THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

Cybersecurity: Survey plus Data Analytics Analysis of SEC Data Indicate Diversity Exists

Pedro Nunez Beltran
Vice President, Department of Accounting,
Nava Land, Inc. Vietnam
Dahli Gray
Professor, Department of Business Administration,
Keiser University, United States

Abstract:
The USA Federal (i.e., Securities and Exchange Commission (SEC)) Cybersecurity Research and Development (R&D) Programs by Agency were analyzed using data analytics. They revealed diversity in the acceptance of R&D Programs as selected by 83 agencies. This indicated that there is a lack of agreement among the agencies as to which R&D programs should be utilized. Artificial Intelligence Programs were inserted by 36% of the agencies as part of Internal Control. Nine agencies inserted privacy as part of their Internal Controls. After joining the files using IDEA software, a negative correlation was found between all objectives (e.g., deter, protect, detect, respond) and the R&D Programs. This indicated a need for additional research, so a survey was completed in June 2022 of 151 adults in the USA general population. It revealed that the majority felt the SEC was doing a good job of providing cybersecurity guidance (e.g., via the Public Company Accounting Oversight Board) and enforcement. However, a significant number disagreed, indicating that the SEC could do a better job.

Keywords: *Cybersecurity, Securities and Exchange Commission, data analytics, public company accounting oversight board*

1. Introduction

This article presents research results based on the use of data analytics to analyze the adoption of the United States of America (USA) Securities and Exchange Commission (SEC) Research and Development (R&D) programs by USA agencies. In addition, diversity was discovered that motivate a survey of the general USA adult population regarding their opinions of the SEC. The research results are presented next.

2. SEC

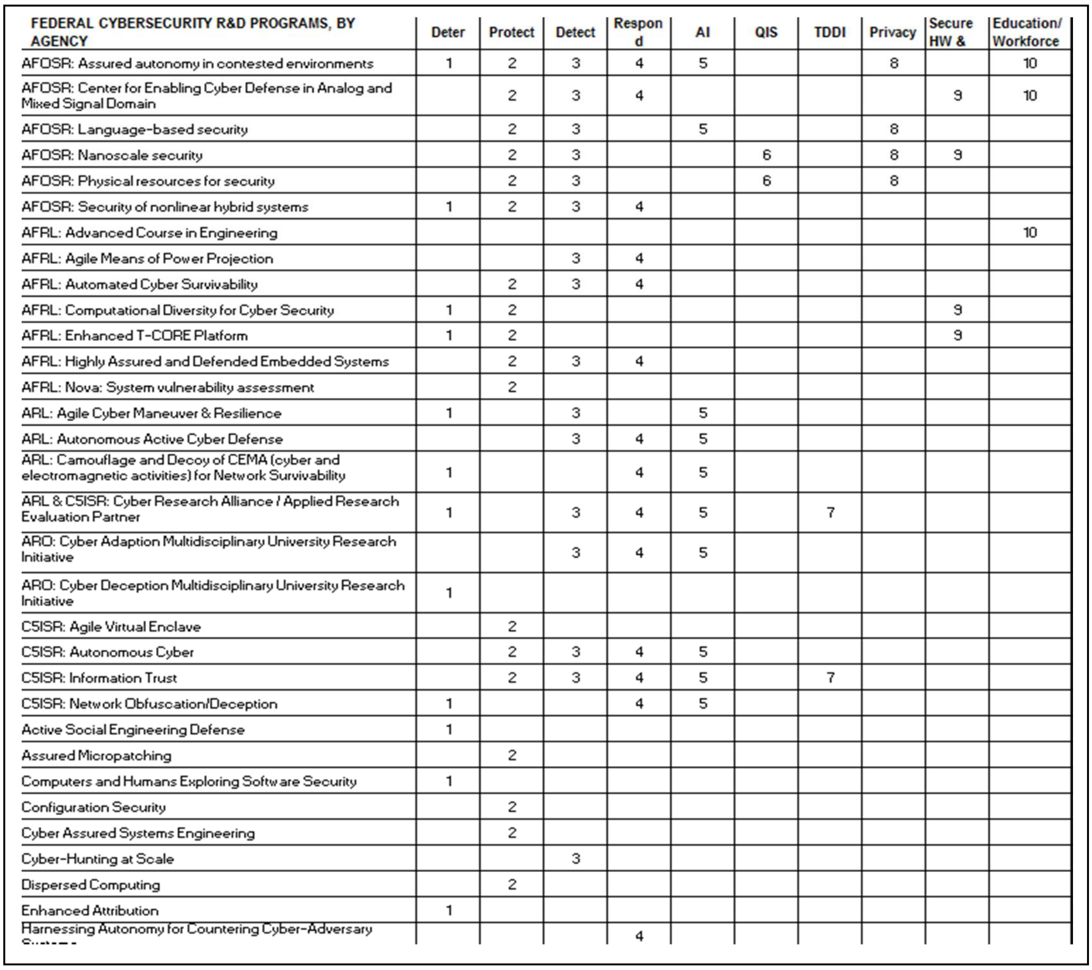
Comments on the issue of how to act in case a data breach takes place are such as the SEC (2022) points out.

Regardless of size, Cybersecurity and Infrastructure Security Agency (CISA) recommends that all organizations adopt a heightened cybersecurity posture and protect their most critical assets. Recommended actions include:

- Reducing the likelihood of a damaging cyber intrusion,
- Taking steps to detect a potential intrusion quickly,
- Ensuring that the organization is prepared to respond if an intrusion occurs, and
- Maximizing the organization's resilience to a destructive cyber incident.

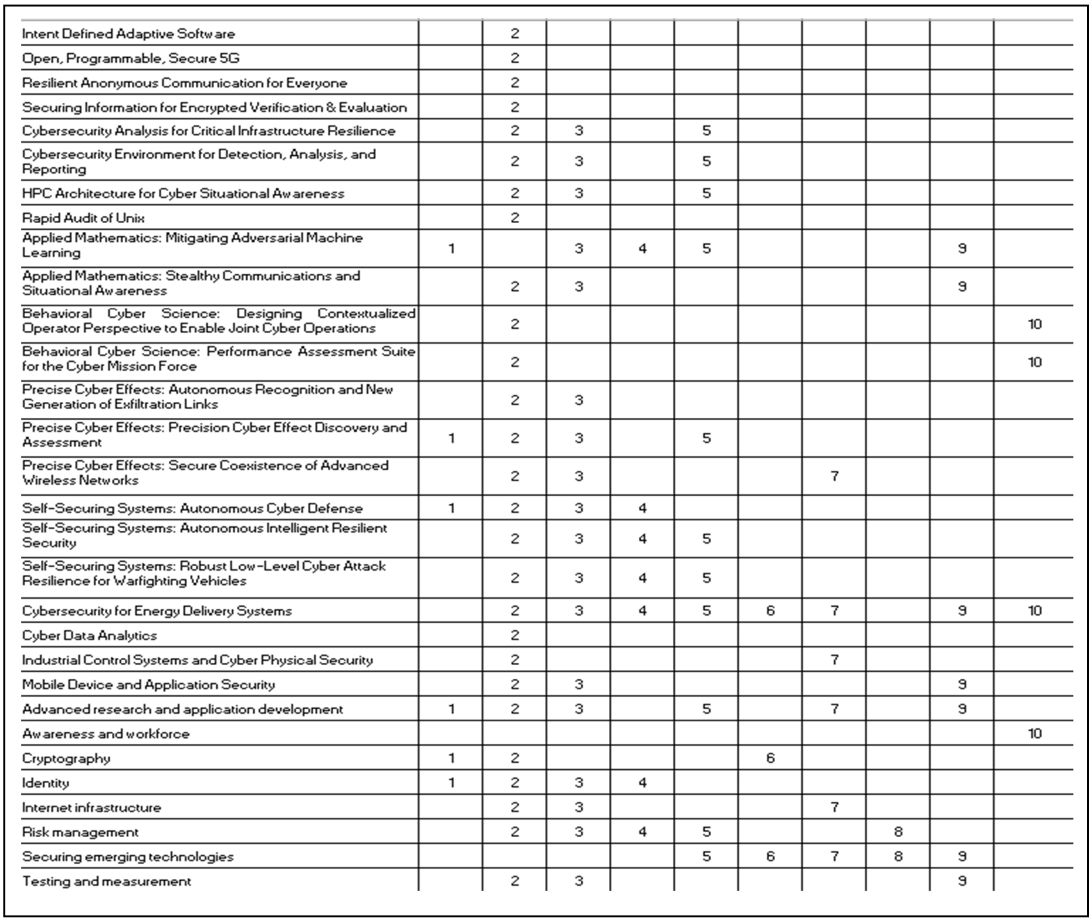
Using an accounting information system (AIS) can help achieve the above goals. An AIS collects, records, and stores accounting information and then compiles that information using accounting rules to report financial and non-financial information to decision-makers. A well-designed accounting system helps auditors to trace transactions. 'AIS programs bridge the gap between accounting and technology' (O'Donnell, 2019). An example of an accounting information system can be a Transaction Processing System (TPS). This type of program helps to translate daily transactions into accounting entries. Automatic entries can help to avoid human errors. It can also speed up the process of recording transactions and events. The survey incorporates accounting and auditing issues under the guidance of the SEC. This will be discussed later in the article.

