Deloitte.

# השוק הישראלי ואיומי סייבר
## תמונת מצב 2017

לקראת שבוע הסייבר הלאומי ערכו פירמת הייעוץ והאיש החשבון Deloitte, אינוד האינטרנט הישראלי, חברת הייעוץ קונפידנט והמרכז למחקר סייבר בינתחומי ע"ש בלווטניק באוניברסיטת תל אביב, סקר במטרה לבנש 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 יותר טיפול בכוון יותר של ארגונים בתקיפות סייבר שמעידו את השלכותיהן על הארגון.

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


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

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

מינוי מנהל הגנת הסייבר
**51% מהחברות**
(לעומת 23% ב-2016)

תוכנית מודעות להגנת הסיכונים בכל האוכלוסיות בארגון
**53% מהחברות**
(לעומת 24% ב-2016)

בדיקה אפקטיביות מערכי ההגנה באמצעות תרגול לניהול הסיכונים אחת לשנה
**48% מהחברות**
(לעומת 23% ב-2016)

שיפור מערכי הזיהוי והתחקור באמצעות טכנולוגיה ותהליכי שיפור
**62% מהחברות**
(לעומת 22% ב-2016)



הקמת צוות לניהול משברי סייבר ותרגיל תוכנית להתמודדות עם אירועי סייבר
**58% מהחברות**

## חברות גדולות יותר משקיעות יותר בכל מדדי הגנת הסייבר

### מדיניות תאגידית:

הביקורת הפנימית מבקרת את ניהול ויישום הגנת הסייבר
**57%** מהחברות הגדולות לעומת 40% בממוצע

ההנהלה והדירקטוריון מקבלים דיווח שוטף על סיכוני ואיראוי סייבר
**63%** מהחברות הגדולות לעומת 52% בממוצע

מועסק מנהל הגנת סייבר
**77%** מהחברות הגדולות לעומת 51% בממוצע

### ניהול סיכונים:



הארגון אוסף ומנתח מידע לקבלת תמונת איום סייבר עדכנית
**60%** מהחברות הגדולות לעומת 45% בממוצע



קיימת בארגון מסגרת לניהול סיכוני סייבר ומדיניות הגנת סייבר תאגידית
**56%** מהחברות הגדולות לעומת 45% בממוצע



נערך סקר סיכוני סייבר רחבי בשנה האחרונה
**52%** מהחברות הגדולות לעומת 42% בממוצע

### מודעות ותרגול:



לארגון תוכנית מודעות ותרגול לשיפור הגנת הסייבר
**71%** מהחברות הגדולות לעומת 53% בממוצע



אפקטיביות מערך הגנת הסייבר בארגון נמדדה
**61%** מהחברות הגדולות לעומת 48% בממוצע

## 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.

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

18%
פונים לדוגלטור אחותאי

32%
פונים לרשות הסייבר הלאומית

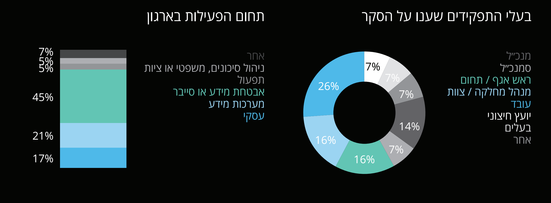
27%
פונים ליחידת הסייבר של משטרת ישראל

32%
פונים לקולנות מקצועיים

45%
פונים לחברות פרטיות

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

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




כמחצית מהמנהלים צופים
**11% גידול ממוצע בתקציב**
הגנת הסייבר בארגונם במהלך השנה הקרובה. העלייה הצפויה בשנים האחרונות בתקציבי הגנת הסייבר ניכרת בייחוד אצל "חוסר בתקציבים" ו"פערים טכנולוגיים" כמעשות עיקרי ליישום מדיניות הגנת הסייבר של ארגונים.



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 ההנהלה מקשות על יישום אסטרטגיות הגנת הסייבר.

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.


סיבות לרכישת שירותי סייבר מנוהלים:

## מתוך הסקר עולות 5 פרקטיקות לשיפור הגנת הסייבר



1 מינוי מנהל הגנת הסייבר



2 תוכנית מודעות להגנת הסיכונים בכלל האוכלוסיות בארגון



3 בדיקה אפקטיביות מערכי ההגנה באמצעות תרגול לניהול הסיכונים אחת לשנה



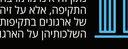
4 שיפור מערכי הזיהוי והתחקור באמצעות טכנולוגיה ותהליכי שיפור



5 הקמת צוות לניהול משבר סייבר וכתיבת תוכנית להתמודדות עם אירועי סייבר

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

### מספר עובדים בארגון

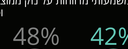



- עד 50 עובדים
- 51-100 עובדים
- 101-500 עובדים
- 501-2,000 עובדים
- מעל 2,000 עובדים

### תעשייה אליה משתייך הארגון


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

### בעלי התפקידים שענו על הסקר




- מנכ"ל
- סמנכ"ל
- ראש אגף / תחום
- מנהל מחלקה / צוות
- עובד
- יועץ חיצוני
- בעלים
- אחר

### תחום הפעילות בארגון


- אחר
- ניהול סיכונים, משפטי או ציות
- תפעול
- אבטחת מידע או סייבר
- מערכות מידע
- עסקי