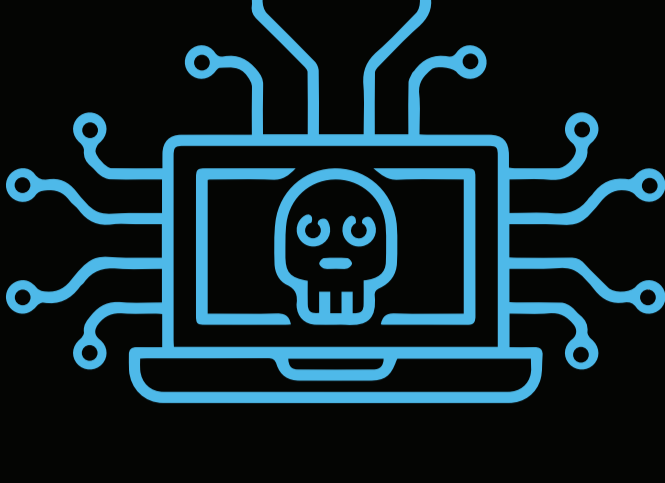




# השוק הישראלי ואיומי סייבר

תמונת מצב 2017

לקראת שבוע הסייבר הלאומי ערכו פירמת הייעוץ וראיית החשבון Deloitte, איגוד האינטרנט הישראלי, חברת הייעוץ קונפיידס והמרכז למחקר סייבר בינתחומי ע"ש בלווטניק באוניברסיטת תל אביב, סקר במטרה לגבש תמונת מצב עדכנית על אופן ההתמודדות בישראל עם סיכוני הסייבר.

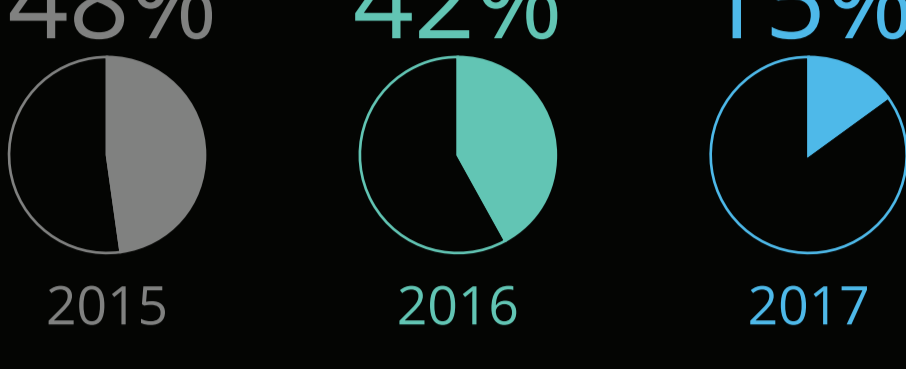


השנה נרשמה ירידה משמעותית במספר הארגונים שחוו אירוע סייבר משמעותי שהשפיע בפועל על ארגונם. נתון זה אינו מרמז בהכרח על ירידה בהיקף התקיפה, אלא על זיהוי וטיפול נכון יותר של ארגונים בתקיפות סייבר שמזערה את השלכותיהן על הארגון.



החברות שכן חוו אירוע סייבר משמעותי מדווחות על נזק ממוצע של כ- 100 אלף דולר ופגיעה משמעותית במוניטין שלהן.

היקף הארגונים שחוו אירוע סייבר שהשפיע בפועל על ארגונם **צומצם בשני שלישי** בשנתיים האחרונות.



## הישראלים מתחילים להבין שניתן לצמצם את סיכון הסייבר משמעותית, בין היתר באמצעות:

- מינוי מנהל הגנת הסייבר מהחברות** (לעומת 23% ב-2016)
- תוכנית מודעות להבנת הסיכונים בכלל האוכלוסיות בארגון** (לעומת 24% ב-2016)
- בדיקה אפקטיבית מערכי ההגנה באמצעות תרגול וניהול הסיכונים אחת לשנה** (לעומת 23% ב-2016)
- שיפור מערכי הזיהוי והתחקור באמצעות טכנולוגיה ותהליכי שיפור** (לעומת 22% ב-2016)
- הקמת צוות לניהול משברי סייבר וכתובת תוכנית להתמודדות עם אירועי סייבר** (לעומת 22% ב-2016)

