Scientific Research Publishing

Open Journal of Social Sciences, 2026, 14(6), 293-306
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

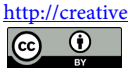
Cybersecurity Risks and Preparedness Strategies in the Remote Work Set-Up among BPO Enterprises in Nueva Ecija

Shaira Portia Villanueva Arevalo*, Dulce Amor Salvio Padilla

Graduate School, Wesleyan University Philippines, Cabanatuan City, Philippines
Email: *shairaportia@gmail.com

How to cite this paper: Arevalo, S. P. V., & Padilla, D. A. S. (2026). Cybersecurity Risks and Preparedness Strategies in the Remote Work Set-Up among BPO Enterprises in Nueva Ecija. *Open Journal of Social Sciences, 14,* 293-306.
https://doi.org/10.4236/jss.2026.146017

Received: May 8, 2026
Accepted: June 15, 2026
Published: June 18, 2026



Abstract

This study examined how BPO employees' socio-demographic characteristics relate to their perceptions of organizational cybersecurity threats and their use of technology-based readiness measures. It also includes how those measures are associated with incident frequency in the sector. Gathering information on respondents' education, employment status, monthly income, years of experience, and service category, along with their perceptions of the prevalence of phishing, malware, and unauthorized access and their reported use of MFA, firewalls/IDS, and VPNs. The study explored relationships among demographics, risk perception, technical readiness, and reported incidents. The analysis finishes with a focused cybersecurity mitigation action plan that prioritizes the identified critical issues, objectives, strategies/interventions, responsible unit, schedule, and anticipated outcomes.

Keywords

BPO, Cybersecurity Risk, Risk Mitigation, Socio-Demographics, Technical Preparedness Strategies

1. Introduction

The term "Business Process Outsourcing" (BPO) refers to the practice of delegating information technology-intensive corporate tasks to third-party organizations (Trefis Team, 2015). The BPO sector in the Philippines is a significant economic driver. Because it deals with a significant amount of sensitive foreign data, the cybersecurity infrastructure of the organization is a cause for concern not only for the Philippines but also for the rest of the globe. A new set of cybersecurity challenges has arisen for Philippine business process outsourcing

organizations as they make the switch to remote employment (The Asia Foundation, 2022). Hackers now have additional means to gain access to systems through insecure home networks and unmanaged personal devices as a result of this move, which has made existing cybersecurity flaws wider (The Asia Foundation, 2022).

Even while certain businesses, such as BPO, have started to address these challenges, the majority of research continues to concentrate on metropolitan areas and national data as a whole. As a result, there has been limited examination of semi-urban or rural regions, such as Nueva Ecija. Furthermore, despite the fact that research has demonstrated that technical controls reduce risk, there is a lack of comprehension regarding the precise links that exist between socio-demographic variables, technical preparedness techniques, and the frequency of security events in decentralized teams. Despite the government regulations, compliance varies across sectors (Department of Information and Communications Technology, 2022).

This study tried to answer the following to explored relationships among demographics, risk perception, technical readiness, and reported incidents: 1) the socio-demographic profile of the respondents be described in terms of: Highest educational attainment, Employment status, estimated monthly income, years of experience, BPO service category currently employed; 2) the cybersecurity risks be described by respondents in the organization in terms of: Phishing, Malware, Unauthorized access; 3) the technical preparedness strategies be described in terms of cybersecurity risk mitigation: Multi-factor authentication (MFA), Firewalls and intrusion detection systems, Virtual Private Networks (VPNs); 4) the significant relationship between respondents' socio-demographic profile and their descriptions of cybersecurity risks; 5) the significant relationship between technical preparedness strategies and the frequency of reported cybersecurity incidents; 6) the significant relationship between respondents' socio-demographic profiles and how they describe technical preparedness strategies.

Hypotheses include: 1) There is no significant relationship between the socio-demographic profile of the respondents and their description of cybersecurity risk. 2) There is no significant relationship between technical preparedness strategies and the frequency of reported cybersecurity incidents. 3) There is no significant relationship between the socio-demographic profile of the respondents and how they describe technical preparedness strategies.

