

פיילוט מחקרי – היערכות למצבי משבר בסייבר בארגונים בישראל

דצמבר 2018

שריד
שרותי מחקר והדרכה



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי



מחקר שמביא תוצאות

רקע

כחלק מהתפיסה הלאומית בסייבר להיערכות ולניהול מצבי משבר פותח שאלון "מידת היערכות למצבי משבר בסייבר (Top10)"

- [https://survey.gov.il/he/preparedness for cyber crises](https://survey.gov.il/he/preparedness%20for%20cyber%20crises)
- [קישור לתפיסה \(שאלון בעמוד 35\)](#)

השאלון כולל עשרה נושאים מרכזיים הרלוונטיים להיערכות למצבי משבר בסייבר

- אחריות ארגונית, נכסי סייבר חיוניים, ניהול סיכונים, מצבי כוננות בסייבר, ידע מקצועי, כ"א, טכנולוגיות ואמצעים, הכשרה ותרגול, ניהול מצבי משבר

שאלון זה נועד להיות כלי מחקרי ועזר היערכות לטובת בעלי תפקידים בארגונים במשק (למידה ו-Benchmark)

רקע

המטרה: תיקוף השאלון ככלי מחקרי ("פיילוט") בקרב מספר מצומצם של ארגונים מתחומים שונים, לקראת מחקרי המשך ו/או הנגשת הכלי.

אופן הביצוע: ראיונות טלפוניים עם מקבלי החלטות רלוונטיים בקרב ארגונים במשק, מתחומים שונים, כאשר בכל ארגון רואיין בעל תפקיד בכיר (לפי השאלון). מרבית הראיונות בוצעו טלפונית (בודדים בחרו להשיב באופן מקוון ישירות בשאלון).

השאלון היה אנונימי (אין שיוך לארגון או האדם המשיב), רק לתחום פעילות הארגון. רואיינו 51 מקבלי החלטות.

מקורות המדגם: שילוב של "ריכוז מפעלים חיוניים" של מערך הסייבר + דגימה מתוך נתוני Dun & Bradstreet עבור חברות ציבוריות ותעשייה + מקורות גלויים (השכלה גבוהה + אינטגרטורים IT + מוניציפלי)

סיכום ומסקנות

ישנם ארגונים רבים הסבורים ש"סייבר אינו רלוונטי להם", להערכתנו הדבר נובע מחוסר מודעות

ישנם ארגונים רבים שיש להם "איש מחשבים או חברה שדואגת לנושא המחשוב" (ולכן לא הצלחנו לראיין אותם), להערכתנו גם פה מדובר בבלבול או חוסר מודעות אצל מקבלי החלטות (איש מחשבים \neq יועץ סייבר)

התהליך המחקרי הינו Scalable, על ידי הגדלת מידת המעורבות של מערך הסייבר באיסוף הנתונים (פירוט בהמשך)

מסתמנים הבדלים בנושא ההיערכות בין חברות מתחומי פעילות שונים או בין פעילויות ספציפיות, אך בשלב זה המדגם הינו מצומצם מכדי להסיק סטטיסטית

שאלות ולקחים ברמת התהליך

- האם התהליך Scalable? כיצד לרתום שיתוף פעולה של הארגונים?
 - שיפור היעילות של איסוף הנתונים – לדוגמה על ידי ביצוע משולב של מכון שריד + מערך הסייבר
 - ייתכן, על ידי ארגון כנסים ייעודיים לתחומי עיסוק מסוימים
 - ייצור Benchmark רחב על פני מגזרים שונים
- שינויים ועדכונים "טכניים" בשאלון
 - הוספת "לא יודע/ת" באפשרויות הבחירה
 - הכנת ממשק להערכה עצמית (בניית כלי-מחשבון מבוסס Excel או Online)
- פעילויות להמשך
 - בניית כלי-מחשבון מבוסס Excel או Online
 - הכשרה של אנשי המערך בשיטות לביצוע ראיונות איכותניים וכמותיים
 - מפגשים F2F
 - סדנאות של המערך