The following data (see Figure 1 below) has been analyzed for this article using the data analytics IDEA software program to determine the priorities in the Federal SEC Cybersecurity Research and Development (R&D) Programs as adopted by 83 Agencies.



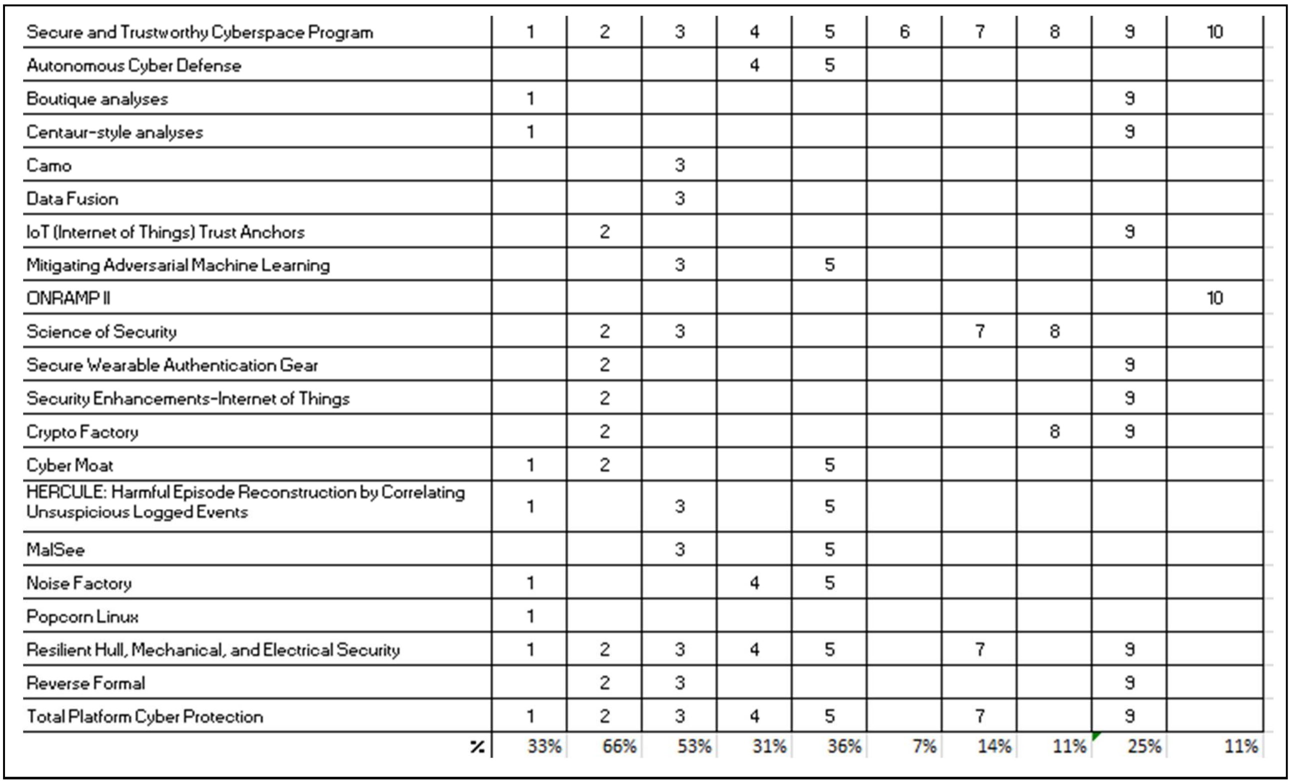
FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW &	Education/ Workforce
AFOSR: Assured autonomy in contested environments	1	2	3	4	5			8		10
AFOSR: Center for Enabling Cyber Defense in Analog and Mixed Signal Domain		2	3	4					9	10
AFOSR: Language-based security		2	3		5			8		
AFOSR: Nanoscale security		2	3			6		8	9	
AFOSR: Physical resources for security		2	3			6		8		
AFOSR: Security of nonlinear hybrid systems	1	2	3	4						
AFRL: Advanced Course in Engineering										10
AFRL: Agile Means of Power Projection			3	4						
AFRL: Automated Cyber Survivability		2	3	4						
AFRL: Computational Diversity for Cyber Security	1	2							9	
AFRL: Enhanced T-CORE Platform	1	2							9	
AFRL: Highly Assured and Defended Embedded Systems		2	3	4						
AFRL: Nova: System vulnerability assessment		2								
ARL: Agile Cyber Maneuver & Resilience	1		3		5					
ARL: Autonomous Active Cyber Defense			3	4	5					
ARL: Camouflage and Decoy of CEMA (cyber and electromagnetic activities) for Network Survivability	1			4	5					
ARL & C5ISR: Cyber Research Alliance / Applied Research Evaluation Partner	1		3	4	5		7			
ARO: Cyber Adaption Multidisciplinary University Research Initiative			3	4	5					
ARO: Cyber Deception Multidisciplinary University Research Initiative	1									
C5ISR: Agile Virtual Enclave		2								
C5ISR: Autonomous Cyber		2	3	4	5					
C5ISR: Information Trust		2	3	4	5		7			
C5ISR: Network Obfuscation/Deception	1			4	5					
Active Social Engineering Defense	1									
Assured Micropatching		2								
Computers and Humans Exploring Software Security	1									
Configuration Security		2								
Cyber Assured Systems Engineering		2								
Cyber-Hunting at Scale			3							
Dispersed Computing		2								
Enhanced Attribution	1									
Harnessing Autonomy for Countering Cyber-Adversary Systems				4						

Table 1



Intent Defined Adaptive Software		2								
Open, Programmable, Secure 5G		2								
Resilient Anonymous Communication for Everyone		2								
Securing Information for Encrypted Verification & Evaluation		2								
Cybersecurity Analysis for Critical Infrastructure Resilience		2	3		5					
Cybersecurity Environment for Detection, Analysis, and Reporting		2	3		5					
HPC Architecture for Cyber Situational Awareness		2	3		5					
Rapid Audit of Unix		2								
Applied Mathematics: Mitigating Adversarial Machine Learning	1		3	4	5				9	
Applied Mathematics: Stealthy Communications and Situational Awareness		2	3						9	
Behavioral Cyber Science: Designing Contextualized Operator Perspective to Enable Joint Cyber Operations		2								10
Behavioral Cyber Science: Performance Assessment Suite for the Cyber Mission Force		2								10
Precise Cyber Effects: Autonomous Recognition and New Generation of Exfiltration Links		2	3							
Precise Cyber Effects: Precision Cyber Effect Discovery and Assessment	1	2	3		5					
Precise Cyber Effects: Secure Coexistence of Advanced Wireless Networks		2	3				7			
Self-Securing Systems: Autonomous Cyber Defense	1	2	3	4						
Self-Securing Systems: Autonomous Intelligent Resilient Security		2	3	4	5					
Self-Securing Systems: Robust Low-Level Cyber Attack Resilience for Warfighting Vehicles		2	3	4	5					
Cybersecurity for Energy Delivery Systems		2	3	4	5	6	7		9	10
Cyber Data Analytics		2								
Industrial Control Systems and Cyber Physical Security		2					7			
Mobile Device and Application Security		2	3						9	
Advanced research and application development	1	2	3		5		7		9	
Awareness and workforce										10
Cryptography	1	2				6				
Identity	1	2	3	4						
Internet infrastructure		2	3				7			
Risk management		2	3	4	5			8		
Securing emerging technologies					5	6	7	8	9	
Testing and measurement		2	3						9	

