PEOPLE: International Journal of Social Sciences
ISSN 2454-5899

Puay Fong Oh, 2026

Volume 12 Issue 2, pp. 66-77

Received: 27th June 2026

Revised: 30th April 2026, 16th July 2026

Accepted: 23rd July 2026

Date of Publication: 31st July 2026

DOI- https://doi.org/10.20319/pijss.2026.122.6677

This paper can be cited as: Oh, P.F. (2026). Results of Pilot Survey to Examine Sunzi's Art of War's Applicability to Cyber Risk Management. PEOPLE: International Journal of Social Sciences, 12(2), 66-77

RESULTS OF PILOT SURVEY TO EXAMINE SUNZI'S ART OF WAR'S APPLICABILITY TO CYBER RISK MANAGEMENT

Puay Fong Oh
Strategic Technology Management Track, Franklin Hudson–The International School of Management, Paris, France
ohpuayfong@gmail.com

Abstract

The Chinese classic on strategy, Sunzi's The Art of War (hereafter SAW), is often quoted in the cybersecurity literature without further explanation or justification why or how it is applicable to cyber risk management (CyRM). This paper presents the results of a pilot survey that was part of a larger study using a mixed-methods approach to rigorously and systematically examine this issue. The results based on a sample size of 50 respondents reinforced the same observation that prompted the study, namely, while there was agreement on SAW's applicability to CyRM, there was less understanding on how it could be operationalized in practice. Following data collection, the Chi-square independence tests revealed statistically significant differences between observed and expected frequencies for age; gender; education level; employment status; geographical location; possession or lack of cybersecurity qualification(s); employment in a small or medium enterprise (SME); and familiarity with SAW. The Cronbach alpha calculated for the theoretical categories that emerged from the earlier qualitative phases of the study fell within acceptable

range. Notably, removing data outliers did not change the results, suggesting that data saturation was achieved. Nonetheless, further research, such as follow-up interviews with selected participants or focus groups, and a full survey with more participants, including more CyRM professionals, are recommended.

Keywords:
Cyber Risk Management, Cybersecurity, Sunzi, Sun Zi, Sun Tzu, (The) Art of War

1. Introduction

The Chinese classic on strategy, *Sunzi's The Art of War* (hereafter SAW), is often quoted in the cybersecurity literature without further explanation or justification why or how it is applicable to cyber risk management (CyRM) practitioners (e.g., Carlsson & Gustavsson, 2017; Ching, 2022; Gros, 2021; Kim & Lowry, 2020; Madsen, 2019; M.K. Miller, 2001; Sayegh, 2023; Wang & D'Cruze, 2020; Yehezkel, 2022). This paper presents the results of a pilot survey that was part of a larger study using a mixed-methods approach to rigorously and systematically examine this issue.

From the initial two qualitative phases, six theoretical categories emerged from the data that were conceptually and operationally defined, which were: *Intelligence* to *Insight, Invisibility*, (Cyber) *Immunity*, *Fluidity*, and *Resources*. A 70-item survey instrument using a 7-point Likert scale with the options of *Don't Know* and *Don't Understand* comprising 60 questions, 9 questions related to the participant's profiles, and a freeform textbox was then developed; assessed by an expert panel of three to obtain its content validity scores confirming the survey items were relevant and clear before the pilot survey was launched online. Following the data collection and analysis, a new theoretical category named *Inclusivity* was teased out, giving a total of seven theoretical categories.

The following sections present the profile of the participants.

2. Profile of Participants

A total of 50 complete responses were collected, exceeding the minimum of 30 required for a pilot study (Memon et al., 2020). All participants answered the 60 questions pertinent to this

study but a few skipped questions related to their personal information such as their education level, industry, or country of residence.

