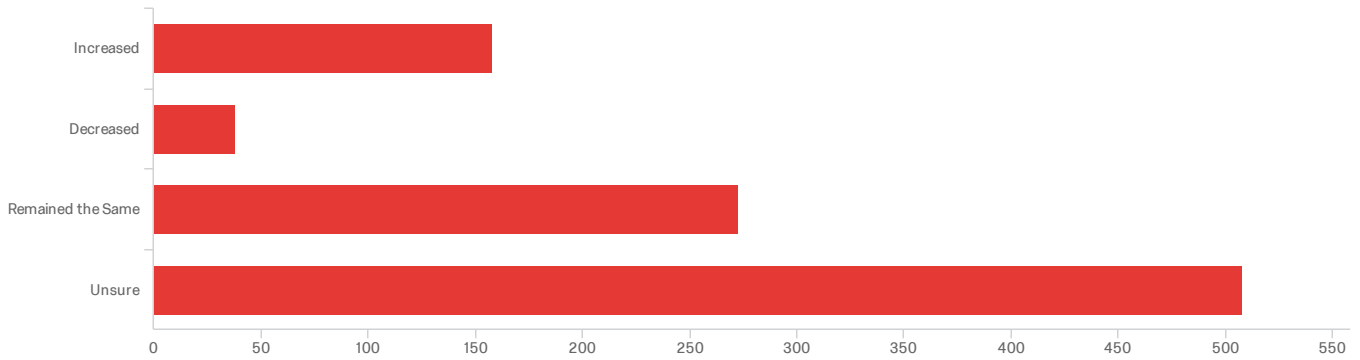
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	How recent was your last computer compromise?	1.00	5.00	3.93	1.50	2.24	393

#	Field	Choice Count
1	0-3 Months	12.21% 48
2	4-6 Months	11.96% 47
3	7-9 Months	6.62% 26
4	10-12 Months	8.65% 34
5	Over 1 Year	60.56% 238
		393

Showing rows 1 - 6 of 6

## Q7 - Over the past 12 months, have the number of cyberattacks targeting your

organization:

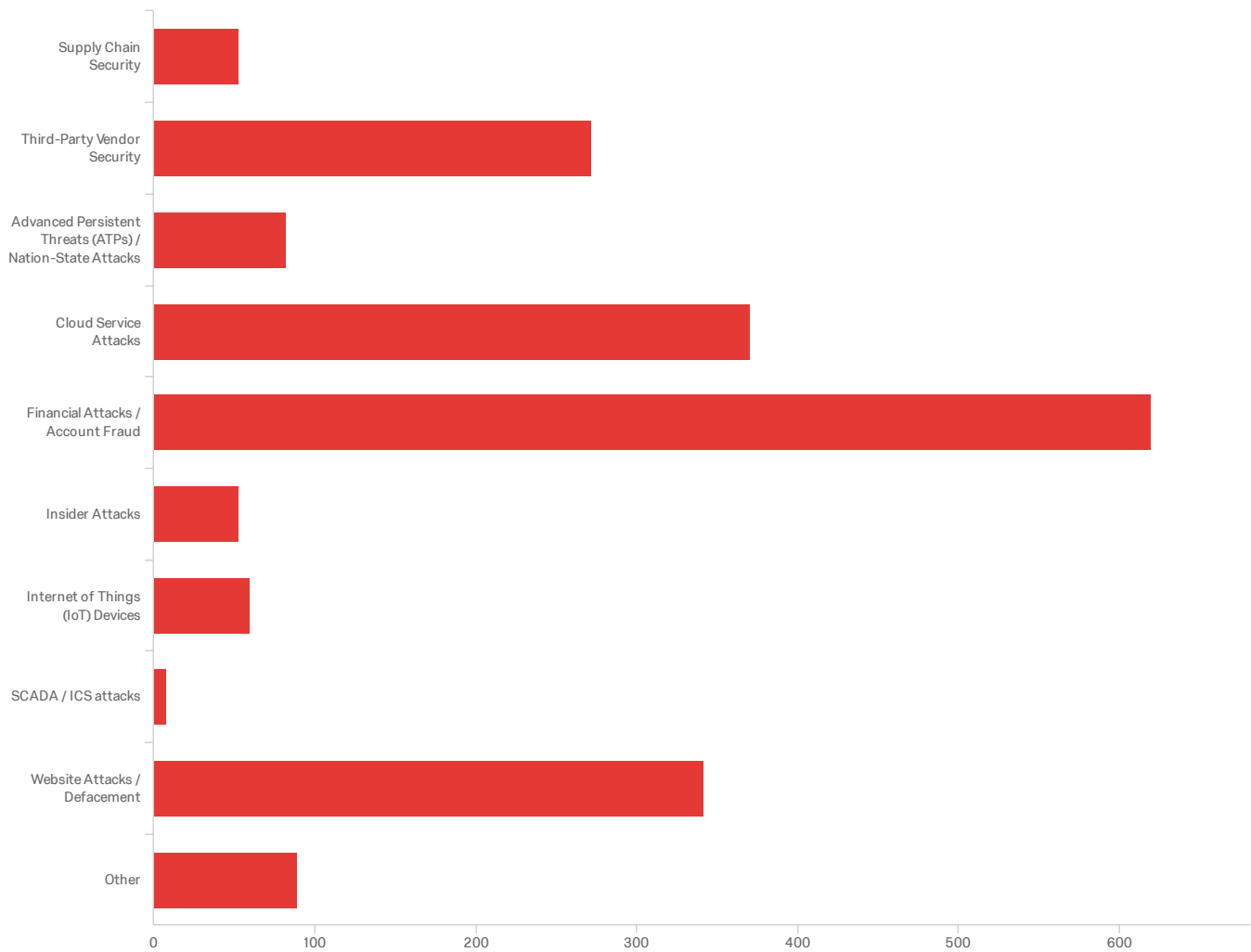


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Over the past 12 months, have the number of cyberattacks targeting your organization:	1.00	5.00	2.47	0.90	0.81	977

#	Field	Choice Count
1	Increased	16.17% 158
2	Decreased	3.89% 38
3	Remained the Same	27.94% 273
4	Unsure	52.00% 508
		977