2. Methodology

Within the context of Business Process Outsourcing (BPO) companies in Nueva Ecija, this study employed a quantitative correlational research approach in order to investigate the connections that exist between cybersecurity risk exposure, preparedness strategies, and business resilience. Because it made it easier to investigate hypotheses regarding the connections between these variables without affecting any of the conditions, this approach is particularly suitable for naturally oc-

curring organizational practices in remote work environments. It is an excellent example of how to conduct research.

This study is to investigates how BPO employees in Nueva Ecija manage cybersecurity threats in remote or hybrid work settings between the months of January 2020 and June 2025. The scope of this investigation will include the COVID-19 transition as well as current trends in remote work. It will be essential to have a comprehensive understanding of the risk assessment, technological safeguards, organizational management, and instructional components of cybersecurity resilience.

The respondents were 105 employees of business process outsourcing (BPO) enterprises and are located in the province of Nueva Ecija. These employees were involved in working remotely or in hybrid arrangements.

The researcher collected data by use of a questionnaire form that composed of socio-demographic and Likert scale questions. It was organized into three main sections to capture background, perceptions, and practical controls. 1) Socio demographic profile, respondents provided information on their highest educational attainment, employment status, estimated monthly income, years of BPO experience, and BPO service category. 2) Cybersecurity risk perceptions, a series of Likert scale items measured perceived severity and vulnerability to threats such as phishing, malware, and unauthorized access. 3) Preparedness strategies, items assessed the presence and use of technical controls, including multi factor authentication, firewalls/IDS, and VPNs, to gauge how well organizations and individuals are positioned to prevent and respond to incidents.

For the purpose of ensuring that the questionnaire is both clear and reliable, it was tested prior to use. Employees, supervisors, and information technology and security personnel from business process outsourcing (BPO) companies in Nueva Ecija who are directly involved in remote work operations were among the participants. For the purpose of analyzing the data and evaluating the hypotheses of the study, inferential statistical tests were considered. It is possible to evaluate the strength and direction of correlations between risks, strategies, and preparedness results by using the Pearson correlation. The study determined the extent to which organizational impediments have a predictive impact on the implementation of cybersecurity operations.

3. Results and Discussion

3.1. Socio-Demographic Profile of the Respondents

Table 1 shows the data gathered on socio-demographic characteristics of the respondents, including sex, highest educational attainment, current employment status, estimated monthly income, years of experience, and BPO service category.

The study comprises 105 respondents, including 61 females (58.10%) and 44 males (41.90%). The predominance of female respondents may influence communication styles, team dynamics, and participation rates in training or policy implementation. Consequently, for cybersecurity planning, it is advisable to design awareness campaigns and training that engage the majority group while

Table 1. Socio-demographic profile.

	Frequency	Percentage
Sex		
Male	44	41.90
Female	61	58.10
Total	**105**	**100.00**
Age		
<30 years old	56	53.33
30 - 39 years old	40	38.10
40 - 49 years old	8	7.62
>50 years old	1	0.95
Total	**105**	**100.00**
Highest Educational Attainment		
Elementary graduate	0	0.00
Highschool graduate	10	9.52
College graduate	75	71.43
Post graduate	13	12.38
Technical/Vocational	7	6.67
Total	**105**	**100.00**
Current employment status		
Regular/Permanent Employee	74	70.48
Probationary Employee	10	9.52
Contractual Employee	14	13.33
Project-based Employee	7	6.67
Total	**105**	**100.00**
Estimated monthly income		
less than ₱10,000	0	0.00
₱10,001 – ₱20,000	5	4.76
₱20,001 – ₱30,000	16	15.24
₱30,001 – ₱40,000	33	31.43
₱40,001 – ₱50,000	22	20.95
more than ₱50,000	29	27.62
Total	**105**	**100.00**
Years of experience		
less than 1 year	14	13.33
1 - 3 years	26	24.76

Continued

4 - 6 years	32	30.48
7 - 10 years	21	20.00
more than 10 years	12	11.43
Total	**105**	**100.00**
BPO service category		
Customer Service/Contact Center	19	18.10
Telemarketing/Sales	14	13.33
Technical Support	16	15.24
Back-Office Processing	15	14.29
Finance & Accounting Outsourcing	23	21.90
Human Resources Outsourcing	11	10.48
Knowledge Process Outsourcing (KPO)	6	5.71
Others	1	0.95
Total	**105**	**100.00**

ensuring inclusivity, thereby enhancing the resonance of messaging and maximizing adoption throughout the workforce.