Table 2



Secure and Trustworthy Cyberspace Program	1	2	3	4	5	6	7	8	9	10
Autonomous Cyber Defense				4	5					
Boutique analyses	1								9	
Centaur-style analyses	1								9	
Camo			3							
Data Fusion			3							
IoT (Internet of Things) Trust Anchors		2							9	
Mitigating Adversarial Machine Learning			3		5					
ONRAMP II										10
Science of Security		2	3				7	8		
Secure Wearable Authentication Gear		2							9	
Security Enhancements-Internet of Things		2							9	
Crypto Factory		2						8	9	
Cyber Moat	1	2			5					
HERCULE: Harmful Episode Reconstruction by Correlating Unsuspicious Logged Events	1		3		5					
MalSee			3		5					
Noise Factory	1			4	5					
Popcorn Linux	1									
Resilient Hull, Mechanical, and Electrical Security	1	2	3	4	5		7		9	
Reverse Formal		2	3						9	
Total Platform Cyber Protection	1	2	3	4	5		7		9	
%	33%	66%	53%	31%	36%	7%	14%	11%	25%	11%

Table 3

Abbreviations: AI = Artificial Intelligence; QIS = Quantum Information Systems; TDDI = Trustworthy Distributed Digital Infrastructure; HW & SW = Hardware and Software

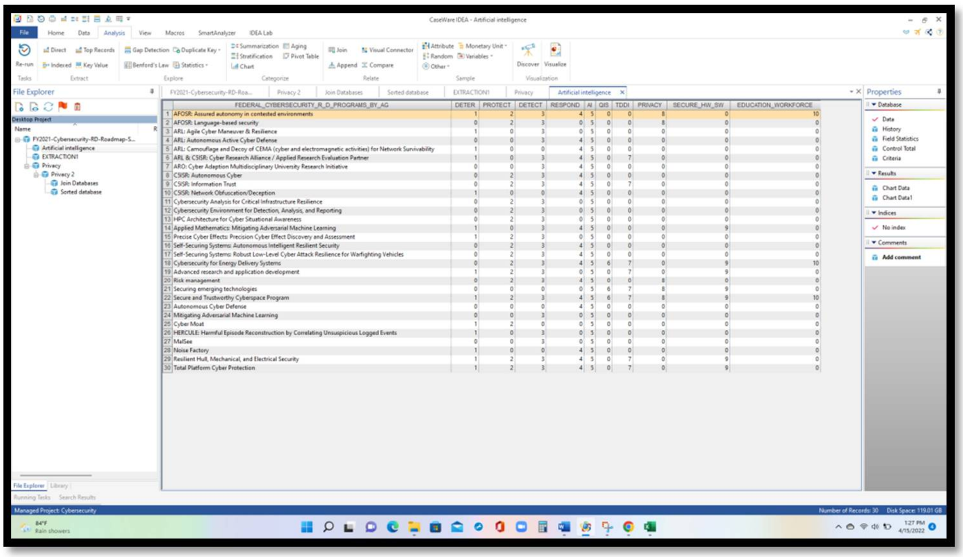
Source of data and abbreviations: Executive Office of the President of the United States (EOPUS). (2021, August 14). *FY2021 federal cybersecurity R&D strategic plan implementation guide.* Available at https://www.nitrd.gov/pubs/FY2021-Cybersecurity-RD-Roadmap.pdf pp. 3-7.

In the world of technology, the possibilities abound. However, one of the hardest tasks to do regarding technology is developing secure applications. Organizations are going through transformations with the help of technology. Modernization brings many advantages as well as disadvantages to data and infrastructure. Organizations like IBM provide cybersecurity services to protect, detect, and respond. For the fiscal year 2021, the USA government, in conjunction with private companies, inserted many other objectives to help assure organizations' data were and will continue to be well-secured.

The priority areas, according to the Executive Office of the President of the United States (2021), are considered to be the following:

Artificial Intelligence (AI) Capabilities that enable computers and other automated systems to perform tasks that have historically required human cognition and what are typically considered human decision-making abilities. Quantum Information Science (QIS) Capabilities harness quantum mechanics and quantum material properties to achieve computation, information processing, communications, and sensing in ways that cannot be achieved with classical physics principles. Trustworthy Distributed Digital Infrastructure (TDDI) Technologies facilitate secure information communications infrastructure. That infrastructure enables next-generation wireless communication, distributed computing, seamless integration of telecommunication systems with cyber-physical systems, and provides the communications infrastructure for the Industries of the Future (IotF). Privacy solutions minimize privacy risks or prevent privacy violations arising from collecting and using peoples' private information. Secure Hardware and Software (HW & SW) Technologies that provide and improve security properties of hardware and software components in computing and communication systems. Implement Education and Workforce Development Programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce.

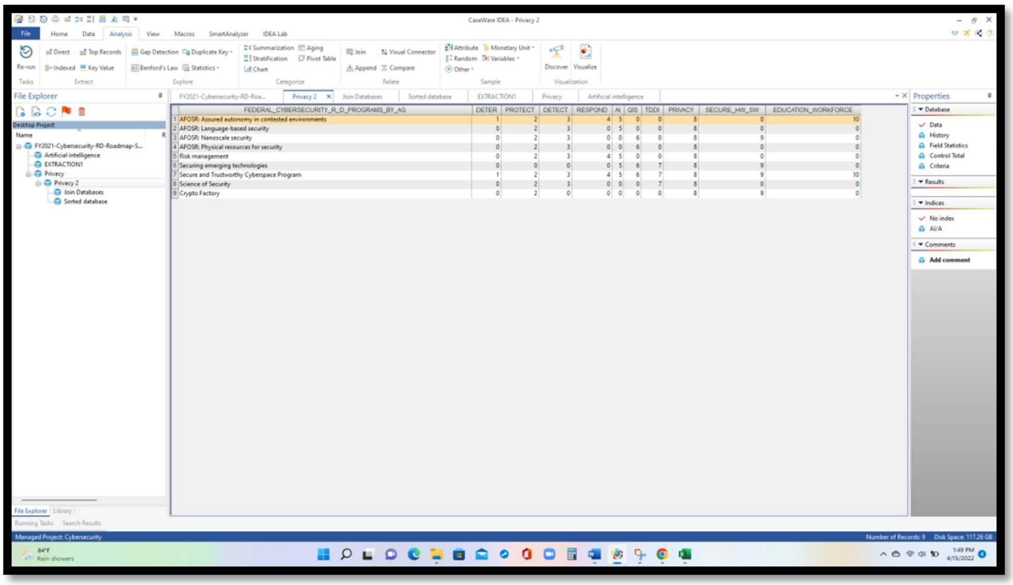
Figure 2 was developed from the Figure 1 data using data analytics IDEA software.