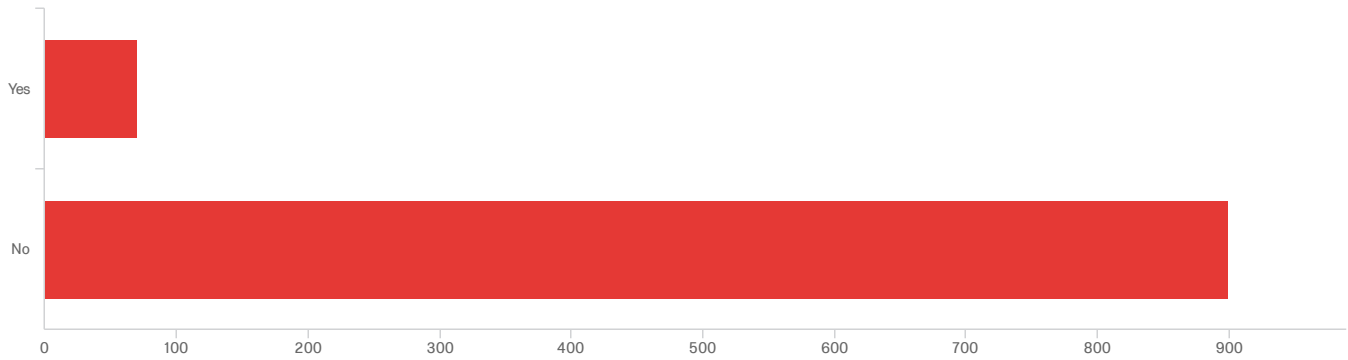
Showing rows 1 - 5 of 5

## Q8 - What concerns you most over the next 12 months? (Choose no more than three)



#	Field	Choice Count
1	Supply Chain Security	2.72% 53
2	Third-Party Vendor Security	13.95% 272
3	Advanced Persistent Threats (ATPs) / Nation-State Attacks	4.21% 82
4	Cloud Service Attacks	19.03% 371
5	Financial Attacks / Account Fraud	31.79% 620
6	Insider Attacks	2.72% 53
7	Internet of Things (IoT) Devices	3.08% 60
8	SCADA / ICS attacks	0.41% 8
9	Website Attacks / Defacement	17.54% 342
10	Other	4.56% 89

Q11 - Have you gathered any positive intelligence from scanning, incidents, or breaches, even if handled in-house (e.g. IP addresses, domain names, email addresses, malware samples, etc), that you are willing to share with law enforcement?

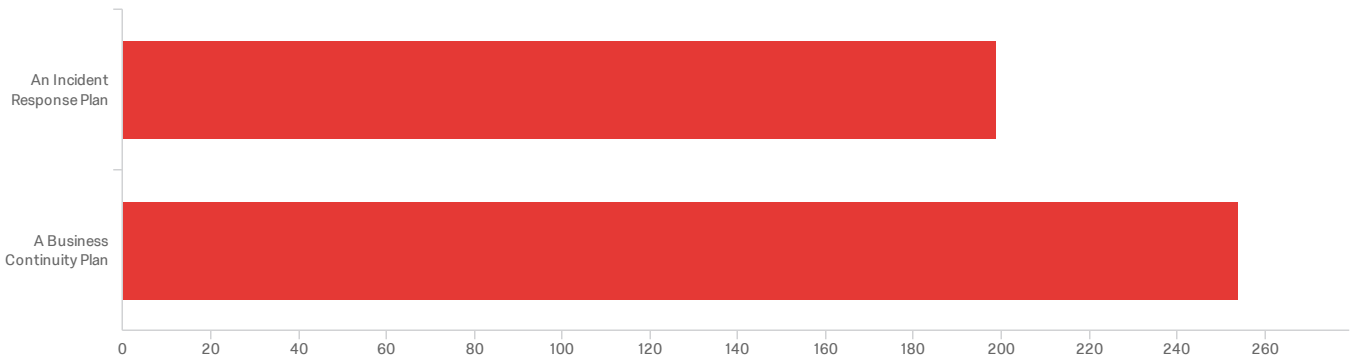


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Have you gathered any positive intelligence from scanning, incidents, or breaches, even if handled in-house (e.g. IP addresses, domain names, email addresses, malware samples, etc), that you are willing to share with law enforcement?	1.00	2.00	1.93	0.26	0.07	970

#	Field	Choice Count
1	Yes	7.22% 70
2	No	92.78% 900
		970

Showing rows 1 - 3 of 3

Q12 - Does your organization have: (Choose all that apply)



#	Field	Choice Count
1	An Incident Response Plan	43.93% 199
2	A Business Continuity Plan	56.07% 254

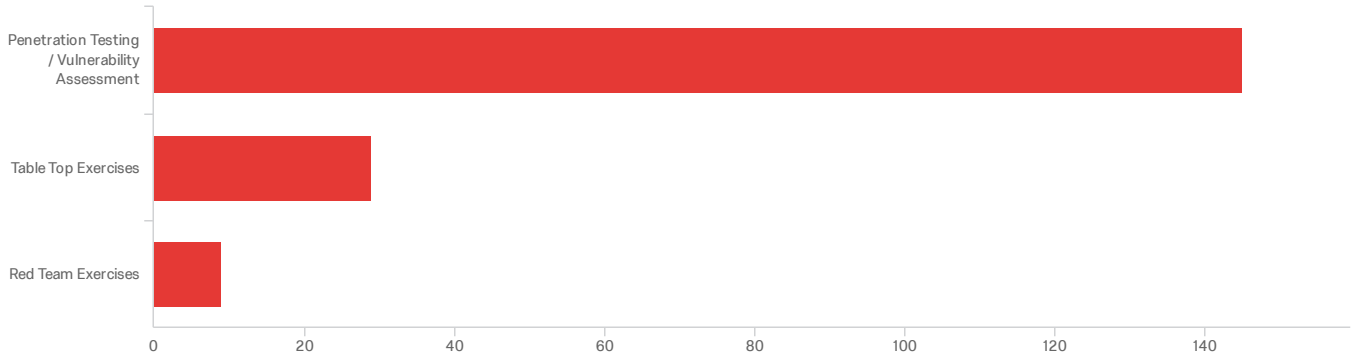
453

Showing rows 1 - 3 of 3



Q13 - Which of the following techniques does your organization utilize to assess

cybersecurity / cyberattack readiness? (Choose all that apply)