This concentration under 40 indicates a workforce that is dominated by early- and mid-career employees who generally possess higher digital fluency but may also adopt informal device and network practices when working remotely, increasing the exposure to cybersecurity risks. Therefore, interventions should leverage their digital-native strengths while explicitly addressing risky habits such as use of personal devices and lax home-network security. Findings reveals that the majority of the respondents are under the age of 30, with 56 (53.33%) being under the age of 30 and 40 (38.10%) being between the ages of 30 and 39, 8 (7.62%) and 1 (0.95%) being 50 or older.

This table presents the highest educational attainment. Most respondents are 75 college graduates (71.43%), followed by 13 post graduates (12.38%), 10 high school graduates (9.52%), and 7 technical/vocational holders (6.67%); this high level of educational attainment suggests a workforce capable of understanding technical concepts and following formal policies an asset for implementing a complex security controls yet education alone does not guarantee or secure behavior, so training should be emphasize and role-specific guidance. In light of this, businesses are able to provide more advanced and technical training that places an emphasis on practical application and policy compliance.

The majority of the people who answered are 74 regular or permanent employees (70.48%), 14 (13.33%) contractual employees, 10 (9.52%) probationary employees, and 7 (6.67%) project-based employees. This means that permanent employees have more stable access privileges and longer-term exposure to the company's culture, while non-permanent employees may have different onboarding,

inconsistent access controls, and uneven training and accountability.

The findings indicate that BPO respondents generally fall within the mid to upper income ranges in terms of estimated monthly income: ₱30,001 - ₱40,000 (33% - 31.43%), ₱40,001 - ₱50,000 (22% - 20.95%), and >₱50,000 (29% - 27.62%). This means that many of the respondents can probably invest in more reliable home infrastructure, like having a personal internet connection and newer personal devices. However, a significant number of them are still in lower income bands and may rely on shared or older equipment, which could make it harder for them to use the recommended security tools, such as separate work devices or paid VPNs. This creates uneven risk exposure, so cybersecurity programmes should take this economic diversity into account by providing or subsidising secure equipment and internet.

In terms of number of years of work, respondents with 4 - 6 years (32; 30.48%), 1 - 3 years (26; 24.76%), 7 - 10 years (21; 20.00%), less than 1 year (14; 13.33%), and more than 10 years (12; 11.43%), the experience frequency shows mostly of the respondents has years of experience in BPO industries.

In terms of type of BPO Service category, respondents work in a variety of roles, including the Finance & Accounting Outsourcing (23; 21.90%), Customer Service/Contact Center (19; 18.10%), Technical Support (16; 15.24%), Knowledge Process Outsourcing (16; 15.24%), Telemarketing/Sales (14; 13.33%), Human Resources Outsourcing (11; 10.48%), Back-Office Processing (5; 4.76%), and Others (1; 0.95%). As a result, most of the respondents were from financial and client data these roles usually handle sensitive data (F&A and customer service), while technical and KPO roles may have privileged access or specialized tools. As a result, role-specific risk profiles are very different, which means that the breaches could have a bigger effect. To lower exposure in a remote work environment, companies should use a role-based security controls that will prioritize protections for high-risk functions, enforce least privilege access, and ensure that the training and monitoring are tailored to the specific data handling and access patterns of each service category.

3.2. Cybersecurity Risk Perception

Table 2 shows the types of cybersecurity risks that influence the occurrence of security incidents in the organization, including phishing, Malware and Unauthorized Access Risks.