## חברות גדולות יותר משקיעות יותר בכל מדדי הגנת הסייבר

**מדיניות תאגידית:** הביקורת הפנימית מבקרת את ניהול ויישום הגנת הסייבר

**ניהול סיכונים:** הארגון אוסף ומנתח מידע לקבלת תמונת איום סייבר עדכנית

57% מהחברות הגדולות לעומת 40% בממוצע

קיימת בארגון מסגרת לניהול סיכוני סייבר ומדיניות הגנת סייבר תאגידית

ההנהלה והדירקטוריון מקבלים דיווח שוטף על סיכוני ואירועי סייבר

נערך סקר סיכוני סייבר רחבי בשנה האחרונה

מועסק מנהל הגנת סייבר

52% מהחברות הגדולות לעומת 42% בממוצע

77% מהחברות הגדולות לעומת 51% בממוצע

**מודעות ותרגול:**

## ועדיין, גם ארגונים גדולים לא מנהלים באופן מלא את סיכוני הסייבר שלהם:

רק מחצית מהארגונים הגדולים ערכו סקר סיכוני סייבר בשנה האחרונה או פיתחו מסגרת לניהול סיכוני סייבר ומדיניות הגנת סייבר תאגידית.

כ-1/4 מהארגונים הגדולים והבינוניים לא מתרגלים כלל את צוות ניהול משברי הסייבר שלהן.

כ-1/3 מהארגונים הגדולים וכ-45% מהארגונים הבינוניים מתרגלים את צוות ניהול משברי הסייבר רק פעם בשנה.

פונים לחברות פרטיות

בעת משבר, ארגונים פונים לחברות פרטיות יותר מאשר לגורמים ממשלתיים.

27% פונים ליחידת הסייבר של משרת ישראל

18% פונים לרגולטור אחראי

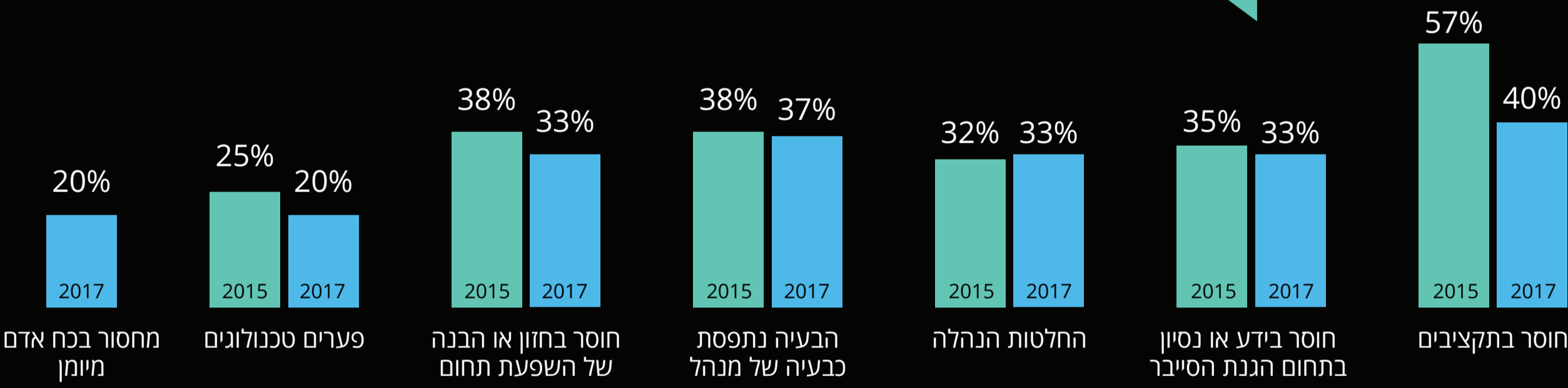
32% פונים לקולגות מקצועיים

32% פונים לרשות הסייבר הלאומית

45%

ובכלל, כרבע מהמשיבים (24%) לא מעוניינים במעורבותם של גורמים ממשלתיים בניהול משברי סייבר. החברות שכן מעוניינות, מצפות למעורבות גורמים ממשלתיים לאחר האירוע (51%) יותר מאשר לפניו (44%) או במהלכו (46%).