	FEDERAL_CYBERSECURITY_R_D_PROGRAMS_BY_AG	DETER	PROTECT	DETECT	RESPOND	AI	QIS	TDDI	PRIVACY	SECURE_HW_SW	EDUCATION_WORKFORCE
1	AFOSR: Assured autonomy in contested environments	1	2	3	4	5	0	0	8	0	10
2	AFOSR: Language-based security	0	2	3	0	5	0	0	8	0	0
3	ARL: Agile Cyber Maneuver & Resilience	1	0	3	0	5	0	0	0	0	0
4	ARL: Autonomous Active Cyber Defense	0	0	3	4	5	0	0	0	0	0
5	ARL: Camouflage and Decoy of CEMA (cyber and electromagnetic activities) for Network Survivability	1	0	0	4	5	0	0	0	0	0
6	ARL & CSISR: Cyber Research Alliance / Applied Research Evaluation Partner	1	0	3	4	5	0	7	0	0	0
7	ARO: Cyber Adaption Multidisciplinary University Research Initiative	0	0	3	4	5	0	0	0	0	0
8	CSISR: Autonomous Cyber	0	2	3	4	5	0	0	0	0	0
9	CSISR: Information Trust	0	2	3	4	5	0	7	0	0	0
10	CSISR: Network Obfuscation/Deception	1	0	0	4	5	0	0	0	0	0
11	Cybersecurity Analysis for Critical Infrastructure Resilience	0	2	3	0	5	0	0	0	0	0
12	Cybersecurity Environment for Detection, Analysis, and Reporting	0	2	3	0	5	0	0	0	0	0
13	HPC Architecture for Cyber Situational Awareness	0	2	3	0	5	0	0	0	0	0
14	Applied Mathematics: Mitigating Adversarial Machine Learning	1	0	3	4	5	0	0	0	9	0
15	Precise Cyber Effects: Precision Cyber Effect Discovery and Assessment	1	2	3	0	5	0	0	0	0	0
16	Self-Securing Systems: Autonomous Intelligent Resilient Security	0	2	3	4	5	0	0	0	0	0
17	Self-Securing Systems: Robust Low-Level Cyber Attack Resilience for Warfighting Vehicles	0	2	3	4	5	0	0	0	0	0
18	Cybersecurity for Energy Delivery Systems	0	2	3	4	5	6	7	0	9	10
19	Advanced research and application development	1	2	3	0	5	0	7	0	9	0
20	Risk management	0	2	3	4	5	0	0	8	0	0
21	Securing emerging technologies	0	0	0	0	5	6	7	8	9	0
22	Secure and Trustworthy Cyberspace Program	1	2	3	4	5	6	7	8	9	10
23	Autonomous Cyber Defense	0	0	0	4	5	0	0	0	0	0
24	Mitigating Adversarial Machine Learning	0	0	3	0	5	0	0	0	0	0
25	Cyber Moat	1	2	0	0	5	0	0	0	0	0
26	HERCULE: Harmful Episode Reconstruction by Correlating Unsuspicious Logged Events	1	0	3	0	5	0	0	0	0	0
27	MalSee	0	0	3	0	5	0	0	0	0	0
28	Noise Factory	1	0	0	4	5	0	0	0	0	0
29	Resilient Hull, Mechanical, and Electrical Security	1	2	3	4	5	0	7	0	9	0
30	Total Platform Cyber Protection	1	2	3	4	5	0	7	0	9	0

Figure 1: USA SEC Cybersecurity 10 R&D Program Objectives as Adopted by 83 Agencies

Figure 1 is data analyzed with the results presented in Figure 2 above, including all the programs selected to insert AI as part of internal control. It constitutes from all the programs involved in this cybersecurity project 36% of participation. In other words, 30 programs plan to implement artificial intelligence in their operating systems. 'As artificial intelligence (AI) becomes more ubiquitous, complex, and consequential, the need for people to understand how decisions are made and to judge their correctness becomes increasingly crucial due to concerns of ethics, accountability, and trust' (Miller, Weber, & Magazzeni, 2020. p. 103).



	FEDERAL_CYBERSECURITY_R_D_PROGRAMS_BY_AG	DETER	PROTECT	DETECT	RESPOND	AI	QIS	TDDI	PRIVACY	SECURE_HW_SW	EDUCATION_WORKFORCE
1	AFOSR: Assured autonomy in contested environments	1	2	3	4	5	0	0	8	0	10
2	AFOSR: Language-based security	0	2	3	0	5	0	0	8	0	0
3	AFOSR: Nanoscale security	0	2	3	0	0	6	0	8	9	0
4	AFOSR: Physical resources for security	0	2	3	0	0	6	0	8	0	0
5	Risk management	0	2	3	4	5	0	0	8	0	0
6	Securing emerging technologies	0	0	0	0	5	6	7	8	9	0
7	Secure and Trustworthy Cyberspace Program	1	2	3	4	5	6	7	8	9	10
8	Science of Security	0	2	3	0	0	0	7	8	0	0
9	Crypto Factory	0	2	0	0	0	0	0	8	9	0

Figure 2: Programs Inserting Artificial Intelligence as Part of Internal Control

Another priority area is privacy. Figure 4 below includes a chart for a better picture of all the programs that take privacy as an essential aspect. Of all the programs, only 11% consider the objective of privacy. The Secure and Trustworthy Cyberspace Program is the only program that considers all the objectives listed in the project. After joining the files, a negative correlation, as presented in the figure below the chart in Figure 4, was found among all the objectives (e.g., deter, protect, detect, respond) listed. The data fell in a downward sloping direction.

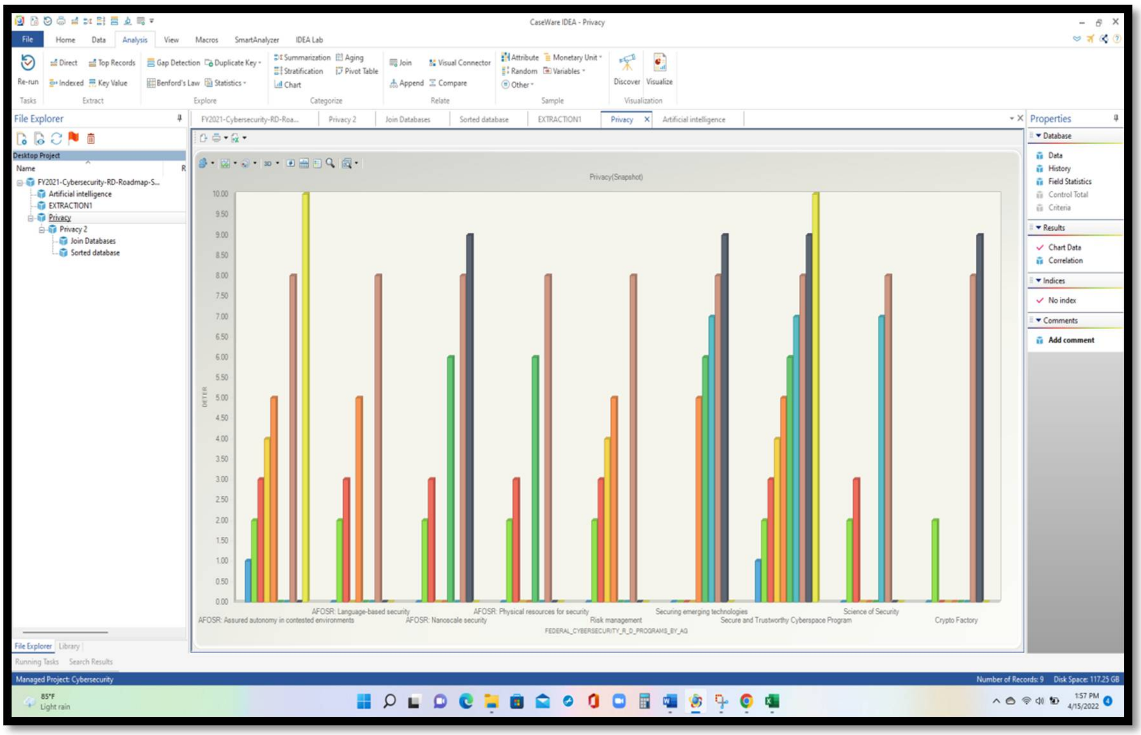
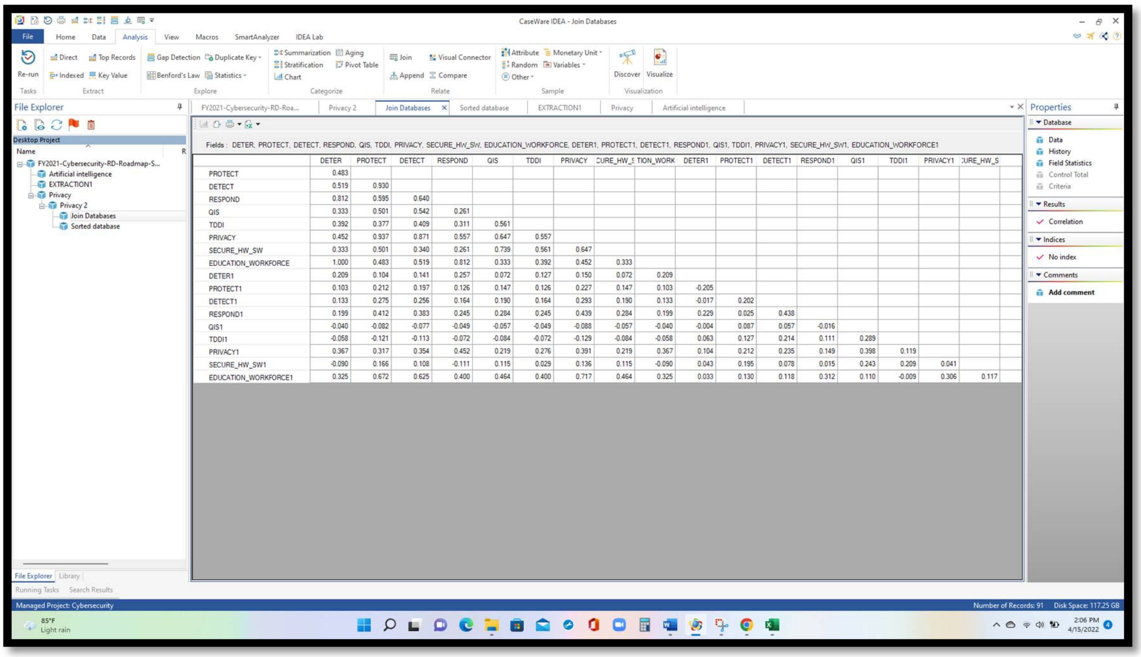