The phishing cluster has high agreement all the way through, with item means running from 3.35 to 3.54 and an overall weighted mean (OWM) of 3.48. Standard deviations (0.52 - 0.69) show that responses were all the same. Because phishing is a very high cybersecurity risk (OWM = 3.48; highest = 3.54; lowest = 3.35), companies should put effort into just-in-time microlearning, scenario-based problem-solving, and simulated phishing campaigns that show real phishing incidents and ask students to find signs, report incidents, and practice containment steps.

The items about malware have strong agreement, with means ranging from

Table 2. Types of cybersecurity risks influence the occurrence of security incidents in the organization

	Mean	SD	Verbal Description
A. Phishing-related Risks			
1. Phishing emails or fake websites are frequently encountered by employees during remote work.	3.54	0.67	Strongly Agree
2. Phishing attacks often lead to disclosure of sensitive company information.	3.52	0.54	Strongly Agree
3. Employees sometimes fall victim to phishing scams due to realistic or convincing messages.	3.35	0.69	Strongly Agree
4. Phishing incidents increase the likelihood of security breaches in the organization.	3.46	0.54	Strongly Agree
5. Phishing significantly disrupts operations by compromising accounts or data access.	3.49	0.52	Strongly Agree
6. Phishing attempts often bypass basic security measures, exposing vulnerabilities in the system.	3.49	0.54	Strongly Agree
7. Lack of employee awareness and training increases susceptibility to phishing attacks.	3.50	0.52	Strongly Agree
8. Phishing scams contribute to financial losses and reputational damage for BPO enterprises.	3.51	0.50	Strongly Agree
Overall Weighted Mean	**3.48**	**0.43**	**Strongly Agree**
B. Malware-related Risks			
9. Malware infections (e.g., viruses, ransomware) are a recurring problem in remote-work systems.	3.49	0.59	Strongly Agree
10. Malware causes system slowdowns, data corruption, or loss of files.	3.50	0.54	Strongly Agree
11. Malware incidents often require technical intervention or downtime to resolve.	3.57	0.50	Strongly Agree
12. Malware increases the number of reported security incidents within the company.	3.52	0.59	Strongly Agree
13. Weak endpoint protection contributes to frequent malware infections in remote devices.	3.54	0.52	Strongly Agree
14. Malware spreads quickly through shared files and email attachments in remote work environments.	3.51	0.52	Strongly Agree
15. Inadequate software updates and patch management increase vulnerability to malware attacks.	3.52	0.52	Strongly Agree
16. Malware compromises sensitive client and company data, leading to potential financial and reputational damage.	3.55	0.50	Strongly Agree
Overall Weighted Mean	**3.53**	**0.46**	**Strongly Agree**
C. Unauthorized Access Risks			
17. Unauthorized access attempts (e.g., login from unknown devices) occur frequently.	3.53	0.57	Strongly Agree
18. Weak or reused passwords among employees lead to unauthorized access.	3.44	0.54	Strongly Agree
19. Unauthorized access incidents often result in data theft or account compromise.	3.45	0.55	Strongly Agree
20. Remote work setups increase vulnerability to unauthorized system access.	3.50	0.56	Strongly Agree
21. Lack of authentication controls (e.g., multi-factor login) allows unauthorized users to breach systems.	3.49	0.52	Strongly Agree
22. Shared accounts or credentials among employees increase the risk of unauthorized access.	3.54	0.52	Strongly Agree
23. Unauthorized access attempts often go undetected due to insufficient monitoring systems.	3.50	0.52	Strongly Agree
24. Insider threats, such as disgruntled employees, contribute to unauthorized access incidents.	3.50	0.54	Strongly Agree

Continued

Overall Weighted Mean	**3.49**	**0.42**	**Strongly Agree**

Legend:

3.25 - 4.00 Strongly Agree (Very High Cybersecurity Risk)

2.50 - 3.24 Agree (High Cybersecurity Risk)

1.75 - 2.49 Disagree (Low Cybersecurity Risk)

1.00 - 1.74 Strongly Disagree (No Cybersecurity Risk)

3.49 to 3.57 and an OWM of 3.53. The standard deviations (SDs) are between 0.5 and 0.59, which shows that people have similar ideas. For example, "Malware incidents often require technical intervention or downtime" (3.57) has the highest mean, while "Malware infections are a recurring problem in remote-work systems" (3.49), has the lowest. Respondents think that malware is common, spreads quickly, and interferes with operations by slowing things down, corrupting data, and increasing the number of incidents that need to be fixed.