תוצאות

שריד
שרותי מחקר והדרכה



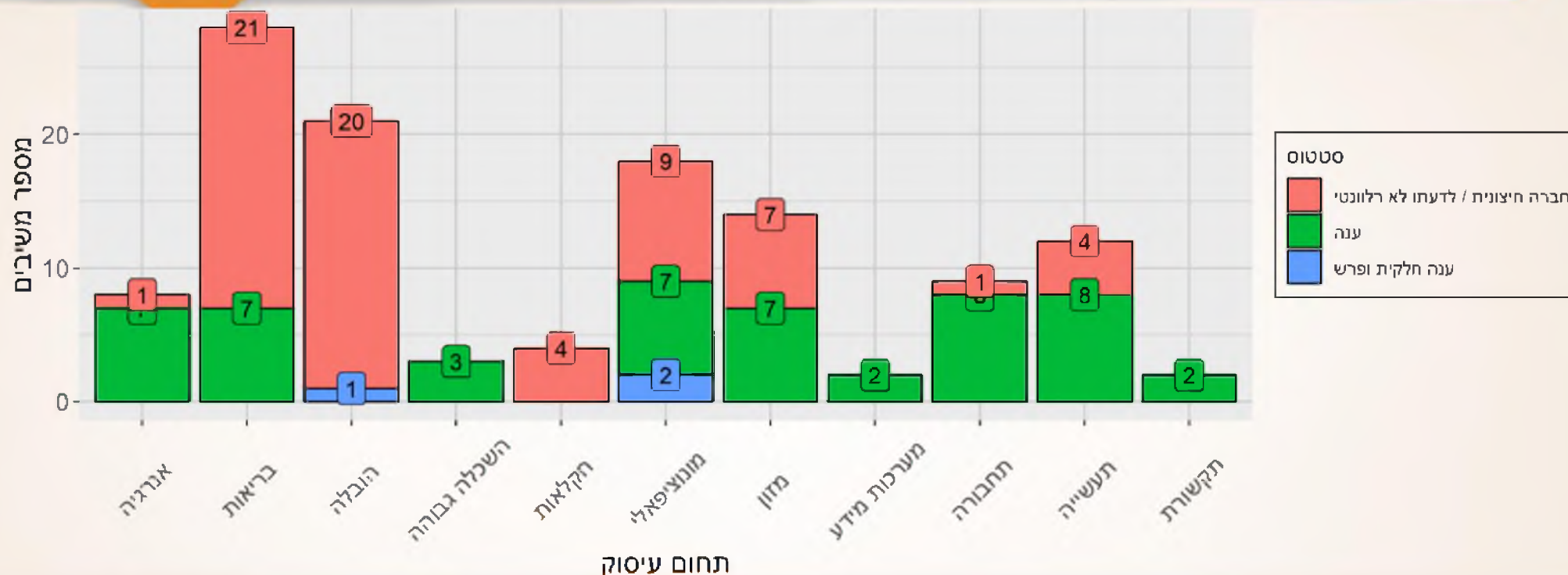
סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי