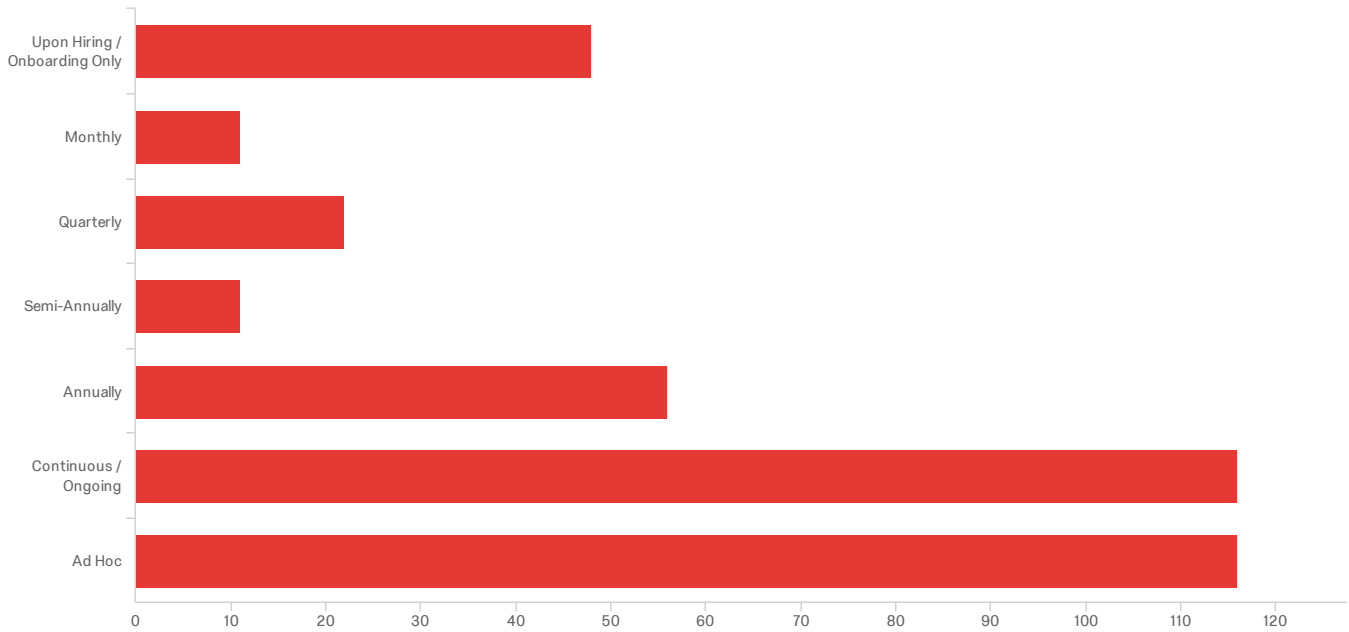


#	Field	Choice Count
1	Penetration Testing / Vulnerability Assessment	79.23% 145
2	Table Top Exercises	15.85% 29
3	Red Team Exercises	4.92% 9
		183

Showing rows 1 - 4 of 4

# Q14 - Which answer best describes how often your organization provides cybersecurity

awareness training?



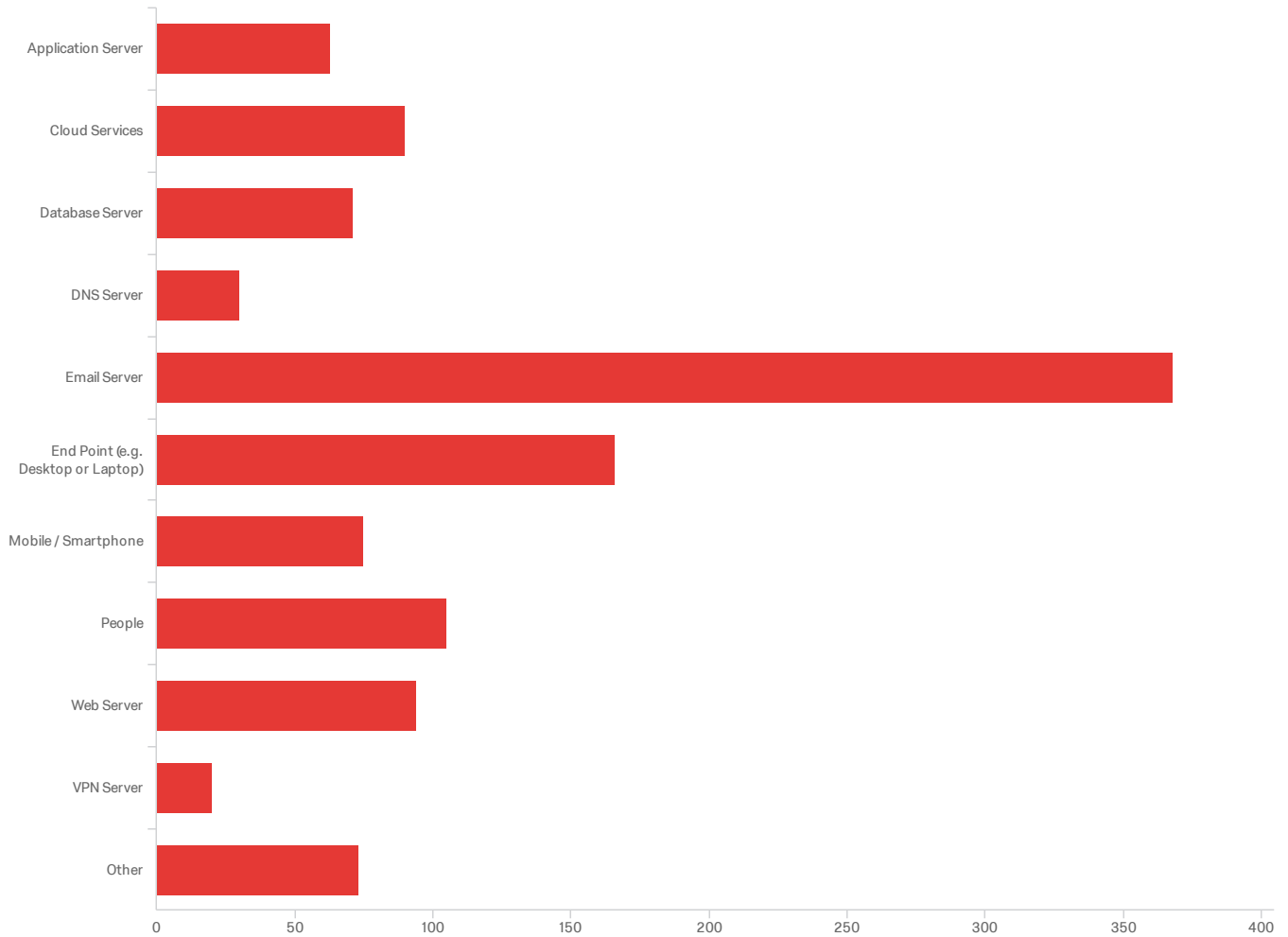
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which answer best describes how often your organization provides cybersecurity awareness training? - Selected Choice	1.00	9.00	5.79	2.67	7.11	380

#	Field	Choice Count
1	Upon Hiring / Onboarding Only	12.63% 48
2	Monthly	2.89% 11
3	Quarterly	5.79% 22
4	Semi-Annually	2.89% 11
5	Annually	14.74% 56
6	Continuous / Ongoing	30.53% 116
9	Ad Hoc	30.53% 116
		380

Showing rows 1 - 8 of 8

## Q15 - Which parts of your organization's infrastructure are most frequently targeted?

(Choose your top three)