When it comes to unauthorized access, the items' means are between 3.44 and 3.54, with an OWM of 3.49 and SDs close to 0.52 to 0.57. This shows that people are generally worried: "Shared accounts or credentials raise the risk" (3.54) has the highest mean, while "Weak or reused passwords allow unauthorized access" (3.44). The results show that people think that misuse of credentials, weak authentication (lack of MFA), poor tracking, working from home, and insider threats are some of the main reasons why breaches and data theft happen. Unauthorized access is a very high risk (OWM = 3.49; highest = 3.54; lowest = 3.44), so companies should use least-privilege and multi-factor authentication. They should also use problem-based learning methods like credential management workshops, team simulations of unauthorized logins, and detection challenge exercises to teach their staff how to properly manage credentials, spot suspicious access, and practice escalation and containment procedures. Since unauthorized access is a very high cybersecurity risk (OWM = 3.49; highest = 3.54; lowest = 3.44), companies should use least-privilege access policies and multi-factor authentication. They should also use problem-based learning methods like credential-management workshops, team simulations of unauthorized logins, and detection-challenge exercises to teach their employees how to properly manage credentials and respond to suspicious access.

3.3. Technical Preparedness Strategies

Table 3 shows the effect of technical preparedness strategies on risk mitigation, including Multi-Factor Authentication (MFA), Firewalls and Intrusion Detection Systems (IDS) and Virtual Private Networks (VPN).

Items about MFA get scores between 3.42 and 3.57, with an average of 3.51 and standard deviations of 0.54 - 0.54. This shows that most people believe that MFA is widely used and works (3.57 for "company requires MFA for all remote logins"

Table 3. Effect of technical preparedness strategies on risk mitigation.

	Mean	SD	Verbal Description
A. Multi-Factor Authentication (MFA)			
1. Our company requires multi-factor authentication for all remote logins.	3.57	0.52	Strongly Agree
2. MFA reduces the chances of unauthorized access to company systems.	3.48	0.54	Strongly Agree
3. Employees find MFA easy and convenient to use during remote work.	3.42	0.53	Strongly Agree
4. MFA has improved overall account security in our organization.	3.52	0.50	Strongly Agree
5. Incidents of compromised passwords have decreased after implementing MFA.	3.50	0.50	Strongly Agree
6. MFA enhances employee confidence in the security of remote work systems.	3.52	0.52	Strongly Agree
7. The implementation of MFA has reduced the number of unauthorized login attempts.	3.52	0.50	Strongly Agree
8. MFA adoption demonstrates the company's commitment to strengthening cybersecurity measures.	3.52	0.50	Strongly Agree
Overall Weighted Mean	**3.51**	**0.42**	**Strongly Agree**
B. Firewalls and Intrusion Detection Systems (IDS)			
9. Our company maintains active firewalls to protect remote connections.	3.45	0.54	Strongly Agree
10. Intrusion detection systems help identify and block suspicious activities.	3.48	0.50	Strongly Agree
11. Firewall protection minimizes external cyberattacks on company networks.	3.49	0.50	Strongly Agree
12. IDS alerts are promptly addressed by the IT/security team.	3.46	0.50	Strongly Agree
13. Firewalls and IDS significantly contribute to reducing security incidents.	3.50	0.50	Strongly Agree
14. Firewalls are regularly updated to address emerging cybersecurity threats.	3.47	0.50	Strongly Agree
15. IDS provides detailed reports that help improve future security strategies.	3.50	0.50	Strongly Agree
16. Combined use of firewalls and IDS strengthens overall network resilience during remote work.	3.50	0.50	Strongly Agree
Overall Weighted Mean	**3.48**	**0.44**	**Strongly Agree**
C. Virtual Private Networks (VPNs)			
17. Employees are required to use company-approved VPNs for remote access.	3.47	0.57	Strongly Agree
18. VPNs provide secure communication between remote employees and company servers.	3.37	0.56	Strongly Agree
19. VPN usage reduces the likelihood of data interception or leaks.	3.45	0.57	Strongly Agree
20. Employees are trained on proper VPN usage and data protection.	3.33	0.61	Strongly Agree
21. VPNs enhance the overall cybersecurity posture of the company.	3.47	0.54	Strongly Agree
22. VPN connections are automatically enforced for all remote sessions.	3.46	0.57	Strongly Agree
23. Split tunneling is disabled to prevent bypassing corporate security controls.	3.49	0.52	Strongly Agree
24. VPN logs are regularly monitored and audited for suspicious activity.	3.50	0.54	Strongly Agree
Overall Weighted Mean	**3.44**	**0.46**	**Strongly Agree**
Legend:			
3.25 - 4.00 Strongly Agree (Very prepared)			
2.50 - 3.24 Agree (Moderately prepared)			
1.75 - 2.49 Disagree (Slightly prepared)			
1.00 - 1.74 Strongly Disagree (Not prepared at all)			