CaseWare IDEA - Privacy
Privacy(Snapshot)
DETER
10.00
9.50
9.00
8.50
8.00
7.50
7.00
6.50
6.00
5.50
5.00
4.50
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
AFOSR: Assured autonomy in contested environments
AFOSR: Language-based security
AFOSR: Nanoscale security
AFOSR: Physical resources for security
Risk management
Securing emerging technologies
Secure and Trustworthy Cyberspace Program
Science of Security
Crypto Factory
FEDERAL_CYBERSECURITY_R_D_PROGRAMS_BY_AG
Number of Records: 9

Figure 3: Nine Programs Inserting Privacy as Key Objective of Internal Control



Fields : DETER, PROTECT, DETECT, RESPOND, QIS, TDDI, PRIVACY, SECURE_HW_SW, EDUCATION_WORKFORCE, DETER1, PROTECT1, DETECT1, RESPOND1, QIS1, TDDI1, PRIVACY1, SECURE_HW_SW1, EDUCATION_WORKFORCE1

	DETER	PROTECT	DETECT	RESPOND	QIS	TDDI	PRIVACY	CURE_HW_S	TION_WORK	DETER1	PROTECT1	DETECT1	RESPOND1	QIS1	TDDI1	PRIVACY1	CURE_HW_S
PROTECT	0.483																
DETECT	0.519	0.930															
RESPOND	0.812	0.595	0.640														
QIS	0.333	0.501	0.542	0.261													
TDDI	0.392	0.377	0.409	0.311	0.561												
PRIVACY	0.452	0.937	0.871	0.557	0.647	0.557											
SECURE_HW_SW	0.333	0.501	0.340	0.261	0.739	0.561	0.647										
EDUCATION_WORKFORCE	1.000	0.483	0.519	0.812	0.333	0.392	0.452	0.333									
DETER1	0.209	0.104	0.141	0.257	0.072	0.127	0.150	0.072	0.209								
PROTECT1	0.103	0.212	0.197	0.126	0.147	0.126	0.227	0.147	0.103	-0.205							
DETECT1	0.133	0.275	0.256	0.164	0.190	0.164	0.293	0.190	0.133	-0.017	0.202						
RESPOND1	0.199	0.412	0.383	0.245	0.284	0.245	0.439	0.284	0.199	0.229	0.025	0.438					
QIS1	-0.040	-0.082	-0.077	-0.049	-0.057	-0.049	-0.088	-0.057	-0.040	-0.004	0.087	0.057	-0.016				
TDDI1	-0.058	-0.121	-0.113	-0.072	-0.084	-0.072	-0.129	-0.084	-0.058	0.063	0.127	0.214	0.111	0.289			
PRIVACY1	0.367	0.317	0.354	0.452	0.219	0.276	0.391	0.219	0.367	0.104	0.212	0.235	0.149	0.398	0.119		
SECURE_HW_SW1	-0.090	0.166	0.108	-0.111	0.115	0.029	0.136	0.115	-0.090	0.043	0.195	0.078	0.015	0.243	0.209	0.041	
EDUCATION_WORKFORCE1	0.325	0.672	0.625	0.400	0.464	0.400	0.717	0.464	0.325	0.033	0.130	0.118	0.312	0.110	-0.009	0.306	0.117

Figure 4

To summarize the analysis from the data extracted and based on the information presented, the objectives presented in the SEC R&D project lack full agency participation. Therefore, there is some uncertainty when new programs are presented for the first time due to the lack of information. In the correlation figure, the first implemented objectives were the highest, including deter, protect, detect, and respond. Hopefully, more programs will include more objectives into their internal control systems as time passes.

Based on this study, with the help of the data analytics software IDEA, the objectives such as QIS and Education and workforce development, the percentage of participation is 7% and 11%, respectively. This result provides an insight that to minimize the risk, there should be more work in these areas. Once the knowledge is acquired, it is advisable to keep upgrading to keep up with technology. The advantage of having the data secured is undeniable, but it also comes with a downside. The cost for the organizations will increase. The most important aspect is to have a system free from intruders, as 'cybersecurity is also a responsibility of every market participant' (SEC, 2022). Since organizations rely on technology, the lack of cybersecurity has become a significant issue.

Most organizations no longer have to have buildings with rooms filled with paper files because everything can be saved with a simple computer with enough space. Accountants can automate entries because computers do whatever they are commanded to do. As a result, the level of error is decreased. This technology era has been a step forward for the whole world. However, it also opens new doors for innovative hackers with enough knowledge to do whatever it takes to invade an organization's information system. Organizations that work together often share much important information. If even one organization is not secured appropriately, it can jeopardize other organizations and individuals. This initial research indicated that additional research would be appropriate. A survey sample of 151 adults in the USA was completed. The results of the survey are presented next.

3. Survey Research Results

Motivated by the initial data analytics analysis findings of the diversity of SEC R&D Programs being selected by agencies, a survey was completed in June 2022 of 151 USA adults. The survey results are included as appendices at the end of the article. The first ten questions gathered opinions about the SEC's effectiveness, including the Public Company Accounting Oversight Board (PCAOB). The PCAOB was established by the SEC to provide guidance and standards for auditors of public, for-profit corporations using the USA stock exchanges.

While 47% or more of the respondents indicated that they agreed that the SEC was doing an accepted figure or better job of instituting cybersecurity programs and practices, between 15% and 40% neither agreed or disagreed with the idea that the SEC was doing an accepfigure job. A question for future research is why between 15% and 40% of the 151 respondents neither agreed nor disagreed.

4. Survey Demographics

The appendices at the end of this article presents survey demographics to document that the random sample of adults completing the survey represented a range of characteristics. Survey question 11 documents that the sample of respondents had household incomes of $0 to over $200,000, with respondents with incomes between these.

- Survey question 12 documents that 40% of the respondents identified themselves as male while 60% were female.
- Survey question 13 documents that the respondents ranged from the age of 18 to over 60.
- Survey question 14 documents that respondents represented the nine major regions of the USA.

The respondents represented a diverse group of USA residents, thereby making the survey results more meaningful and representative of the USA as a whole.

5. Conclusions

Based on all the relevant information provided in this article, the conclusions are that USA federal agencies do not agree on which objectives and R&D programs should be adopted. In contrast, the majority of the 151 USA respondents to the survey expressed the opinion that the SEC was doing an accepfigure job, while a significant number did not believe that the SEC was doing an accepfigure job.