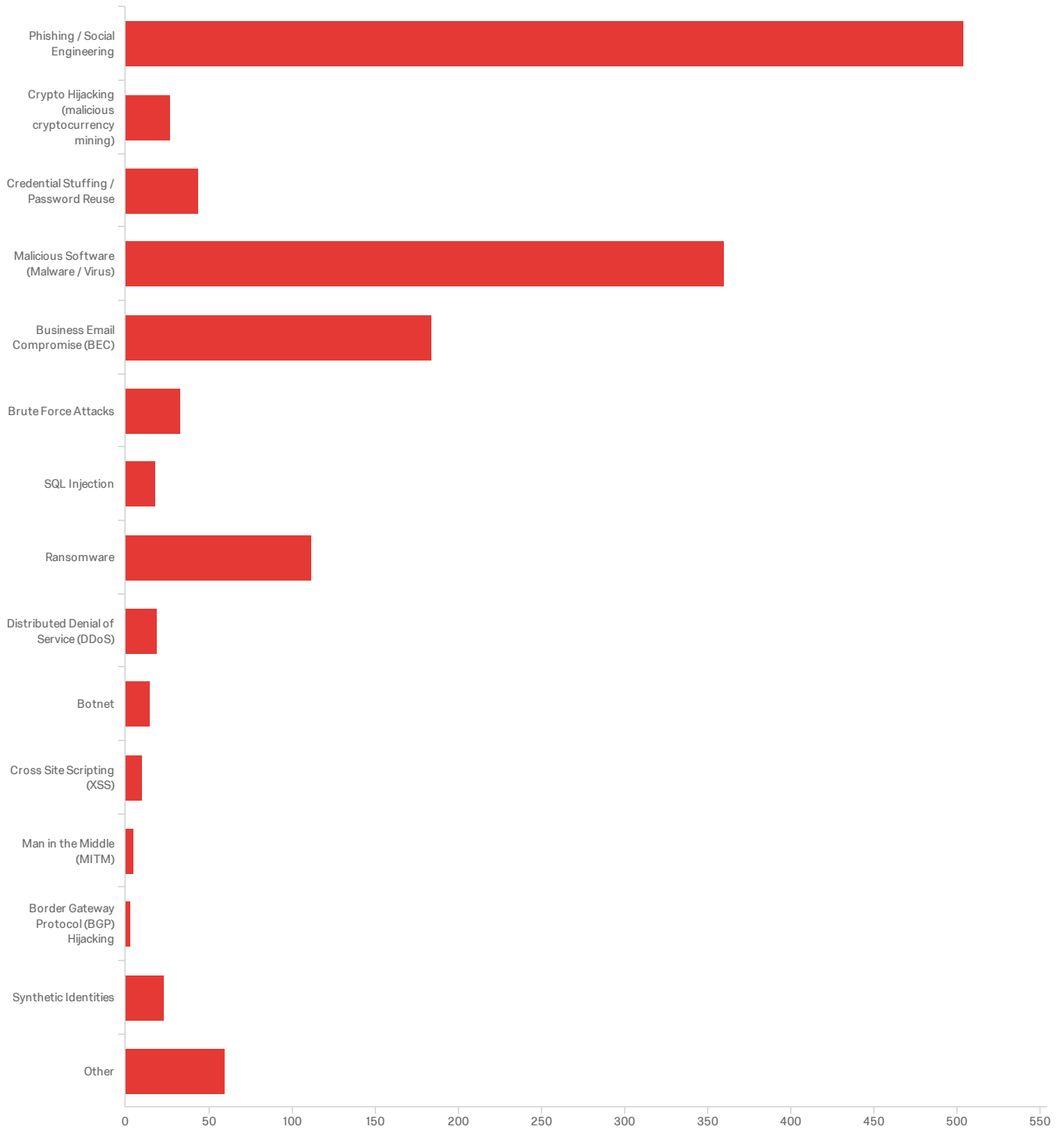


#	Field	Choice Count
1	Application Server	5.45% 63
2	Cloud Services	7.79% 90
3	Database Server	6.15% 71
4	DNS Server	2.60% 30
5	Email Server	31.86% 368
6	End Point (e.g. Desktop or Laptop)	14.37% 166
7	Mobile / Smartphone	6.49% 75
8	People	9.09% 105

#	Field	Choice Count
9	Web Server	8.14% 94
10	VPN Server	1.73% 20
11	Other	6.32% 73
		1155

Showing rows 1 - 12 of 12

Q16 - What type of cyberattacks most frequently target your organization? (Choose no more than five)



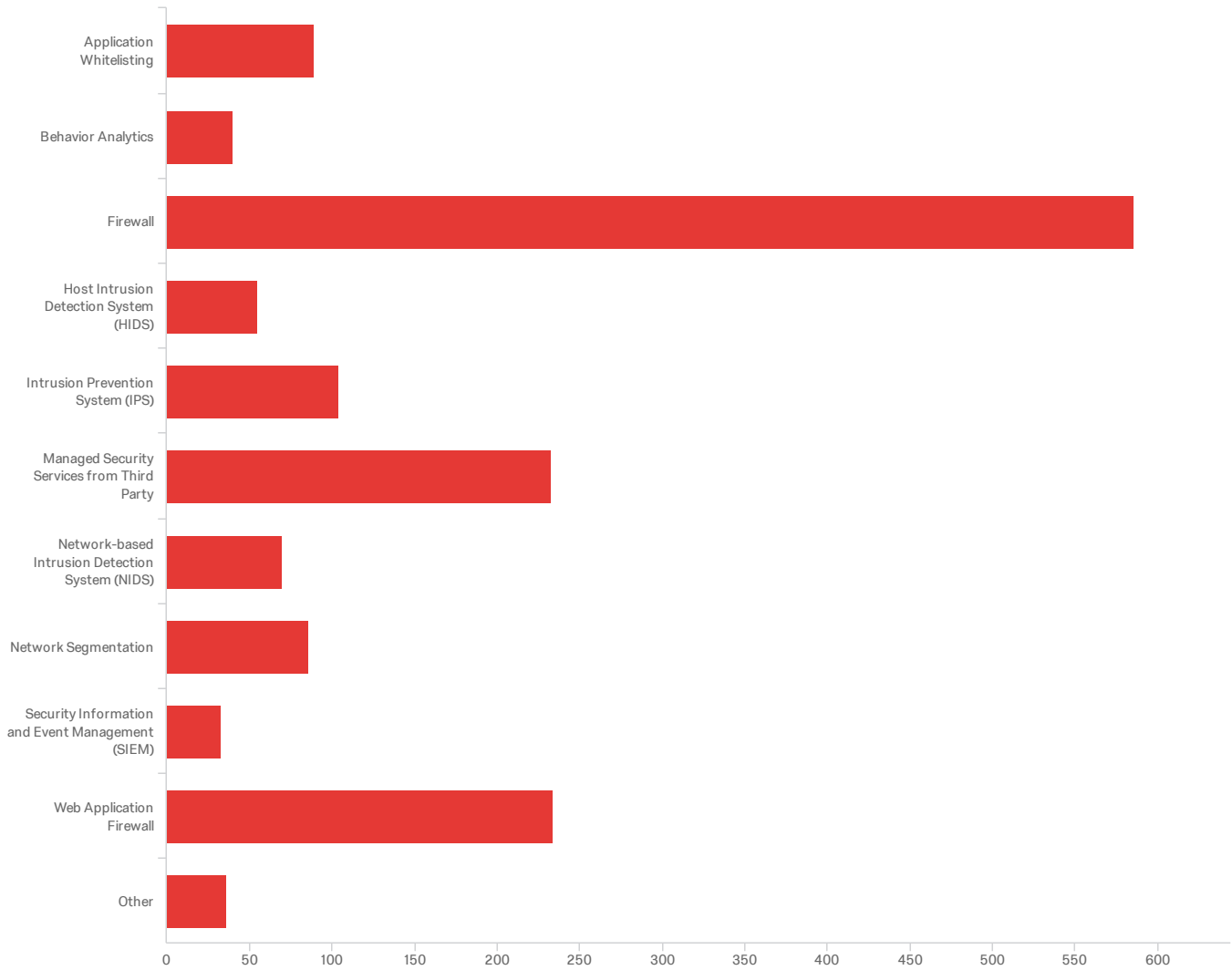
#	Field	Choice Count
1	Phishing / Social Engineering	35.57% 504

