Journal of Humanities and Social Sciences Studies
ISSN: 2663-7197
DOI: 10.32996/jhsss
Journal Homepage: www.al-kindipublisher.com/index.php/jhsss

JHSSS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Cybersecurity as a Catalyst: Enhancing Accountability and Driving Change in Federal Agencies

Maryam Maryam[1], Afrin Hoque Jui[2]✉, Prasenjit Debnath[3] and Yasmeen[4]
[1]Department of Computer Science and Artificial Intelligence, University of Udine, Italy
[2]Department of Management Sciences and Quantitative Methods (Master of Public Administration), Gannon University, PA, USA
[3]Department of Religious Studies, Memorial University of Newfoundland, St. John's, Canada
[4]Department of Media Sciences (MS in Media science), Bahria University, Islamabad, Pakistan
Corresponding Author: Afrin Hoque Jui, **Email:** Jui001@gannon.edu

| ABSTRACT
In an era of rapid technological advancements and increasing cyber threats, cybersecurity preparedness has become a critical component of organizational strategy, impacting the protection of information assets and overall organizational performance. This study examines the relationship between cybersecurity preparedness and key organizational outcomes, specifically accountability and effective changes in addressing challenges, within federal agencies. Data from the 2023 Federal Employee Viewpoint Survey (FEVS) were analyzed. Using descriptive statistics, spearman's rank correlation, ordered logistic regression, and structural equation model, the study assessed the impact of cybersecurity preparedness on organizational performance, controlling for gender, supervisory status, age, and tenure. The results indicate a significant positive association between cybersecurity preparedness and both accountability and effective changes in addressing challenges. Enhanced cybersecurity measures are linked to greater accountability and more effective organizational changes. These findings highlight the importance of robust cybersecurity strategies in improving organizational performance and resilience.

| KEYWORDS

Cyber Security, preparedness, accountability, performance, resilience, technology

| ARTICLE INFORMATION

ACCEPTED: 01 February 2025 **PUBLISHED:** 24 February 2025 **DOI:** 10.32996/jhsss.2025.7.2.5

1. Introduction

The SolarWinds cyberattack in December 2020, one of the most sophisticated and significant breaches in U.S. history, revealed the vulnerability of federal agencies to digital threats. This attack, conducted by hackers believed to be directed by Russian intelligence, infiltrated critical federal departments including Treasury, Justice, Energy, and the Pentagon. Embarrassingly, the hackers also breached the Cybersecurity and Infrastructure Security Agency (CISA) — the office at the Department of Homeland Security tasked with protecting federal computer networks from cyberattacks. This incident starkly highlighted the urgent necessity for robust cybersecurity measures within federal agencies to safeguard sensitive information, maintain operational integrity, and drive essential organizational change and accountability.

The SolarWinds cyberattack underscores the relevance of Christopher Hood's (1991) concept of "New Public Management" (NPM), which emphasized efficiency, performance, and accountability in public services. As a significant evolution in public administration, NPM introduced managerialism and market-based approaches to enhance public sector efficiency (Lapuente and Van de Walle 2020). In today's digital age, these principles have further evolved to incorporate comprehensive cybersecurity measures. By integrating cybersecurity into public administration, organizations ensure not only efficiency and

accountability but also resilience against cyber threats, thus maintaining public trust and operational stability (Yue and Shyu 2024).

Building on NPM, the latest evolution in public administration is the concept of collaborative governance, a new form of governance that emphasizes the importance of multi-stakeholder involvement in addressing complex public issues through collective decision-making and shared responsibility (Cristofoli, Meneguzzo, and Riccucci 2016). Scholars like Ansell and Gash (2008) emphasize that collaborative governance enhances information sharing, resource pooling, and coordinated responses to challenges, making it particularly relevant in the context of cybersecurity.

Cybersecurity serves as a powerful catalyst in federal agencies, driving significant enhancements in accountability and facilitating transformative organizational changes (Pavel, 2024; Pia, 2019). This study explores how robust cybersecurity preparedness can elevate organizational performance and resilience by fostering a culture of accountability and enabling effective responses to evolving challenges. Recent studies highlight the growing frequency and sophistication of cyberattacks, which necessitates robust cybersecurity measures to safeguard organizational integrity and functionality (Li and Liu 2021; Johnson 2015).

The concept of cybersecurity preparedness encompasses a range of activities, including the development of security policies, implementation of technical controls, and fostering a culture of security awareness among employees (Prümmer, van Steen and van den Berg 2024). Effective cybersecurity preparedness is essential for mitigating risks and ensuring that organizations can respond swiftly and effectively to security incidents (Moro-Visconti and Cesaretti 2023). Furthermore, cybersecurity is increasingly seen as integral to maintaining public trust and organizational accountability, particularly in the public sector where the protection of sensitive information is paramount (Hossain et al. 2024).

Accountability in organizations refers to the mechanisms and processes that ensure employees and management are held responsible for their actions and decisions (Han and Hong 2019). In the context of cybersecurity, accountability mechanisms can include comprehensive standards, sanctions, capacity building, stakeholder involvement, transparency, adaptability, and inclusive deliberation to ensure robust, consistent, and responsive cybersecurity practices (Pawlak 2024). Organizations with robust cybersecurity practices are better positioned to foster a culture of accountability, as these practices often involve clear delineation of roles and responsibilities and stringent monitoring of compliance (Safitra, Lubis, and Fakhrurroja 2023)

Additionally, the effectiveness of organizational change is a critical area of study, particularly in how organizations adapt to new challenges and implement changes to address these challenges effectively (Pavel,2024). Research indicates that organizations with strong cybersecurity preparedness are more agile and better equipped to implement changes, as they possess the necessary infrastructure and processes to support such transitions (Neri, Niccolini, & Martino 2024). Effective change management in response to cybersecurity threats not only protects the organization from potential losses but also enhances overall organizational resilience (Trim and Lee 2023).
Despite the growing body of literature on cybersecurity, there is limited research on the direct relationship between cybersecurity preparedness and its impact on accountability and change effectiveness within federal agencies (Abu Sayed et al., 2023). This study aims to fill this gap by investigating how cybersecurity preparedness influences these critical organizational outcomes. By analyzing data from the 2023 Federal Employee Viewpoint Survey (FEVS), this research provides empirical evidence on the importance of cybersecurity in enhancing organizational performance and resilience in the federal sector.