6. Recommendations

It is recommended that all organizations create an IT department where all the information goes in and out safely. Investing in an IT department will be something that all organizations should be thinking about. Even though the costs for the organization might be higher, the benefits should outbalance the costs. Additional research could be done to see if the USA federal agencies adopted more SEC R&D objectives and programs in 2022 and beyond.

7. Summary

This article used data analytics to analyze the adoption of the SEC R&D objectives and programs by 83 agencies. The research results revealed a negative correlation between the objectives and selected programs. The survey of 151 USA respondents indicated that the majority believed that the SEC was doing an accepfigure job. Future research is recommended on this topic and these issues.

8. References

i. Executive Office of the President of the United States (EOPUS). (2021, August 14). *FY2021 federal cybersecurity R&D strategic plan implementation guide*. Available at https://www.nitrd.gov/pubs/FY2021-Cybersecurity-RD-Roadmap.pdf

ii. Miller, T., Weber, R. & Magazenni, D. (2020, Spring). *Report on the 2019 IJCAI explainable artificial intelligence workshop.* AI magazine. Available at https://ojs.aaai.org/index.php/aimagazine/article/view/5302

iii. O'Donnell, J. B. (2019). *Are accounting information systems programs evolving to meet the needs of the accounting profession? An analysis of accounting information systems programs in 2005 and 2019*. Available at https://articlegateway.com/index.php/JABE/article/view/2591

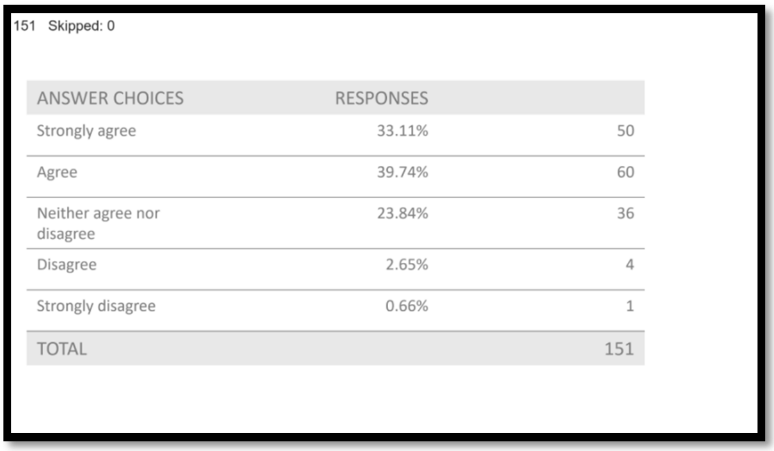
iv. Public Company Accounting Oversight Board (PCAOB). (2021, September 28). *PCAOB solicits additional public comment on proposed new requirements for lead auditor's use of other auditors*. https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-solicits-additional-public-comment-on-proposed-new-requirements-for-lead-auditor-s-use-of-other-auditors

v. Securities Exchange Commission (SEC). (2022, February 17). *Cybersecurity*. https://www.sec.gov/spotlight/cybersecurity

Appendices

Survey Results

Q1: 'As markets grow more global and complex, so too are the threats through cyber intrusion, denial of service attacks, manipulation, misuse by insiders, and other cyber misconduct. In the United States, aspects of cybersecurity are the responsibilities of multiple government agencies, including the [Securities and Exchange Commission] SEC. Cybersecurity is also a responsibility of every market participant. The SEC is committed to working with federal and local partners, market participants, and others to monitor developments and effectively respond to cyber threats (SEC. (2022, February 17). (Cybersecurity. https://www.sec.gov/spotlight/cybersecurity).' In your opinion, do you agree with this quote from the SEC?

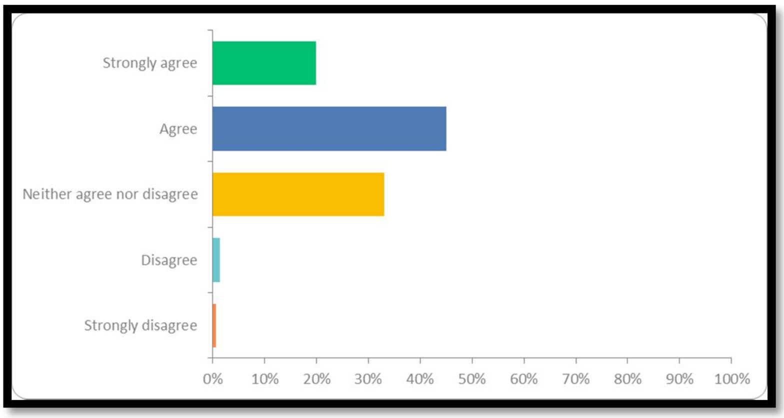


151 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	33.11%	50
Agree	39.74%	60
Neither agree nor disagree	23.84%	36
Disagree	2.65%	4
Strongly disagree	0.66%	1
TOTAL		151

Appendix 1

Q2: Per the Securities and Exchange Commission (SEC). (2022, February 17. Cybersecurity.) https://www.sec.gov/spotlight/cybersecurity, 'the SEC provides valuable guidance, including an Investor Alert and Investor Bulletin to help investors get in the know and protect themselves.' In your opinion, do you agree with the statement?



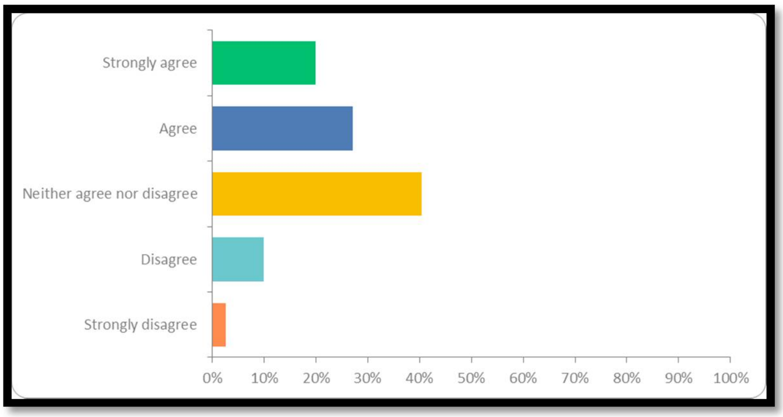
Appendix 2

Answer Choices	Responses	
Strongly agree	19.87%	30
Agree	45.03%	68
Neither agree nor disagree	33.11%	50
Disagree	1.32%	2
Strongly disagree	0.66%	1
TOTAL		151

Appendix 3

Q3: Per the Securities and Exchange Commission (SEC). (2022, February 17). Cybersecurity. https://www.sec.gov/spotlight/cybersecurity, 'the SEC uses its civil law authority to bring cyber-related enforcement actions that protect investors, hold bad actors accountable, and deter future wrongdoing.' In your opinion, do you agree that the SEC has been doing an adequate job of enforcement?