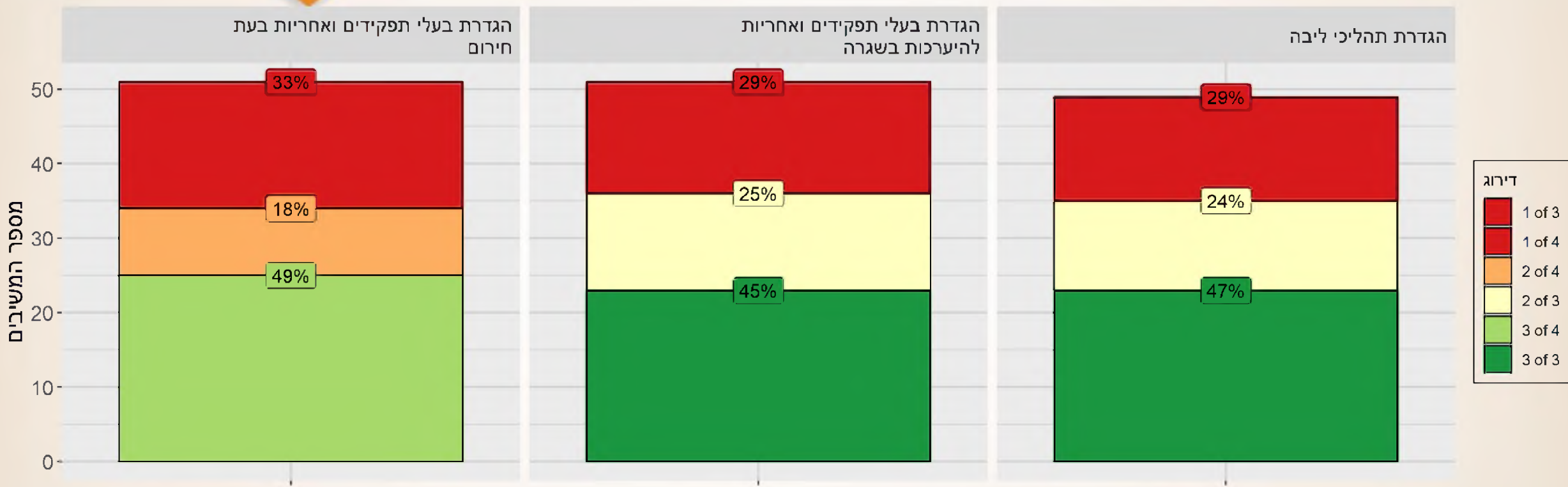
מחקר שמביא תוצאות

נתוני המדגם

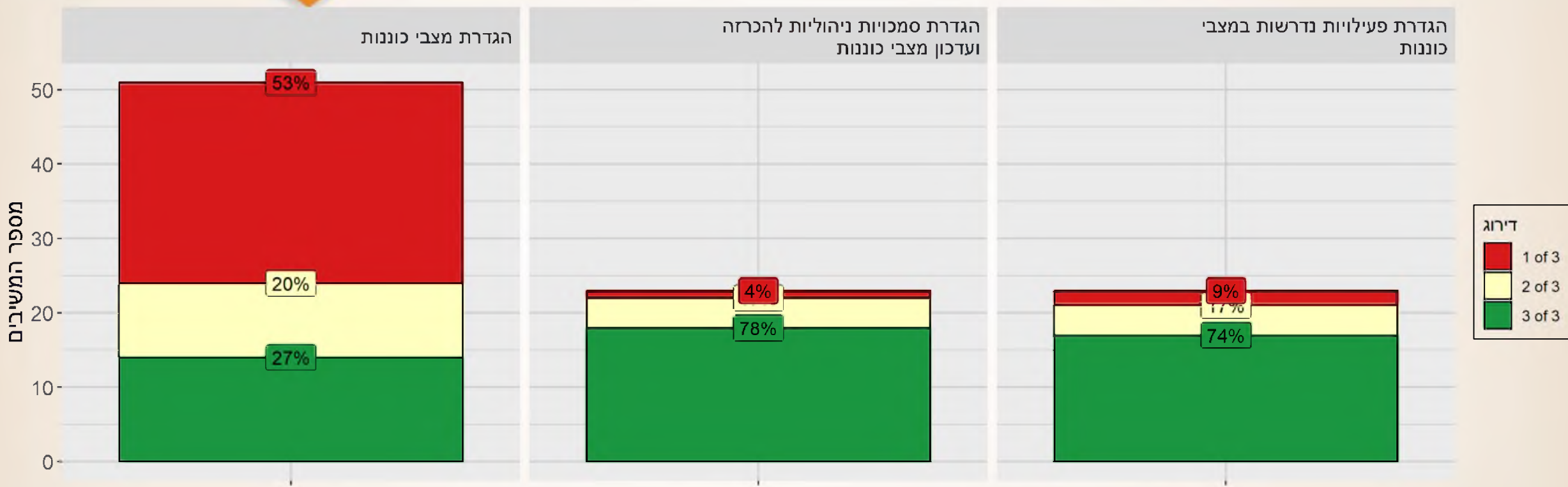


התרשים מציג כ-120 חברות אשר בהן הסוקרים הגיעו לבעל התפקיד הרלוונטי (מנכ"ל / סמנכ"ל), וניתנה הסכמה עקרונית לשתף פעולה. בכמחציתן (53%) ניתנה תשובה של "נושא הסקר לא רלוונטי" בשל העובדה שחברה חיצונית מנהלת את נושא המחשוב (למרות ניסיונות הסוקרים להסביר את הרלוונטיות. מצביע על חוסר מודעות מצד המשיב). בנוסף על נתונים אלו, תועדו עוד 121 סירובים לשיתוף פעולה על הסף, ועוד 217 דחיות ("להתקשר במועד מאוחר יותר"). במקרים מסוימים, הסירוב לווה בחשש הנוגע לחשיפת מידע רגיש למכון המחקר המבצע.