2. Theoretical Framework

2.1 Cybersecurity Preparedness

The increasing frequency and sophistication of cyber-attacks necessitate robust cybersecurity preparedness strategies. Cybersecurity threats have evolved from simple viruses and malware to sophisticated attacks such as ransomware, phishing, and advanced persistent threats (APTs) (Bhardwaj 2021). Cybersecurity preparedness involves several key components, including risk assessment, incident response planning, and continuous monitoring (Shinde and Kulkarni 2021). Risk assessment serves as the foundation, focusing on identifying potential threats, vulnerabilities, and the impact of cyber incidents (Kandasamy et al. 2020). Zahid et al. (2021) emphasize the importance of a systematic approach to risk assessment, incorporating both quantitative and qualitative methods. Effective incident response planning is critical for minimizing the impact of cyber incidents. Studies by Ahmad et al. (2021) highlight the necessity of a well-defined incident response plan that includes preparation, detection, containment, eradication, recovery, and lessons learned. Continuous monitoring is essential for maintaining cybersecurity readiness. As noted by Naseer, Naseer et al. (2021), continuous monitoring enables organizations to detect and respond to threats in real-time, thereby reducing the time to mitigate potential damage.

2.2 Cybersecurity Preparedness and Accountability

Cybersecurity preparedness is a multifaceted construct that involves proactive measures to anticipate, prevent, and respond to cyber threats (Tzavara and Vassiliadis 2024). Studies indicate that well-prepared organizations not only protect their digital assets but also foster a culture of accountability (Alshaikh, 2020). Heimstädt and Dobusch (2020) argue that accountability mechanisms are essential for maintaining organizational integrity and public trust, especially in sectors dealing with sensitive information, such as federal agencies. Organizations with robust cybersecurity frameworks often exhibit clear reporting structures, transparent decision-making processes, and stringent compliance monitoring (Savaş and Karataş 2022).

Slapničar et al. (2023) found that organizations with effective IT governance, which includes cybersecurity measures, tend to have higher levels of accountability. This is because such organizations typically have clearly defined roles and responsibilities, making it easier to hold individuals accountable for their actions. Similarly, Moro-Visconti and Cesaretti (2023) highlight that comprehensive cybersecurity practices necessitate regular audits and compliance checks, further reinforcing accountability mechanisms. These findings suggest that cybersecurity preparedness is likely to have a positive impact on accountability. Thus, the study tests the following hypothesis:

H1: Better cyber security threat preparation is positively associated with greater accountability.

2.3 Cybersecurity Preparedness and Effective Change in Addressing Challenges

According to Hollands, Haensse, and Lin-Hi (2023), the ability of an organization to implement effective changes in response to challenges is critical for maintaining operational resilience. Talaja, Škokić, and Mise (2023) emphasize that organizations with strong change management capabilities can adapt more swiftly to new threats and opportunities. Thus, cybersecurity preparedness plays a significant role in this context by providing the necessary infrastructure and processes to support effective change implementation.

Savaş and Karataş (2022) suggest that organizations with robust cybersecurity measures are better positioned to address and overcome challenges. Their study indicates that cybersecurity preparedness enhances an organization's agility and responsiveness, enabling it to implement changes more effectively. This is supported by Alshaikh (2020), who found that a strong cybersecurity culture not only mitigates risks but also promotes proactive problem-solving and innovation, essential components of effective change management.

Furthermore, Tyler Moore (2010) argues that the economic implications of cybersecurity are profound, affecting not just the direct costs of breaches but also the indirect costs related to organizational efficiency and adaptability. Organizations that invest in cybersecurity are more likely to have streamlined processes and better resource allocation, contributing to more effective changes. These findings indicate that enhancing cybersecurity preparedness is likely to positively influence the effectiveness of organizational changes. Consequently, the study will test the following hypothesis:

H2: Better cyber security threat preparation is positively associated with more effective changes to address challenges.

2.4 Empirical Evidence from Federal Agencies

In the context of federal agencies, cybersecurity preparedness is particularly crucial due to the sensitive nature of the information handled. Frandell and Feeney (2022) highlight the unique challenges faced by public sector organizations in implementing effective cybersecurity measures, emphasizing the importance of a comprehensive approach that includes not only technical solutions but also employee training and awareness programs. This aligns with Hepfer and Lawrence's (2022) suggestion that cybersecurity is integral to overall organizational resilience and performance.

The Federal Employee Viewpoint Survey (FEVS) provides valuable data on cybersecurity preparedness and its potential impact on organizational outcomes such as accountability and changes in addressing challenges. The literature suggests that better cybersecurity threat preparation may be associated with greater accountability and more effective changes to address challenges (Pavel, 2024). Studies across various sectors, including federal agencies, indicate that robust cybersecurity measures can enhance organizational capabilities in accountability and adaptability. These findings highlight the importance of investing in comprehensive cybersecurity strategies to foster a culture of accountability and resilience within organizations.

2.5 Challenging Existing Theories

This study challenges existing theories in several ways, providing fresh insights into the intersection of cybersecurity, organizational accountability, and change management:

2.5.1 Cybersecurity as a Driver of Accountability:

Traditional theories often view cybersecurity primarily as a technical function aimed at protecting information assets and mitigating risks (Borky and Bradley 2019). In today's interconnected world, organizations are not only custodians of vast amounts of data but also operate under increasing scrutiny from regulatory bodies, stakeholders, and the public. Cybersecurity, therefore,

becomes a cornerstone of organizational governance and ethical responsibility. This study, however, demonstrates that cybersecurity preparedness goes beyond technical measures and significantly contributes to enhancing organizational accountability (Pavel & Pia, 2024). The study also highlights the role of leadership in driving cybersecurity initiatives. When leaders prioritize cybersecurity, they signal its importance to the entire organization, encouraging a top-down approach to security that aligns with the organization's strategic goals. This leadership commitment is essential for fostering a security-first mindset, which is integral to the broader accountability framework. By showing a strong positive association between cybersecurity measures and accountability, the study challenges the conventional notion that cybersecurity is solely a technical issue.