2.1 Profile of Participants

52% of respondents identified as male, 44% as female, while 2% each chose other options. The modal age group of 25-34 years constituted 46% of all respondents. 78% reported having at least a bachelor's degree (39%), or a graduate or professional degree (39%). Finance (12%) was the most represented industry, followed by Construction (10%), Media and Entertainment (10%), and a catch-all Others category (14%). 60% were employed, either part-time (22%) or full-time (38%). 63% reported that their organization was not a small or medium enterprise (SME, defined as having less than 100 employees or less than US$5 million in annual revenue). 31% said they had not heard of SAW, 35% said they had heard of it, 27% said they had read it while 8% reported being able to quote from it. 35% were from Cambodia and Singapore although a total of 17 geographical locations were represented. Only 10% reported they held cybersecurity qualifications.

2.2 Respondents' Demographics and Response Patterns

Given that respondents' demographics are categorical variables, the non-parametric Chi-square tests of independence were used to determine if there was any association between the respondents' demographic variables and their responses on the survey. The results revealed p-values less than the critical p-value of 0.05, thus resulting in the rejection of the null hypotheses. Hence, statistically significant differences were found between age; gender; education level; employment status; location; working in a SME or not; possession or lack of cybersecurity qualification(s); familiarity with SAW, and their responses on the survey. For example, women responded with *Don't Know* or *Don't Understand* on the survey more frequently than expected, whereas men responded with *Strongly Disagree*, *Neither Disagree nor Agree*, and *Agree* more frequently than expected. However, without follow-up interviews with selected participants or further research such as focus groups, it would be speculative to offer reasons for the observed differences. Nonetheless, they represent opportunities for further research.

The key findings were presented in the following sections.

3. Key Findings

After data collection, the Cronbach alpha was calculated to ensure internal consistency for each theoretical category and found to be within acceptable range of from >0.70 to <0.95 (Taber, 2018). Notably, values above 0.95 are undesirable as they reveal that there is not enough discriminant validity among the items (Taber, 2018). Furthermore, removing data outliers did not change the results, suggesting that data saturation was achieved.

The following tables summarized the key findings.

3.1 Agreement to SAW's Applicability to Cybersecurity

Table 1 summarized the percentage of respondents who agreed or strongly agreed to the SAW quotes representing the theoretical categories.

Table 1: *Percentage of Agreement to SAW's Applicability to Cybersecurity*

Q#	Survey Item (Translation by Giles, 1910)	% who *Agree* or *Strongly Agree*
Q1	Sunzi said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." This quote is applicable to cybersecurity	70%
Q2	Sunzi said, "By discovering the enemy's disposition, we can keep our forces concentrated, while the enemy's must be divided." This quote is applicable to cybersecurity.	60%
Q19	Sunzi said, "By remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided." This quote is applicable to cybersecurity.	52%
Q28	Sunzi said, "The good fighters of old first put themselves beyond the possibility of defeat, and then waited for an opportunity of defeating the enemy." This quote is applicable to cybersecurity.	54%
Q37	Sunzi said, "He who can modify his tactics in relation to his opponent and thereby succeed in winning, may	62%

	be called a gifted leader." This quote is applicable to cybersecurity.	
Q46	Sunzi said, "What we can do is simply to concentrate all our available strength, keep a close watch on the enemy, and obtain reinforcements." This quote is applicable to cybersecurity.	60%

Unsurprisingly, support for the theoretical categories of Invisibility (8% responded *Don't Know*) and Immunity (16% responded *Don't Know* or *Don't Understand*) was borderline as these two theoretical categories were not easy to understand or operationalize.

3.2 Items with Highest and Lowest Agreement

Excluding organization-specific items, the item(s) with the highest and lowest agreement respectively were presented in Table 2.

Table 2: *Survey Item(s) with Highest and Lowest Agreement*

Q#	Survey Item	% who *Agree* or *Strongly Agree*
Highest Agreement		
Q38	One way to respond quickly to changing circumstances in cybersecurity is to establish clear policies, including when frontline staff may activate a kill switch to halt the advances of a potential threat.	80%
Lowest Agreement (Tied)		
Q3	It is possible to know in advance who one's enemy is in cybersecurity.	38%
Q29	It is possible to put oneself "beyond the possibility of defeat" in cybersecurity.	38%

3.3 Items that Participants did not Understand

Table 3 listed the eight survey items with five or more *Don't Understand* responses, likely due to the italicized concepts (my emphasis).