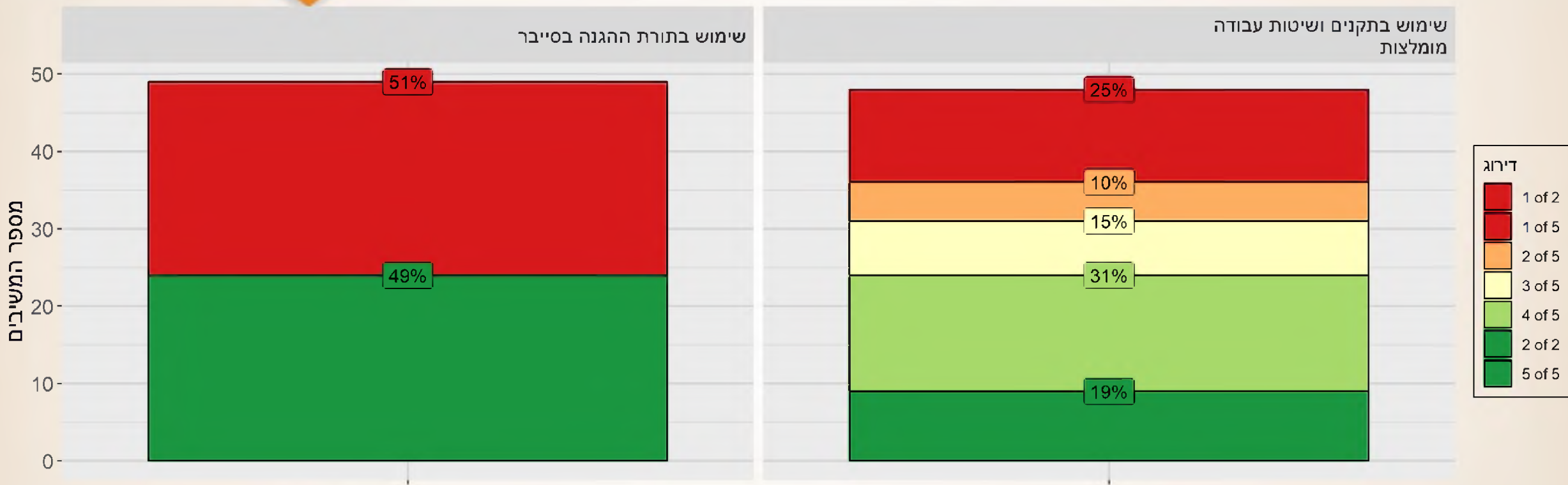
אחריות ארגונית



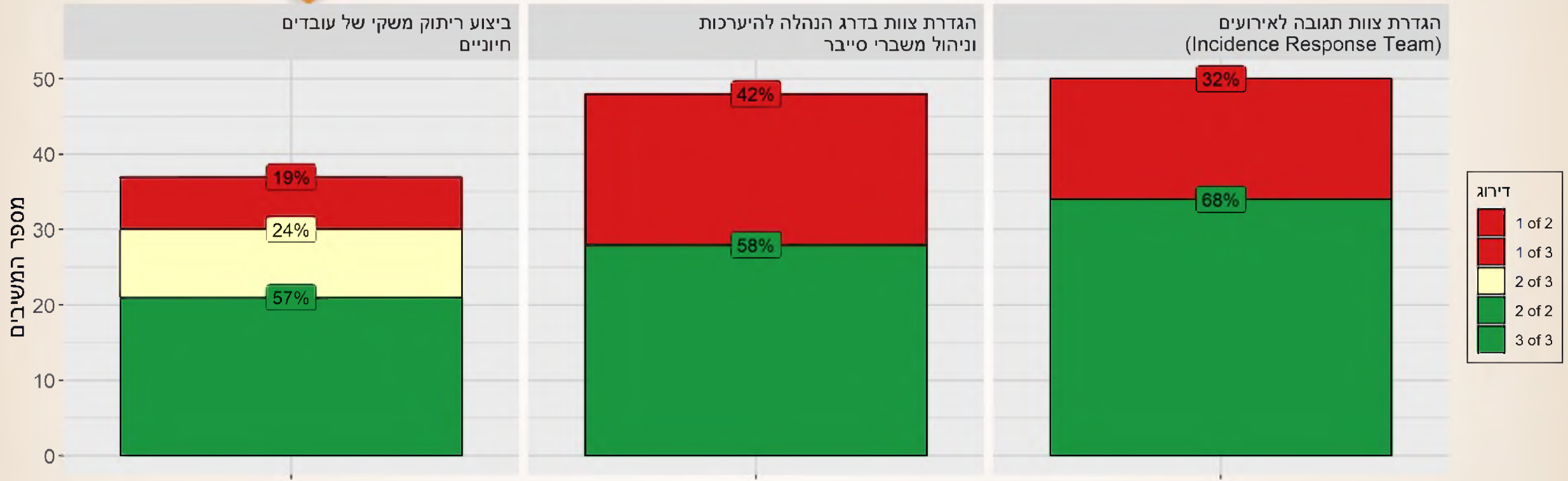
מצבי כוננות בסייבר



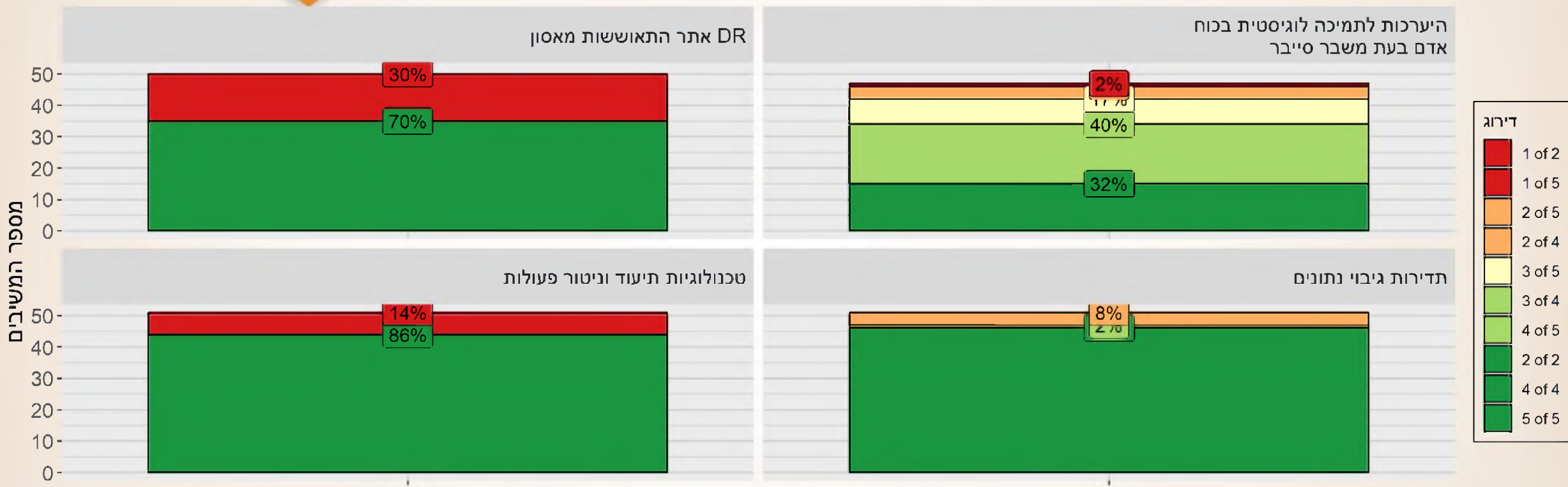
ידע מקצועי



כוח אדם



טכנולוגיות ואמצעים



הסתייעות בגורמים חיצוניים



הכשרה ותרגול



ניהול משברי סייבר



הערות מילוליות – נושאים לשימור

הסקר בנוי טוב ועובר על הכול.

תשובה הם מקושרים ישירות ליחידת הסייבר והם נותנים להם הנחיות.

התחילו את נושא הסייבר לפני כשנתיים. הוא מופתע לטובה ממערך הסייבר הם עובדים בצורה מאוד פתוחה יש הענות לבקשות שלהם. הם מצאו פרטנר טוב לעבודה.

הם כרגע בבניית אתר DR ובניית הנוהל. הוא נעזר וקורא את ההמלצות של מערך הסייבר שנשלחים אליו למייל.

מאוד מרוצה ממערך הסייבר. מתעדכן תמיד, וקורא את המיילים שנשלחים ממערך הסייבר.

הם מקבלים מענה טוב מהסייבר. מקבלים התראות בשטח שזה עוזר להם בעבודה במיוחד בחברות הפרטיות.

זאת השנה הראשונה שלהם המערך הסייבר. הם נעזרים הרבה במערך הסייבר ומתעדכנים מולם.