and 3.42 for "employees find MFA easy/convenient"). Respondents think that MFA lowers the risk of unauthorized access, lowers the number of times passwords are stolen, and raises trust. However, they think it is slightly less easy to use than they think it is effective. The idea is that multifactor authentication (MFA) is a high-value security measure that should be kept and paired with usability improvements and user support, like making the enrollment process clearer, having backup plans, and giving users short, hands-on instructions, to keep adoption high and stop people from finding ways to get around security measures that do not work.

Items about Firewalls and Intrusion Detection Systems (IDS). Most respondents view firewalls and intrusion detection systems (IDS) as effective: item scores range from 3.45 to 3.50 (mean 3.48, SD 0.50 - 0.54). Respondents credit IDS alerts, prompt IT support, and regular updates with improving network reliability. However, slightly lower scores on the basic firewall question indicate some gaps in confidence and communication.

The VPN items have means between 3.33 and 3.50, an average score of 3.44, and standard deviations between 0.52 and 0.61. The table shows that most people agree that VPNs are necessary and helpful, but some have less positive views about training and safe usage (highest score: automatic enforcement of VPN and regular log monitoring, 3.50; lowest score: employees are trained on proper VPN usage, 3.33). This means that VPNs are seen as an important technology control, but that users need to be better trained and that VPNs need to be set up correctly (for example, by turning off split tunneling). So, companies should use company-approved VPNs, automated policies, targeted user training, clear usage instructions, and regular log audits to make sure VPNs lower the risk of interception without leaving holes in usability that allow hackers to find unsafe ways to get around them.

3.4. Cybersecurity Incidents Frequency

The evaluation of the results revealed moderate to strong correlations, with Spearman's rho values ranging from .503 to .692, between exposure to cybersecurity risks and the adoption of preparedness strategies. These values indicate consistent and meaningful relationships across the variables studied. Furthermore, all preparedness correlations were found to be highly significant at $p = 0.000$, reinforcing the reliability and validity of the findings. The strength and significance of these correlations confirm that the observed relationships are not due to chance, but rather reflect genuine patterns in the data.

The consistency of results across different types of risks namely phishing, malware, and unauthorized access and preparedness strategies such as multifactor authentication, firewall implementation, and virtualization demonstrates stability in the overall pattern of outcomes. The application of non-parametric tests further strengthens the credibility of these ratings, as such methods are robust even when data distributions deviate from normality. Collectively, the findings confirm that

the relationships observed are both statistically sound and stable, providing a strong foundation for drawing meaningful conclusions and formulating practical recommendations.