#	Field	Choice Count
2	Crypto Hijacking (malicious cryptocurrency mining)	1.91% 27
3	Credential Stuffing / Password Reuse	3.11% 44
4	Malicious Software (Malware / Virus)	25.41% 360
5	Business Email Compromise (BEC)	12.99% 184
6	Brute Force Attacks	2.33% 33
7	SQL Injection	1.27% 18
8	Ransomware	7.90% 112
9	Distributed Denial of Service (DDoS)	1.34% 19
10	Botnet	1.06% 15
11	Cross Site Scripting (XSS)	0.71% 10
12	Man in the Middle (MITM)	0.35% 5
13	Border Gateway Protocol (BGP) Hijacking	0.21% 3
14	Synthetic Identities	1.62% 23
15	Other	4.23% 60
		1417

Showing rows 1 - 16 of 16

## Q17 - Which of the following does your organization use to detect or prevent

cyberattacks? (Choose all that apply)



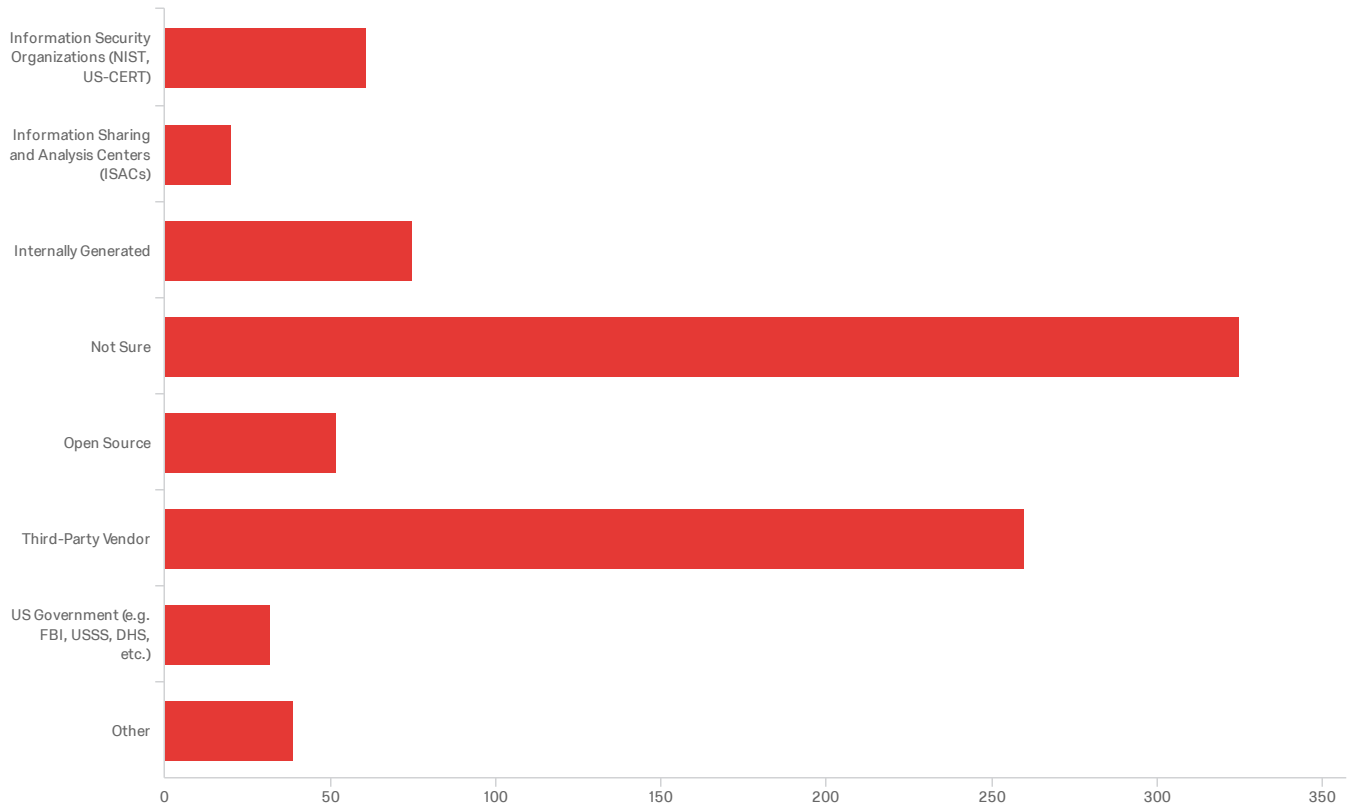
#	Field	Choice Count
1	Application Whitelisting	5.68% 89
2	Behavior Analytics	2.55% 40
3	Firewall	37.42% 586
4	Host Intrusion Detection System (HIDS)	3.51% 55
5	Intrusion Prevention System (IPS)	6.64% 104
6	Managed Security Services from Third Party	14.88% 233
7	Network-based Intrusion Detection System (NIDS)	4.47% 70

#	Field	Choice Count
8	Network Segmentation	5.49% 86
9	Security Information and Event Management (SIEM)	2.11% 33
10	Web Application Firewall	14.94% 234
12	Other	2.30% 36
		1566