2.5.2 Integration with Change Management:

Existing change management theories typically focus on leadership, communication, and stakeholder engagement as primary drivers of successful organizational change (Ford, Ford, and Polin 2021). This study introduces cybersecurity preparedness as a critical factor that supports and facilitates effective change management. By highlighting how robust cybersecurity practices provide the necessary infrastructure for swift and efficient change implementation, the research challenges traditional change management models that overlook the importance of cybersecurity in organizational adaptability and resilience.

2.5.3 Contingency Theory:

Contingency Theory suggests that the best way to structure an organization depends on the specific situation it faces, and there is no one best way to manage (Mahmud, Soetanto, and Jack 2021). This study expands Contingency Theory by highlighting that cybersecurity preparedness is a critical contingency factor that influences organizational accountability and change management. It shows that robust cybersecurity practices can help organizations navigate various environmental uncertainties and complexities more effectively. The research illustrates that in environments with high cyber threats, organizations must tailor their management practices to include strong cybersecurity measures to maintain accountability and effective change management. This adaptation is necessary to respond to the specific context of increasing cyber threats and the need for data protection, thereby broadening the scope of Contingency Theory to include cybersecurity as an essential organizational variable. Furthermore, the study suggests that organizations with high cybersecurity preparedness are better equipped to implement changes quickly and effectively, responding to external pressures and internal demands with agility and resilience. This finding implies that cybersecurity is not just a technical requirement but a strategic asset that shapes organizational behavior and outcomes (Pavel & Pia, 2024).

3.Method

This study utilized data collected from the 2023 Federal Employee Viewpoint Survey (FEVS), which measures federal employees' perceptions of their work experiences. The survey included items related to cybersecurity threat preparation, accountability, and changes in addressing challenges. The key variables used in this study are detailed in the table below:

Variable	Type	Description	Response Levels
Cybersecurity Preparedness	Independent	Measured by employees' responses to the implementation of cybersecurity measures and protocols	Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, Strongly Agree
Accountability	Dependent	Measured by employees' perceptions of accountability mechanisms	Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, Strongly Agree
Changes in Addressing Challenges	Dependent	Measured by employees' perceptions of organizational changes	Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, Strongly Agree
Gender	Control	Indicating gender of participants	Male, Female
Supervisory Status	Control	Indicating whether an employee holds a supervisory role	Non-Supervisor/Team Leader, Supervisor/Manager/Executive
Age	Control	Measured in years	Under 40, 40 or older
Tenure	Control	Measured as the number of years an employee has worked in their current organization	Ten years or fewer, Eleven to 20 years, more than 20 years

Descriptive statistics were calculated to understand the distribution of responses across different levels of cybersecurity preparedness and the dependent variables. The frequency distribution table provided insights into how respondents' perceptions of cybersecurity preparedness relate to their perceptions of accountability and organizational change. Spearman's rank correlation coefficients were calculated to assess the strength and direction of the association between variables. This non-parametric method was chosen due to the ordinal nature of the survey responses. Correlations between cybersecurity preparedness, accountability, changes in addressing challenges, and control variables (gender, supervisory status, age, and tenure) were examined.

To further analyze the relationships between cybersecurity preparedness and the dependent variables (accountability and changes in addressing challenges), ordered logistic regression models were employed. This method is suitable for analyzing ordinal dependent variables and helps in understanding the probability of being in a certain category of the dependent variable based on the independent and control variables. The regression models included cybersecurity preparedness, gender, supervisory status, age, and tenure as predictors. The models were estimated using maximum likelihood estimation. The results provided coefficients, standard errors, z-values, p-values, and 95% confidence intervals for each predictor, allowing for a detailed interpretation of the relationships (Pavel, 2024).

Structural Equation Modeling (SEM) was used to provide a comprehensive analysis of the relationships between cybersecurity preparedness, accountability, and change, incorporating the control variables. The SEM approach allows for the simultaneous estimation of multiple relationships between variables, providing a more detailed understanding of the direct and indirect effects. Fit statistics such as the Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Root Mean Squared Error of Approximation (RMSEA), and Standardized Root Mean Squared Residual (SRMR) were used to assess the model fit. The SEM model was estimated using maximum likelihood estimation, and the results included coefficients, standard errors, z-values, p-values, and 95% confidence intervals for each path in the model.

4. Results

Descriptive Statistics			**Accountability**			
Cyber security preparedness						
	Strongly Disagree	**Disagree**	**Neither Agree nor Disagree**	**Agree**	**Strongly Agree**	**Total**
Strongly Disagree	2,320	867	2,008	3,063	2,928	11,186
Disagree	700	1,336	3,141	7,746	5,234	18,157
Neither Agree nor Disagree	1,402	2,097	13,856	27,804	20,203	65,362
Agree	2,228	5,017	23,818	148,207	139,193	318,463
Strongly Agree	626	863	4,012	23,309	149,058	177,868
Total	7,276	10,180	46,835	210,129	316,616	591,036

Table: 1

Descriptive Statistics			**Change**			
Cyber security preparedness						
	Strongly Disagree	**Disagree**	**Neither Agree nor Disagree**	**Agree**	**Strongly Agree**	**Total**
Strongly Disagree	7,528	1,535	1,037	574	197	10,871
Disagree	4,881	5,209	4,024	2,570	571	17,255
Neither Agree nor Disagree	10,803	12,099	23,900	12,321	2,747	61,870
Agree	21,312	39,493	81,485	131,991	28,976	303,257
Strongly Agree	5,174	8,441	19,566	48,982	91,054	173,217
Total	49,698	66,777	130,012	196,438	123,545	566,217

Table: 2

The descriptive statistics (table 1) reveal a clear trend in the relationship between cybersecurity preparedness and accountability. A significant number of respondents who agree or strongly agree with the statement about their organization's cybersecurity preparedness also agree or strongly agree with statements about accountability. This suggests a potential positive relationship between these two variables. The analysis of the relationship between cybersecurity preparedness and organizational change (table: 2) provides significant insights. The descriptive statistics reveal a clear trend: a substantial number of respondents who agree or strongly agree with their organization's cybersecurity preparedness also perceive positive changes within their organization. This suggests a potential positive relationship between these two variables.

