

הפרת בטחון מידע בקבוצות ווטסאפ ארגוניות

נעמה איזנרייך, אבי ברששת | הפקולטה לטכנולוגיות למידה



רקע למחקר

מידע ברשת חשוף לכל ולפעמים חושפי המידע הם גורמים מתוך המערכת המהווים סיכון לא פחות מהותי מאשר גורמים חיצוניים (Chen & Li, 2014)

אויבי הסייבר מתמקדים באיסוף מידע ובגניבת מידע מארגונים דרך עובדיהם איום שגדל לצד התפשטות הרשתות החברתיות (Abdul Molok, Chang & Ahmad, 2010)

מתחדד הצורך ביצירת תרבות ארגונית של שמירה על בטחון המידע 75% מהעובדים בישראל שולחים בווטסאפ (קאהאן, 2015) הדועות הקשורות לעבודה (קאהאן, 2015)

מטרות המחקר

לברר אילו גורמים קשורים להפצת מידע מסווג על ידי עובדי ארגונים ביטחוניים בשיחות ווטסאפ עם עובדים נוספים מהארגון

להבין את דפוסי הפעילות וההפרה של העובדים ואת תרבות בטחון המידע הארגונית

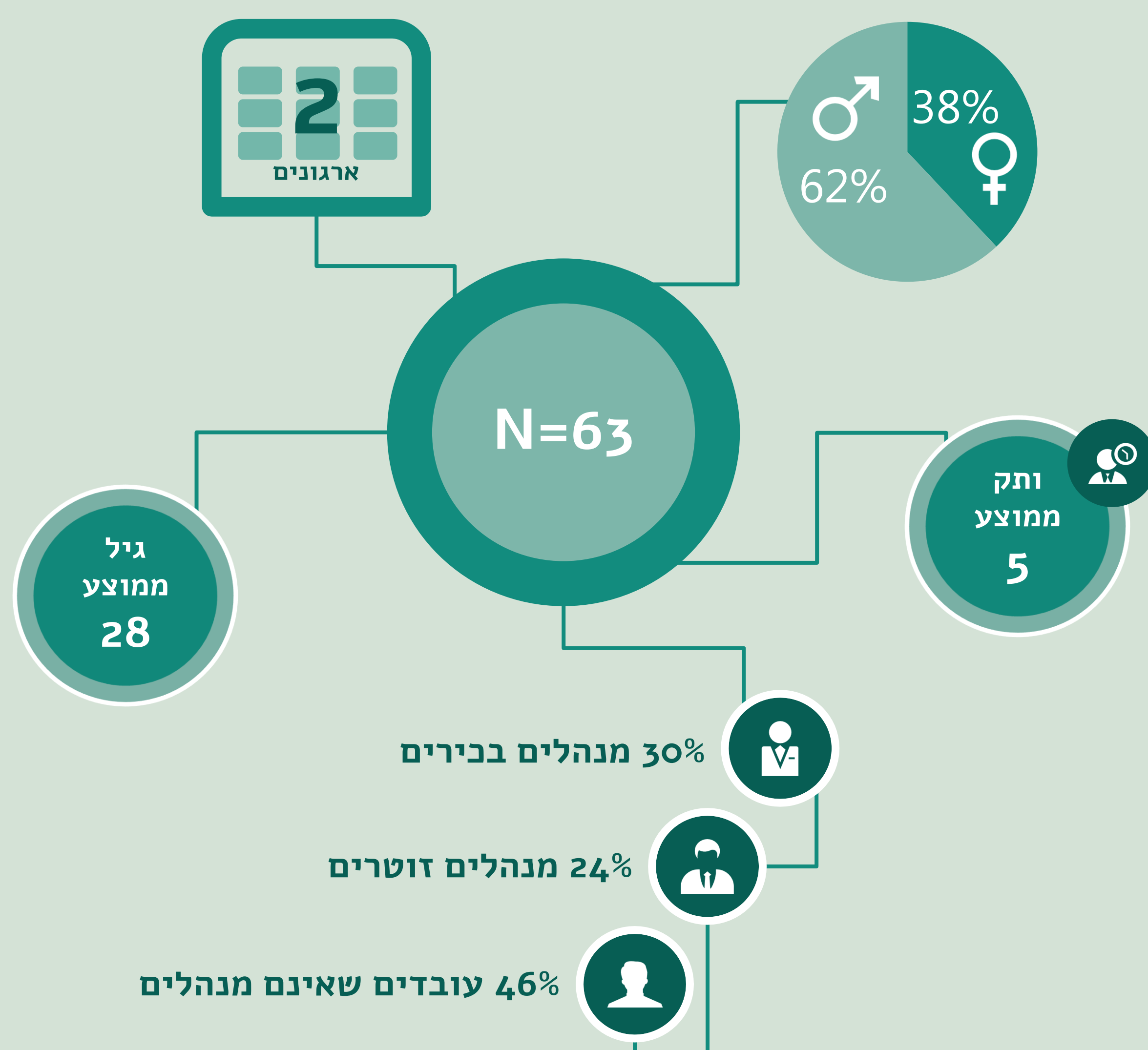
להניח יסוד אמפירי לגיבוש תכנית פעולה ליצירת שינוי ארגוני בתחום השמירה על בטחון המידע

שיטת איסוף הנתונים

הנתונים נאספו בעזרת שאלון GOOGLE ANONIMI מקוון.