Table 4. The significant relationship between the socio-demographic profile of the respondents and their description of cybersecurity risks.

		CR Phishing	CR Malware	CR Unauthorized Access
Sex	Spearman's rho	0.02	−0.018	0.037
	Sig. (2-tailed)	0.84	0.853	0.71
	N	105	105	105
Age	Spearman's rho	−0.148	−0.007	−0.058
	Sig. (2-tailed)	0.133	0.943	0.555
	N	105	105	105
Highest Educational Attainment	Spearman's rho	0.006	0.004	0.125
	Sig. (2-tailed)	0.949	0.967	0.204
	N	105	105	105
Employment Status	Spearman's rho	−0.17	−.259**	−.247*
	Sig. (2-tailed)	0.082	0.008	0.011
	N	105	105	105
Monthly Income	Spearman's rho	−0.059	−0.114	−0.093
	Sig. (2-tailed)	0.551	0.247	0.343
	N	105	105	105
Years of experience	Spearman's rho	0.087	−0.007	0.011
	Sig. (2-tailed)	0.377	0.944	0.912
	N	105	105	105
BPO Service Category	Spearman's rho	0.078	0.026	0.034
	Sig. (2-tailed)	0.429	0.794	0.731
	N	105	105	105

*Correlation is significant at the 0.05 level (2-tailed); **Correlation is significant at the 0.01 level (2-tailed).

Table 4 shows the Spearman's rho correlations between the socio-demographic factors of the respondents and three exposure measures: CR Phishing, CR Malware, and CR Unauthorized Access. Employment Status is the only relationship that is statistically significant. There is a link between employment position and CR Unauthorized Access ($\rho = -0.247$, $p = 0.011$; all tests use N = 105) and CR Malware ($\rho = -0.259$, $p = 0.008$; two-tailed). The levels of significance show that the null hypothesis that there is no connection between these two outcomes is not true.

Table 5. The significant relationship between the socio-demographic profile of the respondents and how they describe technical preparedness strategies.

		TP Multi-Factor Authentication	TP Firewalls and Intrusion Detection Systems	TP Virtual Private Networks
Sex	Spearman's rho	0.155	0.201*	0.054
	Sig. (2-tailed)	0.115	0.04	0.587
	N	105	105	105
Age	Spearman's rho	−0.005	0.004	0.009
	Sig. (2-tailed)	0.963	0.969	0.928
	N	105	105	105
Highest Educational Attainment	Spearman's rho	−0.013	0.1	−0.046
	Sig. (2-tailed)	0.898	0.312	0.643
	N	105	105	105
Employment Status	Spearman's rho	−0.184	−0.04	−0.127
	Sig. (2-tailed)	0.061	0.685	0.197
	N	105	105	105
Monthly Income	Spearman's rho	−0.031	−0.014	−0.032
	Sig. (2-tailed)	0.757	0.885	0.743
	N	105	105	105
Years of experience	Spearman's rho	−0.028	−0.064	−0.018
	Sig. (2-tailed)	0.778	0.519	0.852
	N	105	105	105
BPO Service Category	Spearman's rho	0.144	0.11	0.105
	Sig. (2-tailed)	0.144	0.262	0.289
	N	105	105	105

*Correlation is significant at the 0.05 level (2-tailed); **Correlation is significant at the 0.01 level (2-tailed).

There are Spearman's rho connections between three technical preparedness methods (TP Multi-Factor Authentication, TP Firewall and Intrusion Detection Systems, and TP Virtual Private Networks) and three socio-demographic variables shown in Table 5. The only significant link is between gender and TP Firewall and Intrusion Detection Systems ($\rho = 0.201$, $p = 0.040$, $N = 105$), which means that the null hypothesis that gender and firewall preparedness are not related is not true. The positive coefficient shows that female respondents tend to report higher adoption or perceived effectiveness of firewall/IDS controls.