Spearman's Rank Correlation						
Number of observations=	533,389					
	Cyber security preparedness	**Accountability**	**Gender**	**Supervisory status**	**Age**	**Tenure**
Cyber security preparedness	1					
Accountability	0.4131	1				
Gender	0.0219	0.0139	1			
Supervisory status	0.03	0.039	-0.075	1		
Age	0.0445	0.0023	-0.039	0.1517	1	
Tenure	0.0063	-0.0107	-.0007	0.2251	0.453	1

Table: 4

The Spearman's rank correlation coefficients provide further insight into this relationship. The correlation between cybersecurity preparedness and accountability (table:3) is 0.4131, indicating a positive association. This means that as cybersecurity preparedness improves, perceptions of accountability tend to increase as well. Other variables such as gender, supervisory status, age, and tenure show relatively weak correlations with both cybersecurity preparedness and accountability, suggesting these factors have less influence on the relationship. The correlation between cybersecurity preparedness and change (table: 4) is 0.496, indicating a positive association. This suggests that improvements in cybersecurity preparedness are associated with more effective organizational changes. Other variables such as gender, supervisory status, age, and tenure show weaker correlations with both cybersecurity preparedness and change, indicating these factors have less influence on the relationship.

Iteration 0: Log likelihood = -543164.52						
Iteration 1: Log likelihood = -498968.66						
Iteration 2: Log likelihood = -498305.18						
Iteration 3: Log likelihood = -498302.74						
Iteration 4: Log likelihood = -498302.74						Number of obs = 533,389
						LR chi2(5) = 89723.58
						Prob > chi2 = 0.0000
Log likelihood = -498302.74						Pseudo R2 = 0.0826
Ordered logistic regression						
Accountability	**Coefficient**	**Std. err.**	**z**	**P>z**	**[95% conf.**	**[95% conf. interval]**
Cyber security preparedness	1.041998	0.0036935	282	0	1.034758	1.049237
Gender	0.0135877	0.0055761	2.44	0.015	0.0026587	0.0245168

Supervisory status	0.189419	0.0069656	27.2	0	0.1757666	0.2030714
Age	-0.0782445	0.0072423	-10.8	0	-0.0924392	-0.0640498
Tenure	-0.0399685	0.0039431	-10.1	0	-0.047497	-0.0322401
/cut1	-0.5340733	0.0233555			-0.5798491	-0.4882974
/cut2	0.4209601	0.021554			0.378715	0.4632053
/cut3	1.903082	0.0209547			1.862011	1.944152
/cut4	4.13696	0.021587			4.094651	4.17927

Table: 5

Iteration 0: Log likelihood = -772220.57						
Iteration 1: Log likelihood = -700269.51						
Iteration 2: Log likelihood = -697848.23						
Iteration 3: Log likelihood = -697839.16						
Iteration 4: Log likelihood = -697839.16						
Ordered logistic regression					Number of obs =	515,661
					LR chi2(5) =	148762.83
					Prob > chi2 =	0
Log likelihood = -697839.16					Pseudo R2 =	0.0963
Change	**Coefficient**	**Std. err.**	**z**	**P>z**	**[95% conf.**	**interval]**
Cyber security preparedness	1.301989	0.0036566	356.07	0	1.294822	1.309156
Gender	-0.0220409	0.0051355	-4.29	0	-0.0321063	-0.0119756
Supervisory Status	0.1632929	0.0063368	25.77	0	0.150873	0.1757128
Age	0.0499945	0.0066598	7.51	0	0.0369416	0.0630474
Tenure	-0.0943083	0.0036301	-25.98	0	-0.1014231	-0.0871935
/cut1	2.549773	0.0199373			2.510696	2.588849
/cut2	3.734993	0.0200738			3.695649	3.774337
/cut3	5.032677	0.0205122			4.992474	5.07288
/cut4	6.888256	0.0214378			6.846238	6.930273

Table: 6

The ordered logistic regression model provides a more detailed analysis. The coefficient for cybersecurity preparedness (table: 5) is 1.041998 ($p < 0.001$), indicating a significant positive association with accountability. This strongly supports Hypothesis 1 (H1), which posits that better cybersecurity threat preparation is associated with greater accountability. The model also shows that gender has a small but statistically significant positive association with accountability, while supervisory status has a more substantial positive association. Conversely, age and tenure are negatively associated with accountability, with older and longer-tenured employees perceiving lower levels of accountability.

On the other hand, the coefficient for cybersecurity preparedness (table: 6) is 1.301989 ($p < 0.001$), indicating a significant positive association with effective organizational changes. This strongly supports Hypothesis 2 (H2), which posits that better cybersecurity preparedness leads to more effective changes in addressing organizational challenges. The model also shows that gender has a small but statistically significant negative association with perceived effective changes, while supervisory status has a positive association, suggesting that individuals in supervisory roles are more likely to perceive changes as effective. Age also shows a positive association, indicating that older employees may view changes more favorably. Conversely, tenure has a negative association, suggesting that longer-tenured employees may be less likely to perceive changes as effective.

Endogenous variables							
Observed: Accountability							
Exogenous variables							
Observed: Cyber_security_preparedness Gender Supervisory_status Age Tenure							
Fitting target model:							
Iteration 0: Log likelihood = -2792361							
Iteration 1: Log likelihood = -2792361							
Structural equation model					Number of obs = 533,389		
Estimation method: ml							
Log likelihood = -2792361							
		OIM					
	Coefficient	std. err.	z	p> |z |	[95% conf. interval]		
Structural							
Accountability							
Cyber_security_preparedness	0.3772533	0.001213	311.04	0	0.374876	0.379631	
Gender	0.0084368	0.002023	4.17	0	0.004472	0.012402	
Supervisory_status	0.0671048	0.002505	26.78	0	0.062194	0.072015	
Age	-0.010599	0.002609	-4.06	0	-0.01571	-0.00549	
Tenure	-0.0110765	0.001435	-7.72	0	-0.01389	-0.00826	
_cons	2.799775	0.007421	377.29	0	2.78523	2.814319	
var(e.Accountability)	0.5398098	0.001045			0.537765	0.541862	
LR test of model vs. saturated: chi2(0) = 0.00					Prob> chi2 = .		