Table 3: *Items with Five or More "Don't Understand" Responses*

Q#	Survey Item	Frequency
Q29	It is possible to put oneself "*beyond the possibility of defeat*" in cybersecurity.	7
Q36	It is helpful to think in terms of *cyber immunity*, defined as adapting cybersecurity measures to meet ever-evolving threats.	6
Q12	One way to know one's cyber risks is through a *gap analysis*.	5
Q16	Cyber risks may come from *hostile state actors*.	5
Q48	*Holistic stakeholder management* is necessary to ensure an organization's cybersecurity.	5
Q57	My organization is likely to survive a *DDoS (distributed denial-of-service) attack*.	5
Q59	My organization has *clear roles and responsibilities* for managing cybersecurity.	5

3.4 Organization-Specific Survey Items

Table 4 revealed the percentages and irregular patterns for the organization-specific items. Notably, the total percentages of *Don't Know* and *Don't Understand* responses ranged from 30% to 42%.

Table 4: *Percentages of* Don't Know *and* Don't Understand *Responses to Organization-Specific Items*

Item #	**Survey Item**	**Percentage of *Don't Know* or *Don't Understand***
Q54	My organization is likely to survive a ransomware attack like the WannaCry attack in 2017.	42%
Q55	My organization is likely to survive a Zero Day attack like the log4j vulnerability in 2021.	42%
Q56	My organization is likely to survive a data breach.	34%
Q57	My organization is likely to survive a DDoS (distributed denial-of-service) attack.	38%

Q58	My organization has clear policies and procedures on what to do in case of a cyber incident.	30%
Q59	My organization has clear roles and responsibilities for managing cybersecurity.	32%
Q60	My organization's leaders, including the board directors and C-suite, are proactive in ensuring cybersecurity.	32%

Out of these seven items, only the distribution for Q60 approximated to a negatively-skewed normal distribution, whereas the other distributions showed great variability (Balnaves & Caputi, 2001).

4. Discussion

The following sections discussed the findings by the theoretical categories.

4.1 Theoretical Categories of Intelligence to Insight

Although 70% agreed or strongly agreed that Sunzi's most-famous quote on knowing oneself and one's enemy was applicable to cybersecurity; and 60% agreed or strongly agreed that "By discovering the enemy's dispositions, we can keep our forces concentrated, while the enemy's must be divided" was applicable to cybersecurity, only 38% affirmed that it was possible to know in advance one's enemy in cybersecurity, one of the items with the lowest agreement.

In order of descending support, participants' agreement to the various measures to operationalize the theoretical categories of Intelligence and Insight were: information sharing (64%); threat hunting (62%); reading latest cybersecurity trend or threat reports (60%); and reading what hackers such as Edward Snowden or Kevin Mitnick wrote (56%). 58% acknowledged that insiders posed possible threats, which might be mitigated by: proper grievance handling policies and procedures (58%); automated user behavioral analytics (56%); or whistleblowing (48%).

Although 56% agreed or strongly agreed that a gap analysis was a way to assess one's cyber risks, this item appeared problematic with 16% indicating *Don't Know* or *Don't Understand*, presumably to what a gap analysis was.

While 74% agreed or strongly agreed that it was important to identify, quantify, and plan how to mitigate one's cyber risks beforehand, only 64% thought it was possible.

The majority (72%) accepted that cyber risk management was necessary because the cyber landscape was inherently insecure; 66% thought cyber risks could come from dubious practices in the cybersecurity industry, for example, vendors claiming but failing to implement essential controls; and 60% believed cyber risks could originate from hostile state actors. Only 42% agreed or strongly agreed that technical solutions were sufficient, while 46% strongly disagreed, disagreed or neither disagreed nor agreed.