The link is weak but statistically significant, showing that gender only explains

a small part of the variation in how ready people are for firewalls. Most of the variation is still due to other factors. Because Spearman's rho measures rank association, the finding shows that, on average, women rate themselves higher on how ready they are for a firewall than men do. For program designers, this means two things: first, find out if role assignment, training access, or communication channels consistently favor one gender and fix any gaps so all staff have the same level of technical knowledge; second, use the strength that has been found by making female staff peer champions or trainers for firewall/IDS best practices to get everyone on the team to behave in a good way.

Table 6. Correlation between level of exposure to cybersecurity risks and technical preparedness strategies on the reduction of cybersecurity incidents.

		TP Multi-Factor Authentication	TP Firewalls and Intrusion Detection Systems	TP Virtual Private Networks
CR Phishing	Spearman's rho	0.617**	0.503**	0.555**
	Sig. (2-tailed)	0.000	0.000	0.000
	N	105	105	105
CR Malware	Spearman's rho	0.692**	0.520**	0.552**
	Sig. (2-tailed)	0.000	0.000	0.000
	N	105	105	105
CR Unauthorized Access	Spearman's rho	0.642**	0.650**	0.671**
	Sig. (2-tailed)	0.000	0.000	0.000
	N	105	105	105

*Correlation is significant at the 0.05 level (2-tailed); **Correlation is significant at the 0.01 level (2-tailed).

In Table 6, there are strong, positive, and statistically significant links between the level of exposure to cybersecurity risks and technical preparedness strategies for all pairs (N = 105). These include CR Phishing with TP MFA (0.617), TP Firewall/IDS (0.503), and TP VPN (0.555); CR Malware with TP MFA (0.692), TP Firewall/IDS (0.520), and TP VPN (0.552); and CR Unauthorized Access with TP MFA (0.642), TP Firewall/IDS (0.650), and TP VPN (0.671) (all $p = 0.000$, two-tailed). This means that the null hypothesis that there is no relationship is not true. These factors show that people who say they have been more likely to experience phishing, malware, or unauthorized access also say they use or think that MFA, firewall/IDS, and VPN controls more effectively. Basically, having more risk experience means you are better prepared technically. This pattern could mean that organizations or individuals are reactive and only invest in technical controls after incidents happen, that exposed staff are more aware of the risks, which leads to adoption and compliance, or that organizations give more resources to teams that have had incidents.

4. Conclusion and Recommendation

Respondents most frequently reported phishing, malware, and unauthorized access as threats, often linked with credential misuse and account sharing. Multi-factor authentication (MFA), firewalls/IDS, and VPNs were widely noted as organizational controls, though employees often perceived these measures as reactive rather than preventive. Regular employees indicated higher exposure levels, and gender differences emerged in preparedness, with female respondents reporting slightly greater readiness in certain control practices. These findings highlight the importance of understanding how demographic and role-based factors shape perceptions of cybersecurity resilience.

The results underscore associations between employee profiles, organizational practices, and perceived risk management strategies. While causality cannot be inferred, the patterns observed suggest that inclusive, proactive frameworks may strengthen resilience in remote BPO contexts. Recommended organizational actions include enforcing individual account ownership with MFA and VPNs, issuing pre-secured devices, embedding cybersecurity training into onboarding and mentoring, and conducting practice simulations to sustain vigilance. Continuous monitoring, incident tracking, and real-time analytics are also essential components of a comprehensive approach. By aligning technical safeguards with structured organizational practices, remote BPOs can foster a preventive, inclusive, and resilient cybersecurity posture. However, since the sample was drawn in Nueva Ecija, it may not represent BPO workforces in other provinces, regions, or countries. It is recommended that further research involving more respondents should be conducted to validate the findings.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Department of Information and Communications Technology (2022). *National Cybersecurity Plan 2022*. https://dict.gov.ph

The Asia Foundation (2022). *Cybersecurity in the Philippines: Global Context and Local Challenges*. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

Trefis Team (2015). *Getting a Piece of Business Process Outsourcing*. Forbes. https://www.forbes.com/sites/greatspeculations/2015/06/22/getting-a-piece-of-business-process-outsourcing