Table: 7

Fit statistic	**Value**	**Description**
Likelihood ratio		
chi2_ms(0)	0	model vs. saturated
p > chi2		
chi2_bs(5)	90218.057	baseline vs. saturated
p > chi2	0	
Population error		
RMSEA	0	Root mean squared error of approximation
"90% CI, lower bound"	0	
upper bound	0	
pclose	1	Probability RMSEA <= 0.05
Information criteria		
AIC	5.59E+06	Akaike's information criterion
BIC	5.59E+06	Bayesian information criterion

Baseline comparison		
CFI	1	Comparative fit index
TLI	1	Tucker-Lewis index
Size of residuals		
SRMR	0	Standardized root mean squared residual
CD	0.156	Coefficient of determination

Table: 8

Endogenous variables						
Observed: Change						
Exogenous variables						
Observed: Cyber_security_preparedness Gender Supervisory_status Age Tenure						
Fitting target model						
Iteration 0: Log likelihood = -2887887.2						
Iteration 1: Log likelihood = -2887887.2						
Structural equation model						
Number of obs = 515,661						
Estimation method: ml						
Log likelihood = -2887887.2						
		OIM				
	Coefficient	std. err.	z	p>| z |	[95% conf. interval]	
Structural						
Change						
Cyber_security_preparedness	0.693569	0.001758	394.59	0	0.690124	0.697014
Gender	-0.003896	0.00294	-1.33	0.185	-0.00966	0.001867
Supervisory_status	0.085211	0.003613	23.59	0	0.07813	0.092292
Age	0.041678	0.003793	10.99	0	0.034245	0.049112
Tenure	-0.054062	0.002087	-25.99	0	-0.05815	-0.04997
_cons	0.601435	0.010767	55.86	0	0.580333	0.622538
var(e.Change)	1.101416	0.002169			1.097173	1.105676
LR test of model vs. saturated: chi2 (0) = 0.00					Prob > chi2 = .	

Table: 9

Fit statistic	Value	Description
Likelihood ratio		
chi2_ms(0)	0	model vs. saturated
p > chi2		
chi2_bs(5)	138010.727	baseline vs. saturated
p > chi2	0	
Population error		
RMSEA	0	Root mean squared error of approximation
90% CI, lower bound	0	

upper bound	0	
pclose	1	Probability RMSEA <= 0.05
Information criteria		
AIC	5.78E+06	Akaike's information criterion
BIC	5.78E+06	Bayesian information criterion
Baseline comparison		
CFI	1	Comparative fit index
TLI	1	Tucker-Lewis index
Size of residuals		
SRMR	0	Standardized root mean squared residual
CD	0.235	Coefficient of determination

Table: 10

The Structural Equation Model (SEM) further elucidates the relationships between these variables. The SEM results indicate the following: For Accountability (table: 7), Cybersecurity Preparedness has a coefficient of 0.3772533 ($p < 0.001$), indicating a significant positive relationship. This suggests that better cybersecurity preparedness is associated with higher levels of accountability within organizations. Gender has a coefficient of 0.0084368 ($p = 0.000$), indicating a small but significant positive relationship, suggesting that gender has a minor but statistically significant effect on perceptions of accountability. Supervisory Status has a coefficient of 0.0671048 ($p < 0.001$), showing a significant positive relationship, indicating that individuals in supervisory roles perceive higher levels of accountability. Age has a coefficient of -0.0105989 ($p < 0.001$), indicating a significant negative relationship, suggesting that older employees perceive lower levels of accountability. Tenure has a coefficient of -0.0110765 ($p < 0.001$), indicating a significant negative relationship (Pavel, 2024), suggesting that longer-tenured employees perceive lower levels of accountability.

For Change (table: 9), Cybersecurity Preparedness has a coefficient of 0.6935689 ($p < 0.001$), indicating a significant positive relationship. This suggests that better cybersecurity preparedness is strongly associated with more effective organizational changes. Gender has a coefficient of -0.0038963 ($p = 0.185$), indicating no significant relationship, suggesting that gender does not significantly affect perceptions of change. Supervisory Status has a coefficient of 0.0852111 ($p < 0.001$), indicating a significant positive relationship, showing that individuals in supervisory roles are more likely to perceive changes as effective. Age has a coefficient of 0.0416783 ($p < 0.001$), indicating a significant positive relationship, suggesting that older employees perceive changes more favorably. Tenure has a coefficient of -0.0540622 ($p < 0.001$), indicating a significant negative relationship, suggesting that longer-tenured employees are less likely to perceive changes as effective.

The fit statistics (table: 8 & 10) for the SEM model indicate an excellent fit with the data, with a Comparative Fit Index (CFI) of 1.000, a Tucker-Lewis Index (TLI) of 1.000, a Root Mean Squared Error of Approximation (RMSEA) of 0.000, and a Standardized Root Mean Squared Residual (SRMR) of 0.000. The likelihood ratio test, AIC, and BIC values also suggest that the model is well-specified. These fit statistics indicate that the SEM model accurately represents the relationships between the variables, providing a reliable basis for interpreting the results.

5. Discussion

The findings contribute to the theoretical understanding of the relationship between cybersecurity preparedness and organizational outcomes. The study supports integrating cybersecurity frameworks into broader organizational theories of performance and resilience (Hasani et al. 2023). Future research can explore specific mechanisms through which cybersecurity preparedness influences these outcomes and examine these relationships in different organizational contexts. The study provides empirical evidence supporting existing theories on the importance of cybersecurity in enhancing organizational effectiveness, suggesting that cybersecurity preparedness should be a critical factor in models of organizational change and resilience. Researchers can further investigate how aspects like employee training, technology infrastructure, and policy enforcement contribute to positive organizational outcomes.

The study demonstrates how cybersecurity measures can directly influence organizational culture and operational effectiveness. Suggested actionable steps for enhancing organizational performance through better cybersecurity practices include developing comprehensive cybersecurity strategies, conducting regular training and awareness programs, performing risk assessments and audits, establishing clear accountability mechanisms , enhancing supervisory and leadership involvement,

implementing continuous monitoring and incident response plans, promoting a culture of security awareness, allocating adequate resources, and collaborating with other agencies and organizations. Engaging in information sharing and collaboration enhances overall cybersecurity posture by leveraging shared knowledge and resources (Gil-Garcia and Sayogo 2016). Ensuring sufficient resources for cybersecurity initiatives, including advanced technologies, skilled professionals, and ongoing training, is essential (Shillair et al. 2022). Fostering a culture where cybersecurity is seen as a shared responsibility encourages employees to report suspicious activities and reward proactive security behaviors (Reeves, Delfabbro, and Calic 2021).