Answered: 151 Skipped: 0

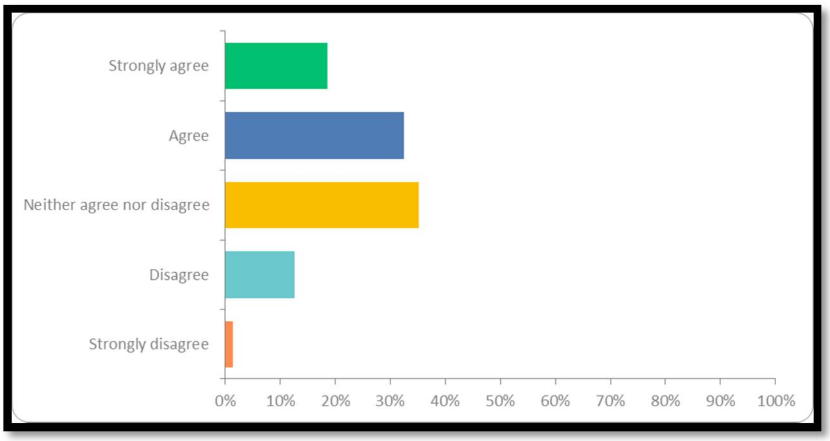


Appendix 4

Answer Choices	Responses	
Strongly agree	19.87%	30
Agree	27.15%	41
Neither agree nor disagree	40.40%	61
Disagree	9.93%	15
Strongly disagree	2.65%	4
TOTAL		151

Appendix 5

Q4: The SEC oversees the Public Company Accounting Oversight Board (PCAOB) that issues auditing standards the auditors (e.g., Certified Public Accountants) must use when auditing public, for-profit corporations that use a USA stock exchange. The PCAOB has solicited comments from interested parties regarding the data security when parts of an audit are sub-contracted (e.g., outsources) to other auditors. The primary and sub-contracted auditors would access the audited organization's financial information. In your opinion, do you agree that this is an accepfigure practice?
Answered: 151 Skipped: 0

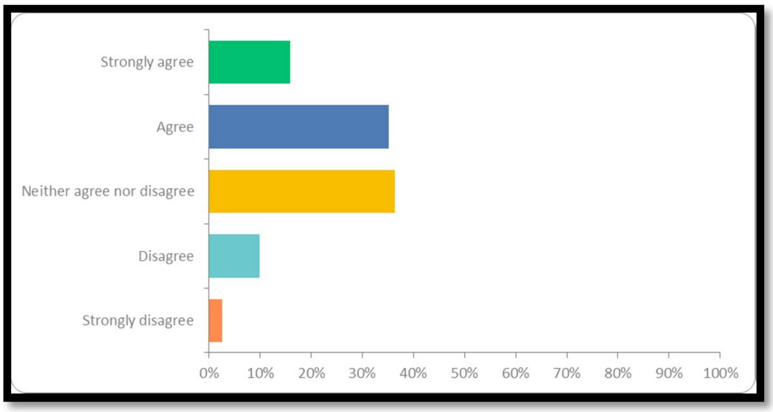


Appendix 6

Answer Choices	Responses	
Strongly agree	18.54%	28
Agree	32.45%	49
Neither agree nor disagree	35.10%	53
Disagree	12.58%	19
Strongly disagree	1.32%	2
TOTAL		151

Appendix 7

Q5: Per the Public Company Accounting Oversight Board (PCAOB, 2021, September 28), the PCAOB solicits additional public comments on proposed requirements for the lead auditor's use of other auditors. https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-solicits-additional-public-comment-on-proposed-new-requirements-for-lead-auditor-s-use-of-other-auditorsWorking with other auditors can differ from working with people from the same audit firm. Outside auditors' work can create challenges in coordination and communication. These challenges can lead to misunderstandings about the nature, timing, and extent of the other auditors' work and can detract from the quality of the audit. In your opinion, do you agree that the last two sentences are true?

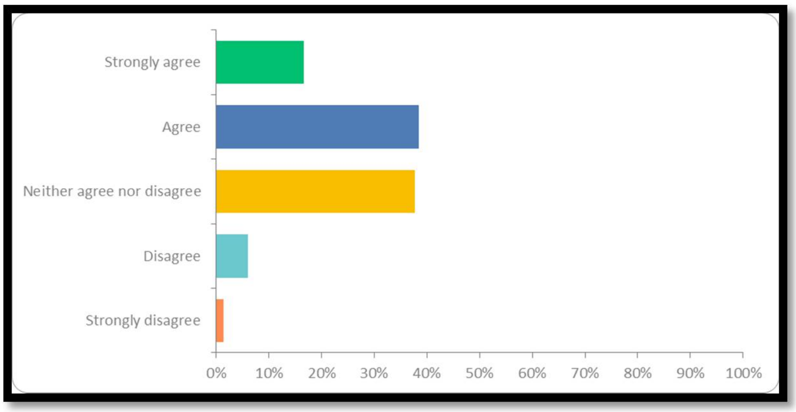


Appendix 8

Answer Choices	Responses	
Strongly agree	15.89%	24
Agree	35.10%	53
Neither agree nor disagree	36.42%	55
Disagree	9.93%	15
Strongly disagree	2.65%	4
TOTAL		151

Appendix 9

Q6: The Public Company Accounting Oversight Board (PCAOB, 2021, September 28) solicits additional comments from interested parties on the proposed requirement of increased supervision of the other auditors by the lead auditor to prevent and/or detect deficiencies in the other auditors' work.https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-solicits-additional-public-comment-on-proposed-new-requirements-for-lead-auditor-s-use-of-other-auditors. In your opinion, do you agree with this change?
Answered: 151 Skipped: 0

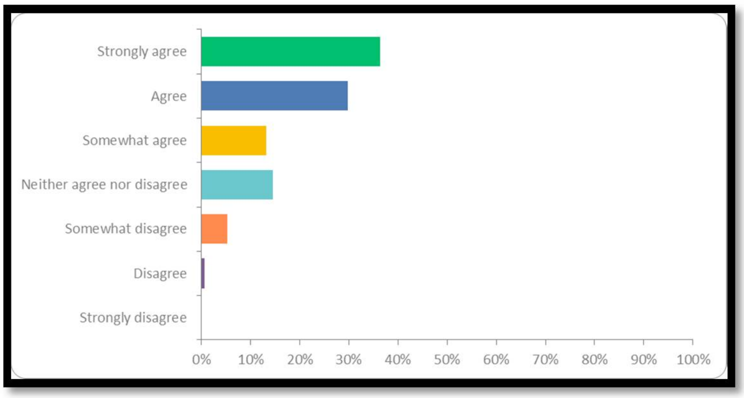


Appendix 10

Answer Choices	Responses	
Strongly agree	16.56%	25
Agree	38.41%	58
Neither agree nor disagree	37.75%	57
Disagree	5.96%	9
Strongly disagree	1.32%	2
TOTAL		151

Appendix 11

Q7: According to the federal government, it is important to have the ability to efficiently discourage malicious cyber activities by increasing the costs, risks, and uncertainty to cybercriminals. In your opinion, do you agree with this strategy?
Answered: 151 Skipped: 0

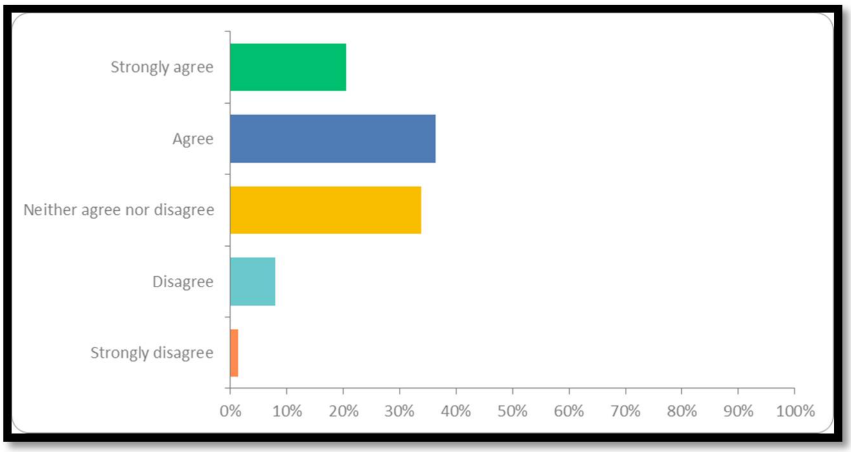


Appendix 12

Answer Choices	Responses	
Strongly agree	36.42%	55
Agree	29.80%	45
Somewhat agree	13.25%	20
Neither agree nor disagree	14.57%	22
Somewhat disagree	5.30%	8
Disagree	0.66%	1
Strongly disagree	0%	0
TOTAL		151

Appendix 13

Q8: According to the federal government, artificial intelligence will play an important role for accountants to work in a safer environment. In your opinion, do you agree with this statement?
Answered: 151 Skipped: 0