4.2 Theoretical Category of Invisibility

52% agreed or strongly agreed to the SAW quote on remaining invisible but only 40% thought it was possible to hide one's presence in cybersecurity. In order of decreasing support, participants' responses to the various measures to operationalize the theoretical category of Invisibility were: encrypt sensitive data (70%); use deception technologies, for examples, virtual private networks (VPNs), decoys, honeypots (66%); segregate networks, including air-gapping or taking some activities offline (64%); or use ad blockers (48%). 42% thought technical solutions like firewalls or IAM (Identity, Access and Privilege) management were sufficient against unauthorized access. There was broad support on the necessity to safeguard user privacy (76%); and data confidentiality, integrity, and availability (74%).

4.3 Theoretical Category of (Cyber) Immunity

54% agreed or strongly agreed that the SAW quote on positioning oneself "beyond the possibility of defeat" was applicable to cybersecurity, yet only 38% thought it was possible with 26% expressing *Don't Know* or *Don't Understand*. 68% each supported multi-layered measures or defense-in-depth; and the Zero Trust approach as ways to put oneself beyond the possibility of defeat, while 48% agreed or strongly agreed that limiting online transactions was one way. 66% supported the Not-If-But-When (NIBW) narrative; 74% thought cyber hygiene, defined as performing basic best practices, was helpful; 70% thought cyber resilience, defined as acquiring the ability to prevent, withstand, and recover from cyber incidents was helpful; and 66% thought cyber immunity, defined as adapting cybersecurity measures to meet ever-evolving threats, was helpful.

4.4 Theoretical Category of Fluidity

62% agreed or strongly agreed to the SAW quote that modifying one's tactics to overcome one's opponent was applicable to cybersecurity but only 50% thought it was possible to respond quickly to changing circumstance in cybersecurity. In order of decreasing support, participants' responses to the various measures to operationalize the theoretical category of

Fluidity were: establishing clear policies, including when frontline staff may activate a kill switch to halt the advances of a potential threat (80%); holding timely staff briefings or training whenever new threats emerged (76%); ensuring timely patching and updating of software (72%); holding unannounced cyber exercises (64%); performing frequent horizon scanning and repositioning to meet emerging threats (60%); engaging in information sharing (56%); and using cybersecurity systems powered by artificial intelligence, for example, to provide real-time intrusion alerts (54%).

4.5 Theoretical Category of Resources

60% agreed or strongly agreed to the SAW quote that "what we can do is simply to concentrate all our available strength, keep a close watch on the enemy, and obtain reinforcements". 64% agreed or strongly agreed that cyber insurance was a form of reinforcement. Although 70% agreed or strongly agreed that proper vendor management, including of suppliers, contractors, interns or temporary staff was necessary; and 76% believed trained human resources were necessary, only 56% affirmed holistic stakeholder management, with 26% expressing *Don't Know* or *Don't Understand*. In order of decreasing support, money for cybersecurity investments (76%); time (68%); and government support (68%) were deemed necessary resources to ensure an organization's cybersecurity.

4.7 Theoretical Category of Inclusivity

A new term called Inclusivity was proposed to replace holistic stakeholder management after analysis of the results revealed that one expert and 26% of survey respondents had difficulty understanding what it meant. Since the need to account as extensively as possible all the stakeholders in one's CyRM was deemed important, this construct was teased out as an additional theoretical category as it warranted separate attention.

The three questions (Q48-50) directly relevant to this category were included under the Resources theoretical category. As reported, with respect to ensuring an organization's cybersecurity, while 76% agreed or strongly agreed that trained human resources – whether they work directly in cybersecurity or not – were necessary; and 70% agreed or strongly agreed that proper management of vendors, including suppliers, contractors, interns or temporary staff, was necessary, only 56% agreed or strongly agreed that holistic stakeholder management was necessary, with 26% expressing *Don't Know* or *Don't Understand* to the last question.

Overall, the findings suggested there was consensus from the survey participants for SAW's applicability to CyRM but also uncertainty over how these theoretical categories could be applied in real life, reinforcing the same observations that prompted this study.