The study's findings significantly contribute to collaborative governance by demonstrating how robust cybersecurity practices can enhance accountability and foster a collaborative environment. By ensuring the protection of shared information and resources, cybersecurity measures build trust among stakeholders, crucial for effective collaboration (Housen-Couriel 2022). Regular risk assessments and continuous monitoring support a unified approach to addressing cyber threats, essential for interagency collaborations (Radanliev 2024). Clear accountability mechanisms and a culture of security awareness create a transparent and responsible environment conducive to collaboration (Blum 2020). The study also highlights the role of cybersecurity preparedness in enhancing organizational resilience, showing that integrating cybersecurity into change management processes enables organizations to swiftly mitigate potential disruptions. This adaptability is crucial in the public sector, where the ability to respond to emerging threats and opportunities can significantly impact service delivery and public trust (Awais et al. 2023).

The focus on cybersecurity training and awareness programs underscores the importance of human resource management in cybersecurity preparedness. Continuous training ensures employees are updated on the latest threats and best practices, creating a culture of security awareness (McIlwraith 2021). Leadership training programs equip managers to promote cybersecurity within their teams, setting the tone for a security-conscious culture. Investing in cybersecurity training and development enhances employee engagement and retention, as employees feel valued and motivated (Reeves, Delfabbro, and Calic 2021). HRM plays a critical role in recruiting and selecting cybersecurity talent, ensuring new hires are aligned with the organization's security culture (Gilch and Sieweke 2021). Performance management systems should incorporate cybersecurity-related objectives, and incentive programs can motivate employees to adhere to security expectations. HRM can also facilitate cross-functional collaboration, integrate cybersecurity policies, and support employee well-being, all contributing to a secure organizational environment.

For policymakers, enhancing cybersecurity preparedness within federal agencies should be a strategic priority. In addition to the existing measures of regular training, clear guidelines, and resource allocation, policies should focus on the integration of advanced technologies such as artificial intelligence (AI) and machine learning (ML) to proactively detect and respond to cyber threats. Establishing public-private partnerships can leverage the expertise and innovation of the private sector to bolster federal cybersecurity efforts (Carr 2016). Policymakers should also consider implementing standardized cybersecurity frameworks across all federal agencies to ensure consistency and comprehensive coverage.

Furthermore, developing a centralized cybersecurity command center can streamline incident response and facilitate coordinated efforts during a cyber-attack (Lehto and Limnéll 2020). This command center can serve as a hub for real-time threat intelligence sharing and collaborative defense strategies. Additionally, policies should mandate periodic cybersecurity drills and simulations to prepare agencies for potential cyber incidents, ensuring that all personnel are familiar with their roles and responsibilities during a crisis.

6. Conclusion

This study demonstrates that cybersecurity preparedness significantly enhances organizational accountability and effective change management within federal agencies. By analyzing data from the 2023 Federal Employee Viewpoint Survey (FEVS) and using robust analytical methods, the findings reveal that cybersecurity is not merely a technical requirement but a strategic asset integral to organizational performance and resilience. The positive associations between cybersecurity measures and key organizational outcomes highlight the need for comprehensive cybersecurity strategies, continuous monitoring, and advanced technologies. This research bridges the gap between cybersecurity and organizational performance theories, suggesting that cybersecurity preparedness should be embedded within broader organizational strategies. Future research could further explore the intricate mechanisms through which cybersecurity influences various organizational dimensions and its potential sector-specific impacts.

Finally, the study underscores the transformative impact of cybersecurity preparedness on federal agencies, advocating for its integration into strategic planning to enhance accountability, adaptability, and overall organizational effectiveness. This

approach safeguards information assets and strengthens the foundation for resilient and accountable federal operations, ultimately contributing to the public good.