Showing rows 1 - 12 of 12



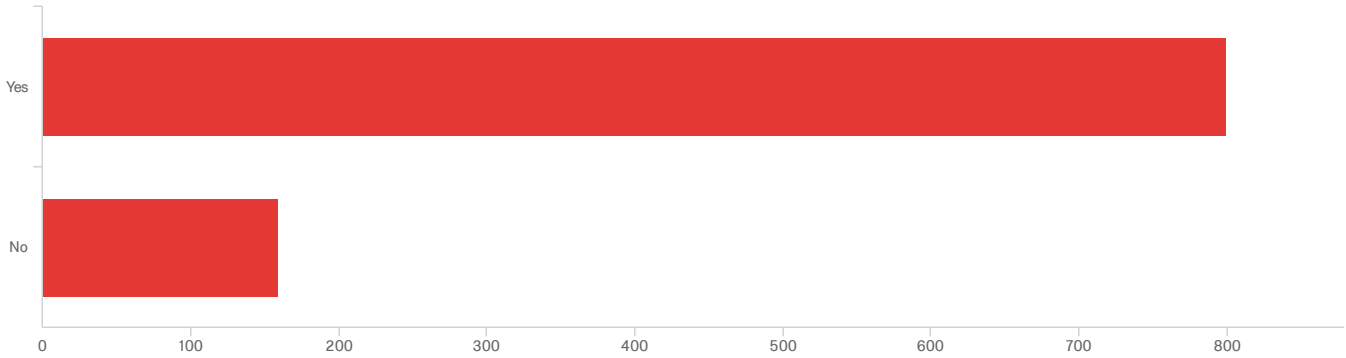
Q18 - What sources of cyberthreat intelligence does your organization use? (Choose all that apply)



#	Field	Choice Count
1	Information Security Organizations (NIST, US-CERT)	7.06% 61
2	Information Sharing and Analysis Centers (ISACs)	2.31% 20
3	Internally Generated	8.68% 75
4	Not Sure	37.62% 325
5	Open Source	6.02% 52
6	Third-Party Vendor	30.09% 260
7	US Government (e.g. FBI, USSS, DHS, etc.)	3.70% 32
8	Other	4.51% 39

864

Q36 - To the best of your knowledge, would your organization report a cyber-incident/  
breach to law enforcement?



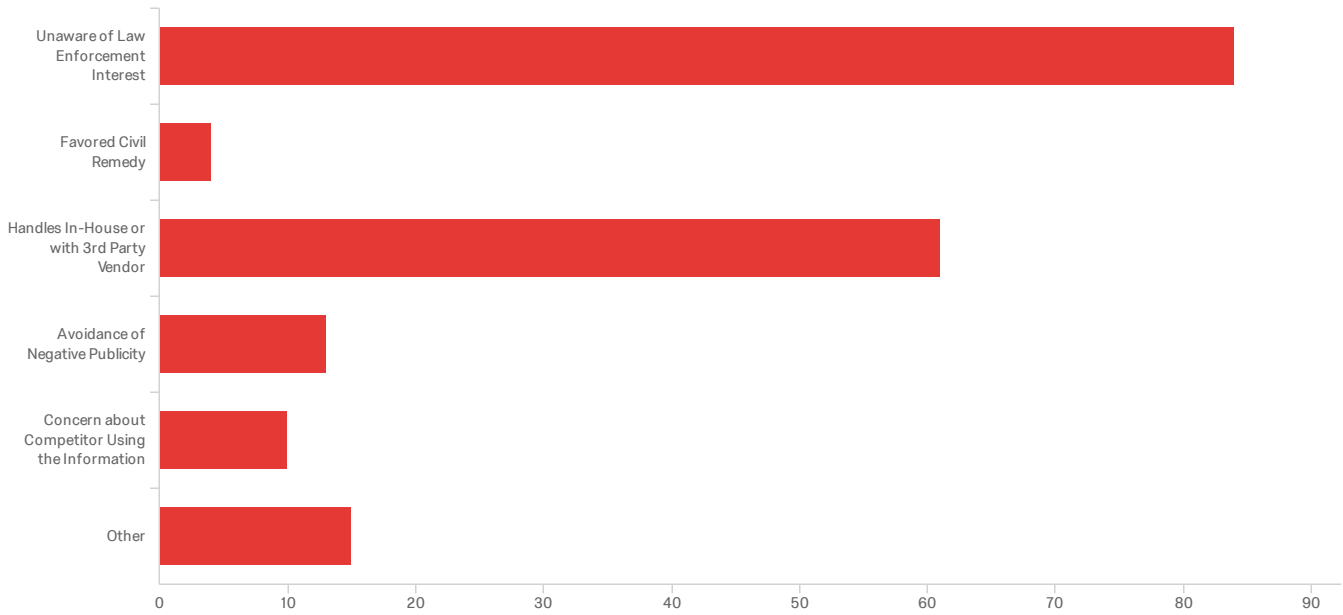
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	To the best of your knowledge, would your organization report a cyber-incident/ breach to law enforcement?	1.00	2.00	1.17	0.37	0.14	959

#	Field	Choice Count
1	Yes	83.42% 800
2	No	16.58% 159
		959

Showing rows 1 - 3 of 3

Q37 - If you would NOT report a cyber-incident or breach please check all that apply

below.

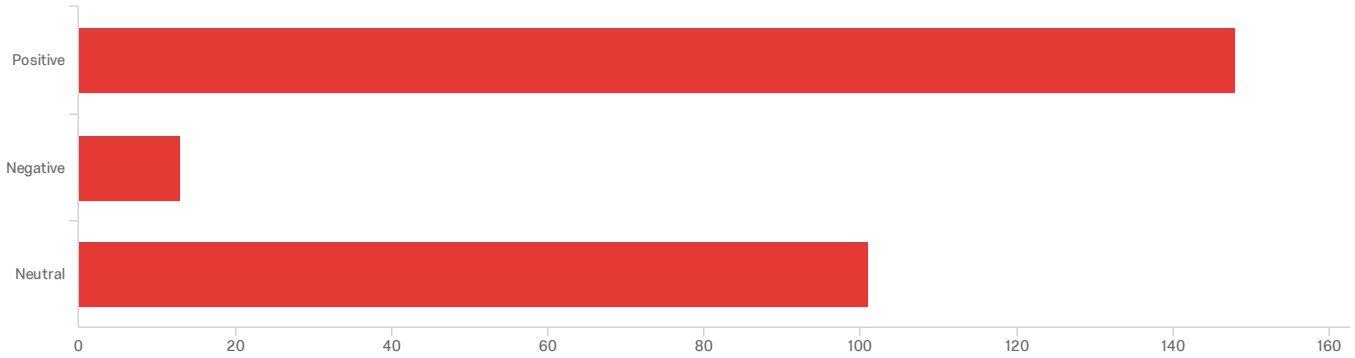


#	Field	Choice Count
1	Unaware of Law Enforcement Interest	44.92% 84
2	Favored Civil Remedy	2.14% 4
3	Handles In-House or with 3rd Party Vendor	32.62% 61
4	Avoidance of Negative Publicity	6.95% 13
5	Concern about Competitor Using the Information	5.35% 10
6	Other	8.02% 15

187

Showing rows 1 - 7 of 7

Q38 - Which best describes your organization's interaction with law enforcement for cyber related incidents / breaches or threat information sharing.