הערות מילוליות – חשיפה נדרשת

מערך הסייבר עושה עבודת קודש. צריך להגן על הדברים החשובים של המדינה במיוחד מערכת הבריאות. צריך שיהיה יותר מודעות לנושא הסייבר. שתהיה תקשורת יותר טובה בין הסייבר למוסדות הבריאות שהמערך יתן יותר הסברים מפורטים בשביל שהמוסדות יבינו מה צריך לעשות.

מבקשת שמערך הסייבר יהיה יותר ברור מפורט. לדוגמא נשלחים אליה מיילים ממערך הסייבר אבל המיילים לא מספיק מפורטים וברורים. (יש מיילים שלא מבינה מה פרושם).

תשמח לקבל עוד מידע והמלצות על נושא הסייבר ממערך הסייבר.

לטענתו הם מועצה מקומית משק לשעת חירום. הם עדיין לא עוסקים, לא נגעו בנושא הסייבר. יודע שהסייבר נושא חשוב אך אין להם את הכלים, והאנשים.

אין יכולות כספיות להשקיע בסייבר.

נושא הסייבר עדיין לא הגיע אליהם. אין להם שום מידע על הסייבר.

ביקש אם אפשר שמערך הסייבר יוצא חוברת או מסמך של כמה עמודים שבו יהיו מפורטות המלצות של מערך הסייבר למפעלים אך לפעול במצבים שונים והמלצות כלליות.

שמחה לקבל את השיחה. אמרה שלא ידעה בכלל על מערך הסייבר הלאומי. אמרה שבסיום השיחה תכנס ותקרא פרטים. וכן תשמח לקבל מידע ממערך הסייבר.

טענו שהם חברה קטנה של 10 אנשים. נושא הסייבר לא רלוונטי להם. כל המסמכים והחומר הדרוש מודפס ושומר.

הערות מילוליות – נושאים לשיפור

להכניס בשאלון אפשרויות של "לא יודע/ת" / דילוג על שאלות

הם תחנת דלק. משק לשעת חירום. היה שמח אם היתה הדרכה או ליווי אישי. שיתן מענה אך להתמודד. היה לו מקרה שנזקק לעזרת הסייבר. הם עזרו לו באופן חלקי עזרה כללית ולא נקודתית. למרות ששלח להם את הבעיה ותפריט מסודר. המענה לא ניתן.

ההנחיות לא תמיד ברורות מהסייבר.

מבקשת שמערך הסייבר יהיה יותר ברור מפורט. לדוגמא נשלחים אליה מיילים ממערך הסייבר אבל המיילים לא מספיק מפורטים וברורים (יש מיילים שלא מבינה מה פרושם).

טוען שבמשרד הבריאות יצאה הודעה על קורס סייבר שיפתח. הקורס נועד רק לעובדי קבלן (מיקור חוץ). אם יש לו עובד מדינה שהוא לא עובד קבלן העובד לא יכול לקבל את הקורס. שזה לא בסדר העובד קבלן הוא לא קבוע.

רשויות בעלות מעמד סוציו-אקונומיות נמוך (הם דרגה 2) שאין להם יכולות כספיות למערך הסייבר. כדאי לפתוח להן הדרכות לארגון ולהנהלה בנושא הסייבר. על מנת ללמוד ולהתפתח בנושא.

לטענתו במועצה אזורית יש רק אדם אחד שמטפל בנושא מיחשוב וסייבר. צריך ליישר קו בצורה מקצועית. מערך הסייבר צריך לבוא לפחות אחת לשנה לתת עידכונים לאיש המחשבים לרענן זאת בשביל לשמור על אותה הרמה לכולם. צריך לצייד את הרשויות בכלים. לעדכן בנוהל מסודר של מערך הסייבר לרשויות. בגלל החשיבות הגדולה של הנושא.

כל נושא הסייבר זה תקציבים. יש מודעות אבל עדיין זה לא מספיק. צריך ל"חנך" את ההנהלה בשביל שיהיה אבטחת מידע ולא את אנשי השטח.

טוענת שהשאלון לא מתאים לעסקים קטנים. שאלות של אוניברסיטה.

תוך כדי השיחה נכנסה לגוגל לאתר הסייבר ובדקה על מה מדובר. אמרה שלא ידעה שקיים אתר הודתה לי ואמרה שתכנס לקרוא.