בשאלון הוצגו היגדים בעלי סולמות מענה של 5-1 (סולם ליקרט), המייצגים את טווח הסכמתם של משתתפי המחקר עם כל היגד

השאלון נותח בכלים סטטיסטיים: לבחינת הקשר בין משתנים חושב מתאם פירסון (r) ונבחנה רמת המובהקות (p). ההבדל בין משתנים תוקף ע"י טבלת T, השוואת ממוצעים של 3 קבוצות תוקפה ע"י מבחן ANOVA ומבחן Tokey



מסקנות

הפרת ביטחון המידע קשורה לאקלים החברתי, לכן יש להקפיד על מדיניות אבטחת המידע בארגון בקרב העובדים והמנהלים כאחד.

יש להקפיד על התנהלות המנהלים, זאת לאור הקשר בין פעילותם בווטסאפ לבין הפרת בטחון המידע על ידי העובדים וגם בגלל הדיווח על הפרה ארגונית שהיה גבוה במיוחד בקרבם.

החשש מענישה עולה כאחד הגורמים שקשורים להפרת בטחון המידע. כדאי להגדיר במדיניות הארגון פעולות ענישה מידתיות ומרתיעות, להביאן לידיעת העובדים ולממשן בעת הצורך.

שאלות המחקר

אילו גורמים קשורים להפצת מידע מסווג על ידי עובדי ארגונים ביטחוניים בשיחות ווטסאפ בנושאי העבודה עם עובדים נוספים מהארגון?

- אילו אוכלוסיות הן הפעילות ביותר בשיחות ווטסאפ בנושאי העבודה עם עובדים נוספים מהארגון?
- אילו אוכלוסיות מפרות במידה הגבוהה ביותר את בטחון המידע בשיחות ווטסאפ בנושאי העבודה עם עובדים נוספים מהארגון?
- אילו הפרות בטחון מידע מתבצעות במידה הגבוהה ביותר?
- האם יש קשר בין מאפיינים אישיים של אוכלוסיית המחקר לבין רמת הפרת בטחון המידע המבוצעת/הנתפסת?
- האם יש קשר בין מאפיינים התרבות הארגונית לבין רמת הפרת בטחון המידע המבוצעת/הנתפסת?
- האם יש הבדל ברמת הפרת בטחון המידע המבוצעת בכל אחד מהארגונים?

ממצאים

קשר בין מידת הפעילות הפרטית בווטסאפ לבין מידת הפעילות בנושאי עבודה תומך בפרשנות לתיאוריית העולמות הקטנים (Burnett, Jaeger & Thompson, 2008)

קשר מובהק בין מידת ההפרה הארגונית, לבין מידת הפעילות של הקולגות ($r=.326, p<0.01$) ולבין מידת ההפרה של המנהלים ($r=.432, p<0.01$) בווטסאפ בנושאי עבודה

חיזוק לקשר בין השפעה חברתית מצד ההנהלה הבכירה, המנהלים והקולגות לבין יישום מדיניות אבטחת המידע (Pahnilaa, Siponen & Mahmood, 2007)

קשר מובהק בין מידת ההפרה הארגונית לבין החשש להיענש ($r=.316, p<0.05$) ולבין החשש להיתפס ($r=.300, p<0.05$) מחזק את התיאוריה כי לחשש להיתפס יש השפעה על כוונתם של עובדים לציית למדיניות בטחון המידע (Herath & Rao, 2009)

מידת ההפרה הארגונית הגבוהה ביותר דווחה על ידי המנהלים הזוטרים, והנמוכה ביותר על ידי עובדים שאינם מנהלים

בין שני הארגונים קיים הבדל מובהק ($t(61)=2.34, p<0.05$) בממוצע הדיווחים על מידת ההפרה הארגונית

תודות

תודה לד"ר חגית מישר-טל על ההנחיה וההכוונה. תודה נוספת לעובדי הארגונים הביטחוניים, משיבי הסקר ומקבלי ההחלטות, שאפשרו התממשותו של מחקר זה ואף בחרו לעשות שימוש פנים ארגוני בתוצאותיו, לכבוד הוא לנו.

מקורות

קאהאן, ר' (2015, 20 באפריל). מחקר: 75% מהעובדים והמנהלים בישראל שולחים מידע רגיש בווטסאפ. כלכליסט. נדלה מתוך <http://www.calcalist.co.il/Internet/articles/0.7340.L-3657296.00.html>

Abdul Molok, N. N., Chang, S., & Ahmad, a. (2010). Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. In C. Bolan, (Ed.) *Proceedings of the 8th Australian Information Security Management Conference* (pp 70-90). Perth: Security Research Centre, Edith Cowan University

Burnett, G., Jaeger, P.T., & Thompson, K.M. (2008). Normative behavior and information: The social aspects of information access. *Library & Information Science Research*, 30, 56-66.

Chen, H. & Li, W. (2014). Understanding organization employee's information security omission behavior: an integrated model of social norm and deterrence. *Proceeding of the 19th Pacific Asia Conference on Information Systems*.

Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 154-165.

Pahnilaa, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*.