## המכשולים המשמעותיים ביותר ביישום האסטרטגיה או התכנית בתחום הגנת הסייבר



למרות המודעות ההולכת וגוברת לחשיבות ניהול סיכוני סייבר...

בכ-40% מהארגונים סיכוני סייבר לא נתפסים כבעיה של כלל הארגון.

בכשליש מהארגונים היעדר חזון והבנה של התחום והחלטות הנהלה מקשות על יישום אסטרטגיית הגנת הסייבר.

כמחצית מהמנהלים צופים 11% גידול ממוצע בתקציב הגנת הסייבר בארגונם במהלך השנה הבאה. העלייה העקבית בשנים האחרונות בתקציבי הגנת הסייבר ניכרת בדירוג היורד של "חסר בתקציבים" ו"פערים טכנולוגיים" כמכשול עיקרי ליישום מדיניות הגנת הסייבר של ארגונים.

היעדר כח אדם מיומן בעל ידע וניסיון מהווה מכשול משמעותי יותר מבעבר ליישום מדיניות הגנת סייבר. מחסור זה הוא גם הסיבה העיקרית לרכישת שירותי סייבר מנהלים.

מחסור בכח אדם 31%

מחסור בידע מקצועי 26%

חשבוני עלות תועלת כלכלית 29%

יעילות 6%

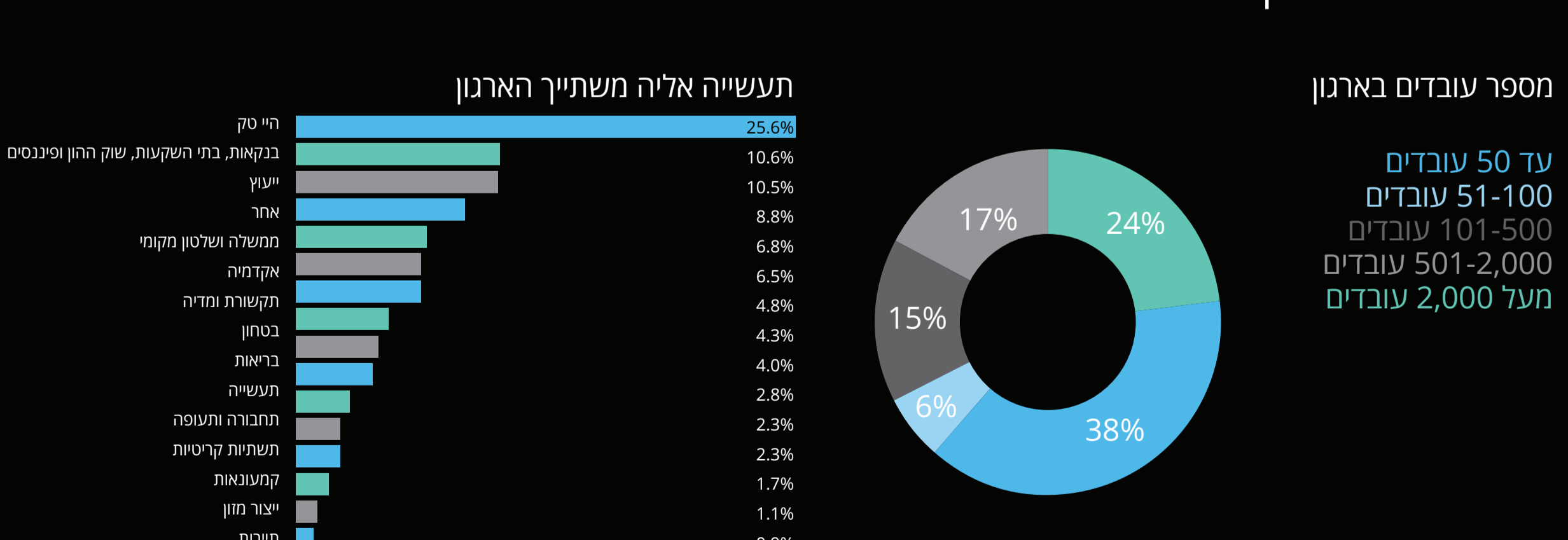
אחר 9%

סיבות לרכישת שירותי סייבר מנהלים:

## מתוך הסקר עולות 5 פרקטיקות לשיפור הגנת הסייבר

- מינוי מנהל הגנת הסייבר
- תוכנית מודעות להבנת הסיכונים בכלל האוכלוסיות בארגון
- בדיקה אפקטיבית מערכי ההגנה באמצעות תרגול וניהול הסיכונים אחת לשנה
- שיפור מערכי הזיהוי והתחקור באמצעות טכנולוגיה ותהליכי שיפור
- הקמת צוות לניהול משברי סייבר וכתובת תוכנית להתמודדות עם אירועי סייבר

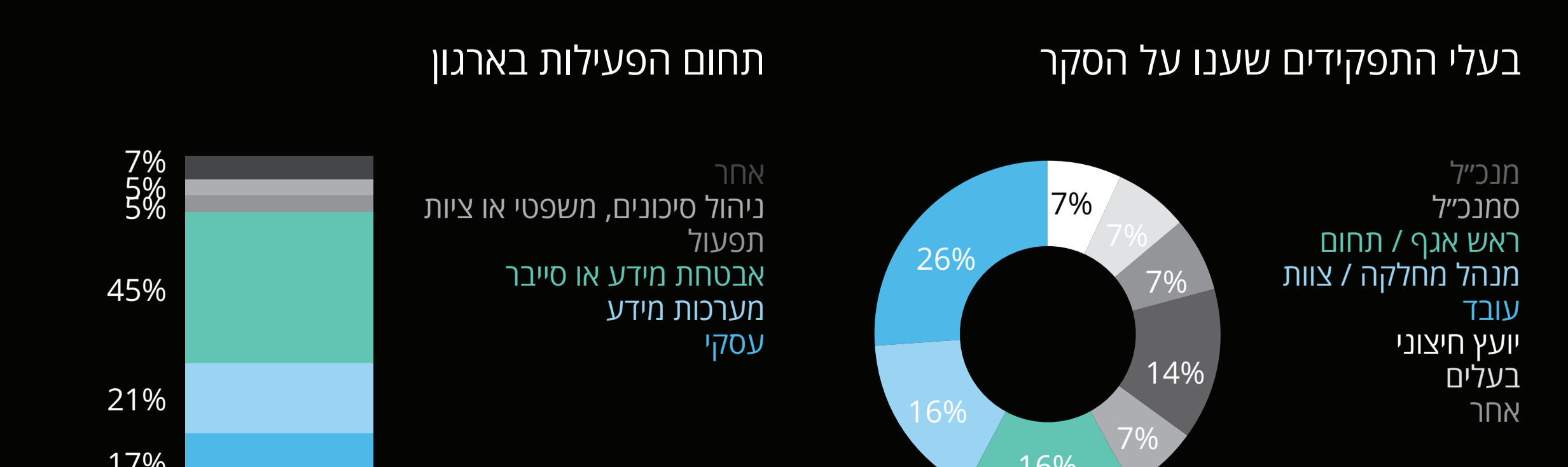
## על הסקר ענו השנה 382 משיבים מארגונים בגדלים שונים ומשלל תעשיות



המדגם מורכב ברובו ממנהלים בתחומי מערכות מידע, אבטחת מידע ותפקידים עסקיים הקשורים לליבת העשייה של הארגון

תחום הפעילות בארגון

בעלי התפקידים שענו על הסקר



7% אחר, 5% ניהול סיכונים, משפטי או ציות תפעולי, 45% אבטחת מידע או סייבר, 21% מערכות מידע עסקי, 17% אחר

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 225,000 professionals are committed to becoming the standard of excellence.

Brightman Almagor Zohar & Co. (Deloitte Israel) is the member firm of Deloitte Touche Tohmatsu Limited in Israel. Deloitte Israel is one of Israel's leading professional services firms, providing a wide range of world-class audit, tax, consulting, financial advisory and trust services. Through 83 partners and directors and approximately 1,000 employees the firm serves domestic and international clients, public institutions and promising fast-growth companies whose shares are traded on the Israeli, US and European capital markets.