5. Opportunities for Future Research

Given the small scale of the pilot survey in this study, future research could involve conducting a full survey with a minimum sample size of 385 (Memon et al., 2020), targeting senior managers and cyber professionals to ascertain if both groups agree on the applicability of SAW to CyRM. It would also be insightful to test if significant differences exist among respondents from different ethnicities or cultural backgrounds (Buckley & Delicath, 2013). Such a quantitative approach could be augmented with qualitative methods such as interviews with selected participants or focus groups to yield more in-depth insights, including to uncover the reasons for the observed differences from expected frequencies between respondents' demographic variables and their responses in this study.

More work needs to be done in terms of establishing broadly, if not universally, acceptable definitions for terms such as gap analysis, hostile state actors, "beyond the possibility of defeat" (Giles, 1910), cyber immunity, holistic stakeholder management, DDoS, clear roles and responsibilities for managing cybersecurity. This may first be examined using a full-scale survey with a sufficiently large sample size including cybersecurity professionals and business leaders to establish whether the confusing terminology found in the pilot survey was specific to this particular sample population, or broadly generalizable.

6. Conclusion

Overall, the results revealed general support for SAW's applicability to CyRM but less understanding on how this could be operationalized in practice, reinforcing the same observations that prompted the study that included this pilot survey. Additionally, respondents expressed difficulty understanding common terms that were taken for granted in the literature. Nonetheless, these gaps represented opportunities for future research.

* END *

References

Balnaves, M., & Caputi. P. (2001). *Introduction to Quantitative Research Methods: An Investigative Approach*. Sage Publications.

Buckley, R., & Delicath, T. (2013). *Dissertation and research success: Hands-on coaching for doctoral success before, during, and after your dissertation*. [E-book]. Xlibris Corporation.

Carlsson, A., & Gustavsson, R. (2017, October 10-13). The art of war in the cyber world. [Conference paper]. *The 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology*. https://doi.org/10.1109/INFOCOMMST.2017.8246345

Ching, A. (2022). The art of cyber resilience: Into the mind of cyber criminals. AgilenLite.

Gros, S. (2021, June 10). Myths and misconceptions about attackers and attacks. [Preprint]. *University of Zagreb*. https://arxiv.org/pdf/2106.05702.pdf

Kim, B., & Lowry, P.B. (2020, May). A review and theoretical explanation of the 'cyberthreat-intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security, 92*. https://www.researchgate.net/publication/339299392_A_Review_and_Theoretical

Madsen, T. (2019). *The art of war for computer security*. [eBook]. https://doi.org/10.1007/978-3-030-28569-2

Memon, M.A., Ting, H., Cheah, J.H., Thurasamy, R., Chuah, F., & Cham, T.H. (2020, June). Sample size for survey research: Review and recommendations. *Journal of Applied Structural Equation Modeling, 4*(2), i-xx. https://jasemjournal.com/wp- content/uploads/2020/08/Memon-et-al_JASEM_-Editorial_V4_Iss2_June2020.pdf

Miller, M.K. (2001, April 2). Sun Tzu and the art of (cyber) war: Ancient advice for developing an information security program (Version 1.2b). *SANS Institute*. https://www.giac.org/paper/gsec/601/sun-tzu-art-cyber-war-ancient-advice-developing-information-security-program/101438

Sayegh. E. (2023, February 14). The art of cyberwar: Understanding your enemy. *Forbes*. https://www.forbes.com/sites/emilsayegh/2023/02/14/the-art-of-cyberwar-understanding-your-enemy/?sh=4bb553f6591b

Sun, T. (1910). *The art of war*. (L. Giles, Trans.). B. Jain Publishers.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*, 1273-1296. https://link.springer.com/article/10.1007/S11165-016-9602-2

Wang, P., & D'Cruze, H. (2020). Lessons on the power of knowledge for cyber defense from Sun Tzu's The Art of War. *Issues in Information Systems, 21*(3), 105-116. https://doi.org/10.48009/3_iis_2020_105-116

Yehezkel, S. (2022, June 30). "Know your enemy," and other cybersecurity lessons from Sun Tzu's Art of War. *Cyber Defense Magazine*. https://www.cyberdefensemagazine.com/know-your-enemy/