Funding: This research received no external funding
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Abu S, M., Tayaba, M., Islam, M. T., Pavel, M. E. U. I., Mia, M. T., Ayon, E. H., Nobe, N., & Ghosh, B. P. (2023). Parkinson's Disease Detection through Vocal Biomarkers and Advanced Machine Learning Algorithms. Journal of Computer Science and Technology Studies, 5(4), 142–149. https://doi.org/10.32996/jcsts.2023.5.4.14
[2] Alshaikh, Moneer. 2020. "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective." *Computers & Security* 98: 102003. https://doi.org/10.1016/j.cose.2020.102003.
[3] Ansell, Chris, and Alison Gash. 2008. "Collaborative Governance in Theory and Practice." *Journal of Public Administration Research and Theory* 18 (4): 543–571. https://doi.org/10.1093/jopart/mum032.
[4] Ahmad, Atif, Sean B. Maynard, Kevin C. Desouza, James Kotsias, Monica T. Whitty, and Richard L. Baskerville. 2021. "How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice." *Computers & Security* 101: 102122. https://doi.org/10.1016/j.cose.2020.102122.
[5] Awais, Muhammad, Amanat Ali, Muhammad Sajid Khattak, Muhammad Irfanullah Arfeen, Muhammad Azam I. Chaudhary, and Aleena Syed. 2023. "Strategic Flexibility and Organizational Performance: Mediating Role of Innovation." *Sage Open* 13 (2). https://doi.org/10.1177/21582440231181432.
[6] Bhardwaj, Akashdeep. 2021. "Cybersecurity Incident Response Against Advanced Persistent Threats (APTs)." In *Security Incidents & Response Against Cyber Attacks*, edited by A. Bhardwaj and V. Sapra, 163-183. EAI/Springer Innovations in Communication and Computing. Cham: Springer. https://doi.org/10.1007/978-3-030-69174-5_9.
[7] Blum, Dan. 2020. "Strengthen Security Culture Through Communications and Awareness Programs." In *Rational Cybersecurity for Business*, 69-85. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-5952-8_4.
[8] Borky, John M., and Thomas H. Bradley. 2019. "Protecting Information with Cybersecurity." In *Effective Model-Based Systems Engineering*. Springer, Cham. https://doi.org/10.1007/978-3-319-95669-5_10.
[9] Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92 (1): 43-62. https://doi.org/10.1111/1468-2346.12504.
[10] Cristofoli, Daniela, Marco Meneguzzo, and Norma Riccucci. 2016. "Collaborative Administration: The Management of Successful Networks." *Public Management Review* 19 (3): 275–83. https://doi.org/10.1080/14719037.2016.1209236.
[11] Ford, Jeffrey, Laurie Ford, and Beth Polin. 2021. "Leadership in the Implementation of Change: Functions, Sources, and Requisite Variety." *Journal of Change Management* 21 (1): 87-119. https://doi.org/10.1080/14697017.2021.1861697.
[12] Frandell, Ashlee, and Mary Feeney. 2022. "Cybersecurity Threats in Local Government: A Sociotechnical Perspective." *The American Review of Public Administration* 52 (8): 558-572. https://doi.org/10.1177/02750740221125432.
[13] Gil-Garcia, J. Ramon, and Djoko Sigit Sayogo. 2016. "Government Inter-Organizational Information Sharing Initiatives: Understanding the Main Determinants of Success." *Government Information Quarterly* 33 (3): 572-582. https://doi.org/10.1016/j.giq.2016.01.006.
[14] Gilch, Phyllis Messalina, and Jost Sieweke. 2021. "Recruiting Digital Talent: The Strategic Role of Recruitment in Organisations' Digital Transformation." *German Journal of Human Resource Management* 35 (1): 53-82. https://doi.org/10.1177/2397002220952734.
[15] Han, Yousueng, and Sounman Hong. 2019. "The Impact of Accountability on Organizational Performance in the U.S. Federal Government: The Moderating Role of Autonomy." *Review of Public Personnel Administration* 39 (1): 3-23. https://doi.org/10.1177/0734371X16682816.
[16] Hasani, Tahereh, Norman O'Reilly, Ali Dehghantanha, Davar Rezania, and Nadège Levallet. 2023. "Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance." *SN Business & Economics* 3: 97. https://doi.org/10.1007/s43546-023-00477-6.
[17] Hepfer, Manuel, and Thomas B. Lawrence. 2022. "The Heterogeneity of Organizational Resilience: Exploring Functional, Operational, and Strategic Resilience." *Organization Theory* 3 (1): 1-22.
[18] Heimstädt, Maximilian, and Leonhard Dobusch. 2020. "Transparency and Accountability: Causal, Critical and Constructive Perspectives." *Organization Theory* 1 (4): 1-24. https://doi.org/10.1177/2631787720964216.
[19] Herath, Tejaswini , and H. Raghav Rao. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures, and Perceived Effectiveness." *Decision Support Systems* 47 (2): 154-165.
[20] Hollands, Lisa, Lukas Haensse, and Nick Lin-Hi. 2023. "The How and Why of Organizational Resilience: A Mixed-Methods Study on Facilitators and Consequences of Organizational Resilience Throughout a Crisis." *The Journal of Applied Behavioral Science*. https://doi.org/10.1177/00218863231165785.
[21] Hood, Christopher. 1991. "A Public Management for All Seasons?" *Public Administration* 69 (1): 3-19. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x.
[22] Hossain, Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, and Yue Xu. 2024. "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework." *Applied Sciences* 14 (13): 5501. https://doi.org/10.3390/app14135501.
[23] Housen-Couriel, Deborah. 2022. "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace." In *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, edited by Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen, 39-63. Cambridge: Cambridge University Press.