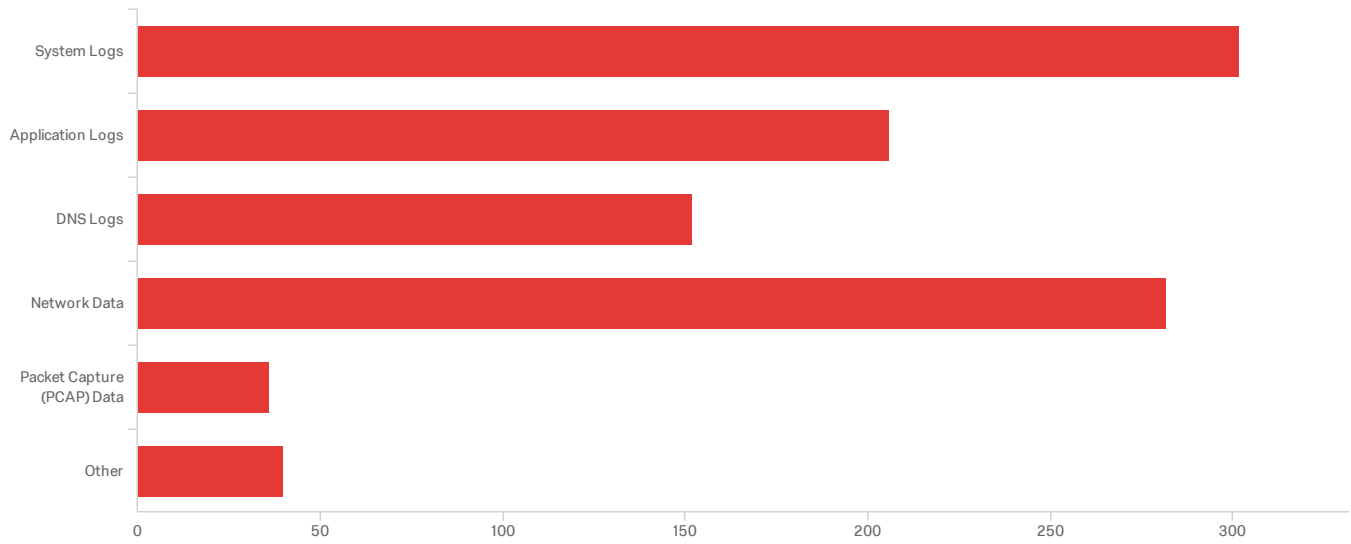


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which best describes your organization's interaction with law enforcement for cyber related incidents / breaches or threat information sharing.	1.00	3.00	1.82	0.96	0.92	262

#	Field	Choice Count
1	Positive	56.49% 148
2	Negative	4.96% 13
3	Neutral	38.55% 101
		262

Showing rows 1 - 4 of 4

### Q39 - Which of the following does your organization retain? (Choose all that apply)

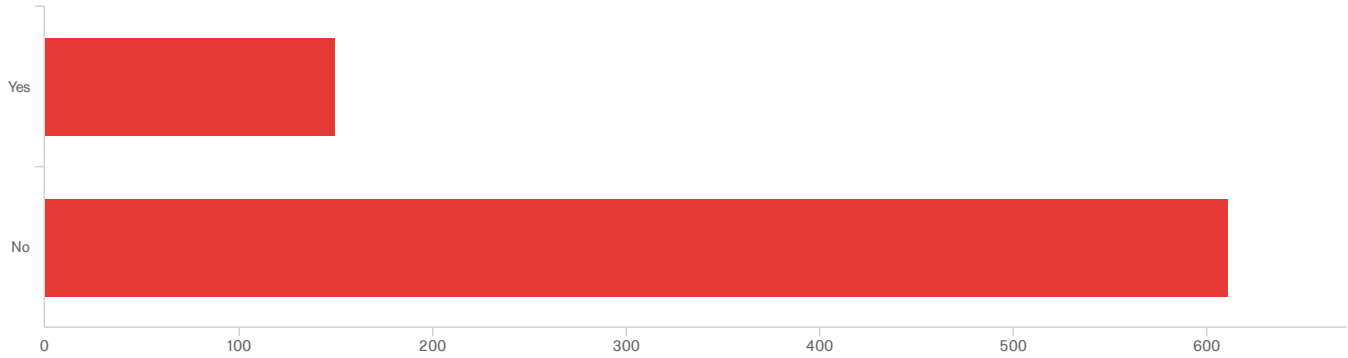


#	Field	Choice Count
1	System Logs	29.67% 302
2	Application Logs	20.24% 206
3	DNS Logs	14.93% 152
4	Network Data	27.70% 282
5	Packet Capture (PCAP) Data	3.54% 36
7	Other	3.93% 40

1018

Showing rows 1 - 7 of 7

Q40 - Is your organization interested in participating in a Table-Top exercise (a half-day cyber preparedness simulation)?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Is your organization interested in participating in a Table-Top exercise (a half-day cyber preparedness simulation)?	4.00	5.00	4.80	0.40	0.16	761