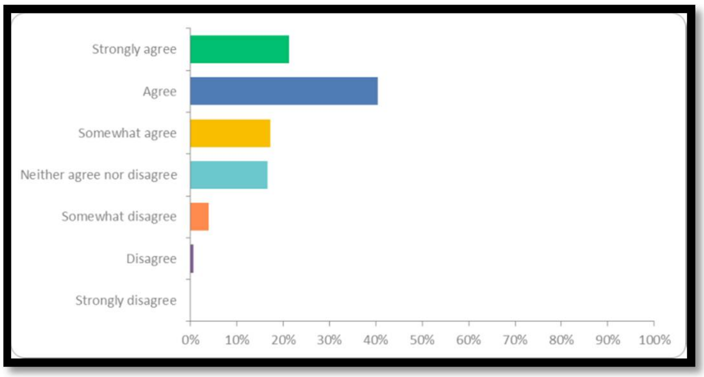


Appendix 14

Answer Choices	Responses	
Strongly agree	20.53%	31
Agree	36.42%	55
Neither agree nor disagree	33.77%	51
Disagree	7.95%	12
Strongly disagree	1.32%	2
Total		151

Appendix 15

Q9: Programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce will help auditors to understand the risks involved when working remotely. In your opinion, do you agree with this statement?
Answered: 151 Skipped: 0

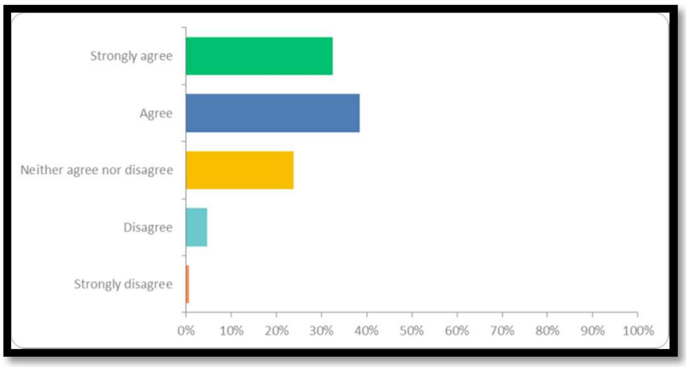


Appendix 16

Answer Choices	Responses	
Strongly agree	21.19%	32
Agree	40.40%	61
Somewhat agree	17.22%	26
Neither agree nor disagree	16.56%	25
Somewhat disagree	3.97%	6
Disagree	0.66%	1
Strongly disagree	0%	0
TOTAL		151

Appendix 17

Q10: According to the Securities and Exchange Commission, the responsibility to have a safe environment free from threats relies on every market participant. In your opinion, do you agree or disagree with this statement?
Answered: 151 Skipped: 0

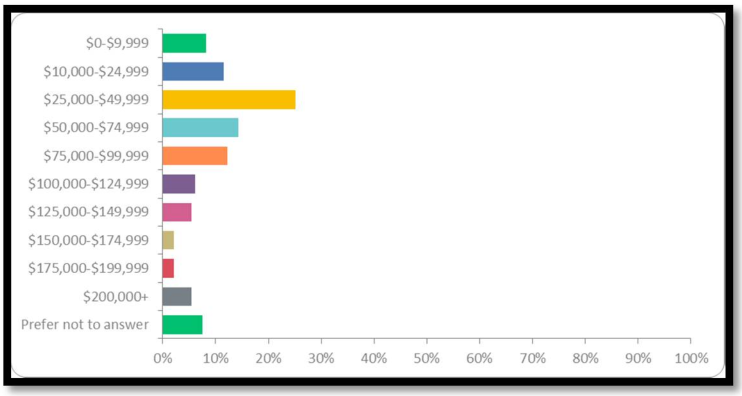


Appendix 18

Answer Choices	Responses	
Strongly agree	32.45%	49
Agree	38.41%	58
Neither agree nor disagree	23.84%	36
Disagree	4.64%	7
Strongly disagree	0.66%	1
Total		151

Appendix 19

Q11: Household Income
Answered: 147 Skipped: 4

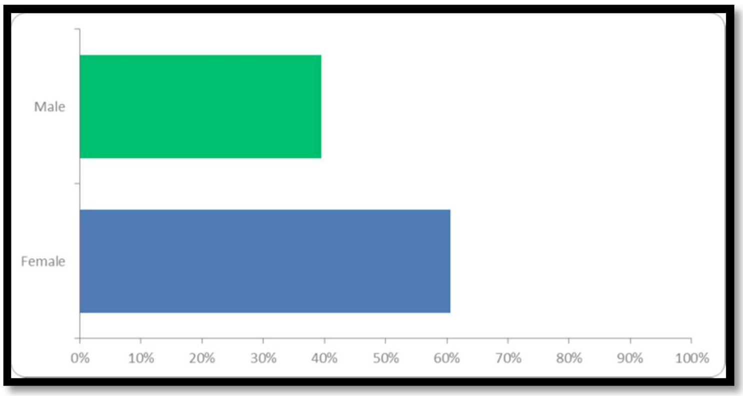


Appendix 20

Answer Choices	Responses	
$0-$9,999	8.16%	12
$10,000-$24,999	11.56%	17
$25,000-$49,999	25.17%	37
$50,000-$74,999	14.29%	21
$75,000-$99,999	12.24%	18
$100,000-$124,999	6.12%	9
$125,000-$149,999	5.44%	8
$150,000-$174,999	2.04%	3
$175,000-$199,999	2.04%	3
$200,000+	5.44%	8
Prefer not to answer	7.48%	11
TOTAL		147

Appendix 21

Q12: Gender
Answered: 147 Skipped: 4

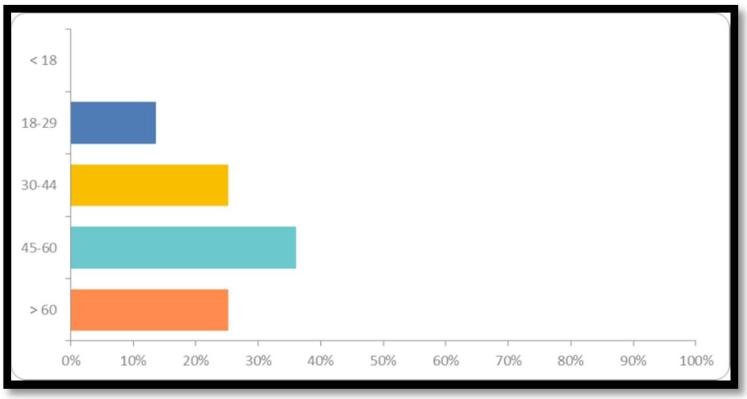


Appendix 22

Answer Choices	Responses	
Male	39.46%	58
Female	60.54%	89
TOTAL		147

Appendix 23

Q13: Age



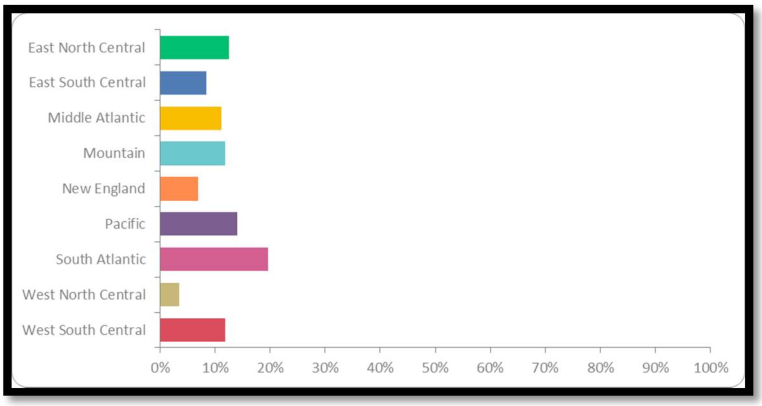
Appendix 24

Answer Choices	Responses	
< 18	0%	0
18-29	13.61%	20
30-44	25.17%	37
45-60	36.05%	53
> 60	25.17%	37
TOTAL		147

Appendix 25

Q14: Region

Answered: 143 Skipped: 8



Appendix 26

Answer Choices	Responses	
East North Central	12.59%	18
East South Central	8.39%	12
Middle Atlantic	11.19%	16
Mountain	11.89%	17
New England	6.99%	10
Pacific	13.99%	20
South Atlantic	19.58%	28
West North Central	3.50%	5
West South Central	11.89%	17
TOTAL		143

Appendix 27