[24] Johnson, Thomas A., ed. 2015. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. 1st ed. Routledge. https://doi.org/10.1201/b18335.
[25] Kandasamy, Kamalanathan, Sethuraman Srinivas, Krishnashree Achuthan, and Venkat P. Rangan. "IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process." *EURASIP Journal on Information Security* 2020, no. 8 (2020). https://doi.org/10.1186/s13635-020-00111-0.
[26] Lapuente, Victor, and Steven Van de Walle. 2020. "The Effects of New Public Management on the Quality of Public Services." *Governance* 33: 461-475. https://doi.org/10.1111/gove.12502.
[27] Lehto, Martti, and Jarno Limnéll. 2020. "Strategic Leadership in Cyber Security, Case Finland." *Information Security Journal: A Global Perspective* 30 (3): 139–148. https://doi.org/10.1080/19393555.2020.1813851.
[28] Li, Yuchong, and Qinghui Liu. 2021. "A Comprehensive Review Study of Cyber-attacks and Cybersecurity: Emerging Trends and Recent Developments." *Energy Reports* 7: 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.078.
[29] Mahmud, Muaz, Danny Soetanto, and Sarah Jack. 2021. "A Contingency Theory Perspective of Environmental Management: Empirical Evidence from Entrepreneurial Firms." *Journal of General Management* 47 (1): 3-17. https://doi.org/10.1177/0306307021991489.
[30] McIlwraith, Angus. 2021. *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. 2nd ed. London: Routledge. https://doi.org/10.4324/9780429281785.
[31] Moore, Tyler. 2010. "The Economics of Cybersecurity: Principles and Policy Options." *International Journal of Critical Infrastructure Protection* 3 (3-4): 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002.
[32] Moro-Visconti, Roberto, and Andrea Cesaretti. 2023. "Cybersecurity." In *Digital Token Valuation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-42971-2_10.
[33] Naseer, Ayesha, Humza Naseer, Atif Ahmad, Sean B. Maynard, and Adil Masood Siddiqui. 2021. "Real-Time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-Based Analysis."*International Journal of Information Management* 59: 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334.
[34] Neri, Martina, Federico Niccolini, and Luigi Martino. 2024. "Organizational Cybersecurity Readiness in the ICT Sector: A Quanti-Qualitative Assessment." *Information and Computer Security* 32 (1): 38-52. https://doi.org/10.1108/ICS-05-2023-0084.
[35] Pavel, M. U. I. (2024). *[Review of the book Street-Level Public Servants: Case Studies for a New Generation of Public Administration, by S. R. Rinfret (Ed.)]. Public Administration Review, 85*(1), 252-254. https://doi.org/10.1111/puar.13913
[36] Pavel, M. E. U. I. (2024). The politics of collaborative public management: A primer [Review of the book The Politics of Collaborative Public Management: A Primer, by R. Agranoff & A. Kolpakov]. Public Administration. https://doi.org/10.1111/padm.12990
[37] Pavel, M. E. U. I. (2024). Do governance structures matter to service provision? International Journal of Arts and Humanities Studies, 4(1), 51 61. https://doi.org/10.32996/ijahs.2024.4.1.8
[38] Pavel, M. E. U. I., & Pia, S. A. (2024). *Balancing acts: Exploring the intersection of cultural understanding and technical support in local government strategies for immigrant micro-financing. International Journal of Arts and Humanities Studies, 4*(1), 35-42. https://doi.org/10.32996/ijahs.2024.4.1.6
[39] Pavel, M. E. U. I., & Pia, S. A. (2024). Exploring the discrepancy between marketing focused on racial and ethnic diversity and the availability of support for immigrant entrepreneurs in economic development. Journal of Humanities and Social Sciences Studies, 6(2), 73-84. https://doi.org/10.32996/jhsss.2024.6.2.10
[40] Pavel, M. U. I. (2023, December 11). Integrating America: Revealing the Complex Tapestry of Immigrant Engagement and Local Governance Dynamics. https://doi.org/10.31235/osf.io/wyz96
[41] Pavel, Md Eyasin Ul Islam. (2024). Building Equity: Exploring the Impact of Sustainable Urban Policies on Social Welfare and Inclusivity. *British Journal of Environmental Studies*, *4*(1), 18-28. https://doi.org/10.32996/bjes.2024.4.1.3
[42] Pia, S. A. (2017). Revisiting Brenda Almond's View of Human Bonds. Philosophy and Progress, 61(1–2). https://doi.org/10.3329/pp.v61i1-2.44207
[43] Pia, S. A. (2018). Climate Change and our Moral Obligations to Future Generations: A Critical Analysis. Jibon Darshon, 8, 141-160. https://www.researchgate.net/publication/365360392_Climate_Change_and_Our_Moral_Obligations_to_Future_Generations
[44] Pia, S. A. (2019). Elizabeth Telfer's View on Self-Respect: An Applied Ethical Analysis. Jibon Darshon, 9, 269- 281. https://www.researchgate.net/publication/365355031_Elizabeth_Telfer's_View_on_Self-Respect_An_Applied_Ethical_Analysis
[45] Pawlak, Patryk. 2024. "The Pursuit of Positive Accountability in the Cyber Domain." *Global Policy* 15: 142-148. https://doi.org/10.1111/1758-5899.13302.
[46] Peters, B. Guy. 2016. *The Politics of Bureaucracy: An Introduction to Comparative Public Administration*. Routledge.
[47] Prümmer, Julia, Tommy van Steen, and Bibi van den Berg. 2024. "A Systematic Review of Current Cybersecurity Training Methods." *Computers & Security* 136: 103585. https://doi.org/10.1016/j.cose.2023.103585.
[48] Radanliev, Petar. 2024. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Security Technology*, February, 1–51. https://doi.org/10.1080/23742917.2024.2312671.
[49] Reeves, Andrew, Paul Delfabbro, and Dragana Calic. 2021. "Encouraging Employee Engagement with Cybersecurity: How to Tackle Cyber Fatigue." *Sage Open* 11 (1). https://doi.org/10.1177/21582440211000049.
[50] Safitra, Muhammad Fakhrul., Muharman Lubis, and Hanif Fakhrurroja. 2023. "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity." *Sustainability* 15 (18): 13369. https://doi.org/10.3390/su151813369.
[51] Sayed, M. A., Ahamed, S., Cao, D. M., Pavel, M. E. U. I., Sarkar, M., & Mia, M. T. (2023). Parkinson's Disease Detection through Vocal Biomarkers and Advanced Machine Learning Algorithms: A Comprehensive Study. arXiv preprint arXiv:2311.05435.
[52] Shillair, Ruth, Patricia Esteve-González, William H. Dutton, Sadie Creese, Eva Nagyfejeo, and Basie von Solms. 2022. "Cybersecurity Education, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise." *Computers & Security* 119: 102756. https://doi.org/10.1016/j.cose.2022.102756.

[53] Shinde, Nivedita, and Priti Kulkarni. "Cyber Incident Response and Planning: A Flexible Approach." *Computer Fraud & Security* 2021, no. 1 (January 2021): 14-19. https://doi.org/10.1016/S1361-3723(21)00009-9.
[54] Slapničar, Sergeja, Micheal Axelsen, Ivano Bongiovanni, and David Stockdale. 2023. "A Pathway Model to Five Lines of Accountability in Cybersecurity Governance." *International Journal of Accounting Information Systems* 51: 100642. https://doi.org/10.1016/j.accinf.2023.100642.
[55] Talaja, Anita, Vlatka Škokić, and Nikol Mise. 2023. "Organizational Change Capability and Ambidexterity: The Mediating Role of Innovativeness and Responsiveness." *Cogent Business & Management* 10 (3): 1-16. https://doi.org/10.1080/23311975.2023.2279380.
[56] Trim, Peter R. J., and Yang-Im Lee. 2023. "Managing Cybersecurity Threats and Increasing Organizational Resilience." *Big Data and Cognitive Computing* 7 (4): 177. https://doi.org/10.3390/bdcc7040177.
[57] Tzavara, Vasiliki, and Savvas Vassiliadis. 2024. "Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review." *International Journal of Information Security* 23: 1695-1719. https://doi.org/10.1007/s10207-023-00811-x.
[58] Yue, Yang, and Joseph Z. Shyu. 2024. "A Paradigm Shift in Crisis Management: The Nexus of AGI-Driven Intelligence Fusion Networks and Blockchain Trustworthiness." *Journal of Contingencies and Crisis Management* 32 (1). https://doi.org/10.1111/1468-5973.12541.
[59] Zahid, Maryam, Irum Inayat, Maya Daneva, and Zahid Mehmood. "Security Risks in Cyber Physical Systems—A Systematic Mapping Study." *Journal of Software: Evolution and Process* 33, no. 9 (2021): e2346. https://doi.org/10.1002/smr.2346.

Data citation:
Office of Personnel Management (OPM). "Federal Employee Viewpoint Survey (FEVS)." OPM.gov. Accessed July 28, 2024. https://www.opm.gov/fevs/public-data-file/.