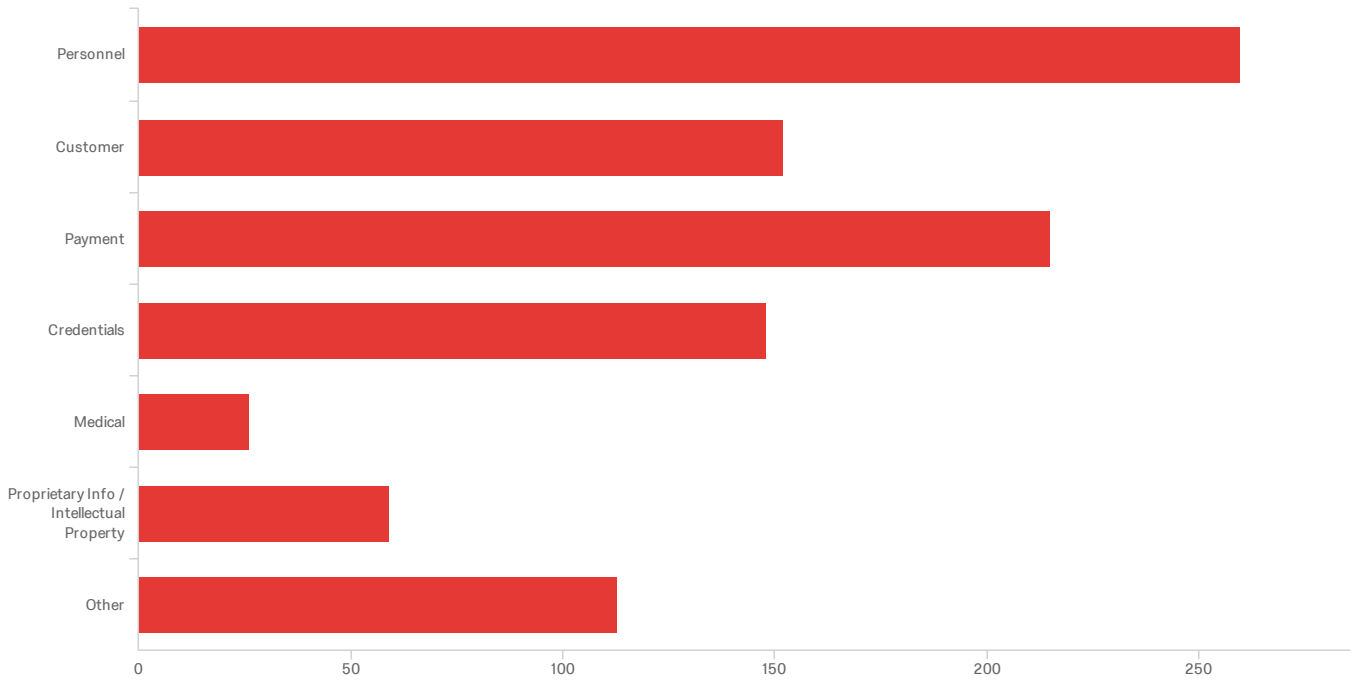
#	Field	Choice Count
1	Yes	19.71% 150
2	No	80.29% 611


761

Showing rows 1 - 3 of 3

# Q41 - What types of data are most frequently targeted in attacks on your organization?

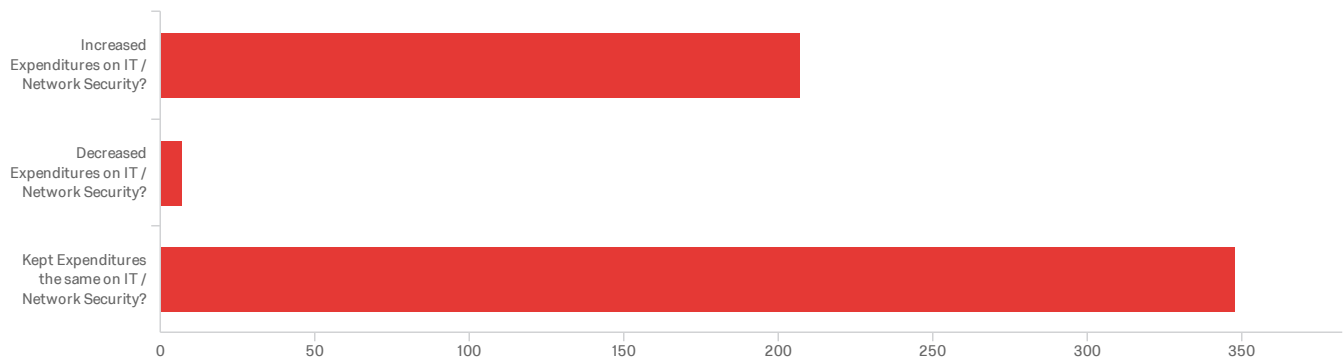
(Choose top three)



  
 Data source misconfigured for this visualization.

#	Field	Choice Count
1	Personnel	26.72% 260
2	Customer	15.62% 152
3	Payment	22.10% 215
4	Credentials	15.21% 148
5	Medical	2.67% 26
6	Proprietary Info / Intellectual Property	6.06% 59
7	Other	11.61% 113
		973

## Q42 - Over the past 12 months, has your organization:



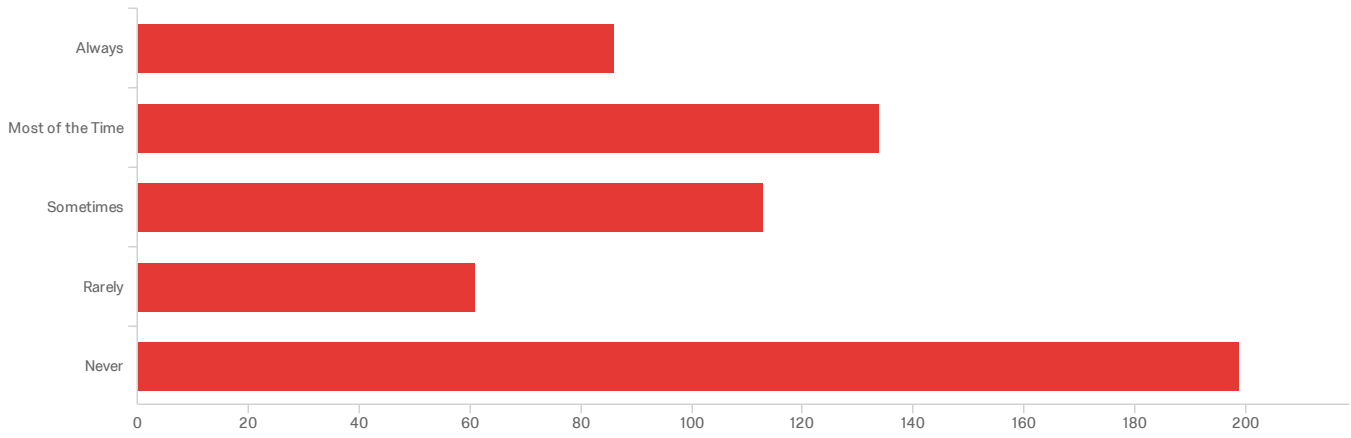
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Over the past 12 months, has your organization:	1.00	3.00	2.25	0.96	0.92	562

#	Field	Choice Count
1	Increased Expenditures on IT / Network Security?	36.83% 207
2	Decreased Expenditures on IT / Network Security?	1.25% 7
3	Kept Expenditures the same on IT / Network Security?	61.92% 348
		562

Showing rows 1 - 4 of 4



Q43 - Is your organization able to find sufficiently qualified cybersecurity applicants to fill open positions in a timely manner?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Is your organization able to find sufficiently qualified cybersecurity applicants to fill open positions in a timely manner?	1.00	5.00	3.26	1.48	2.18	593

#	Field	Choice Count
1	Always	14.50% 86
2	Most of the Time	22.60% 134
3	Sometimes	19.06% 113
4	Rarely	10.29% 61
5	Never	33.56% 199
		593

Showing rows 1 - 6 of 6