

# תורת ההגנה הארגונית

ר' תחום תורה  
אגף אסדרה והכשרה  
יובל שגב

הרשות הלאומית  
להגנת הסייבר

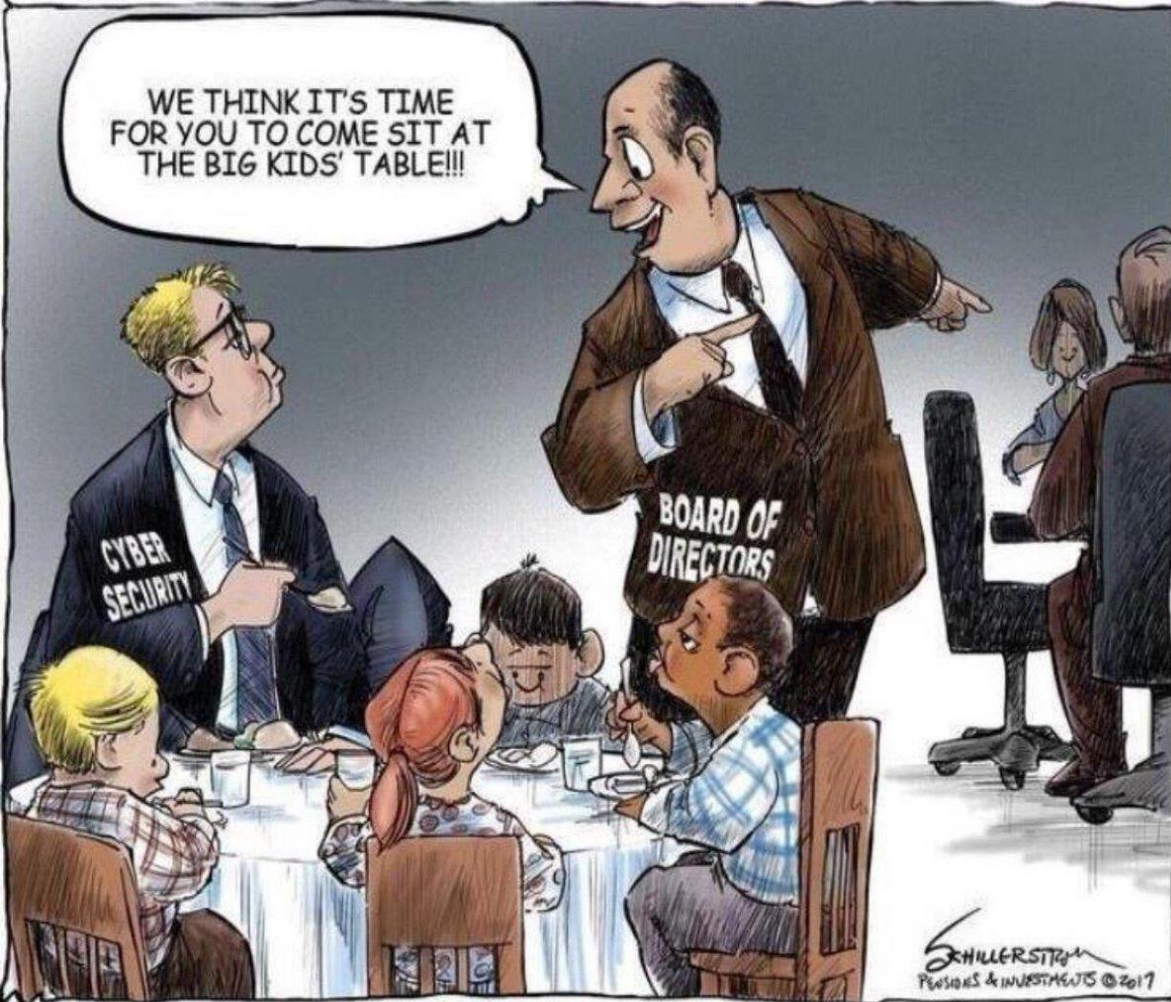


משרד ראש הממשלה  
משרד הסייבר הלאומי



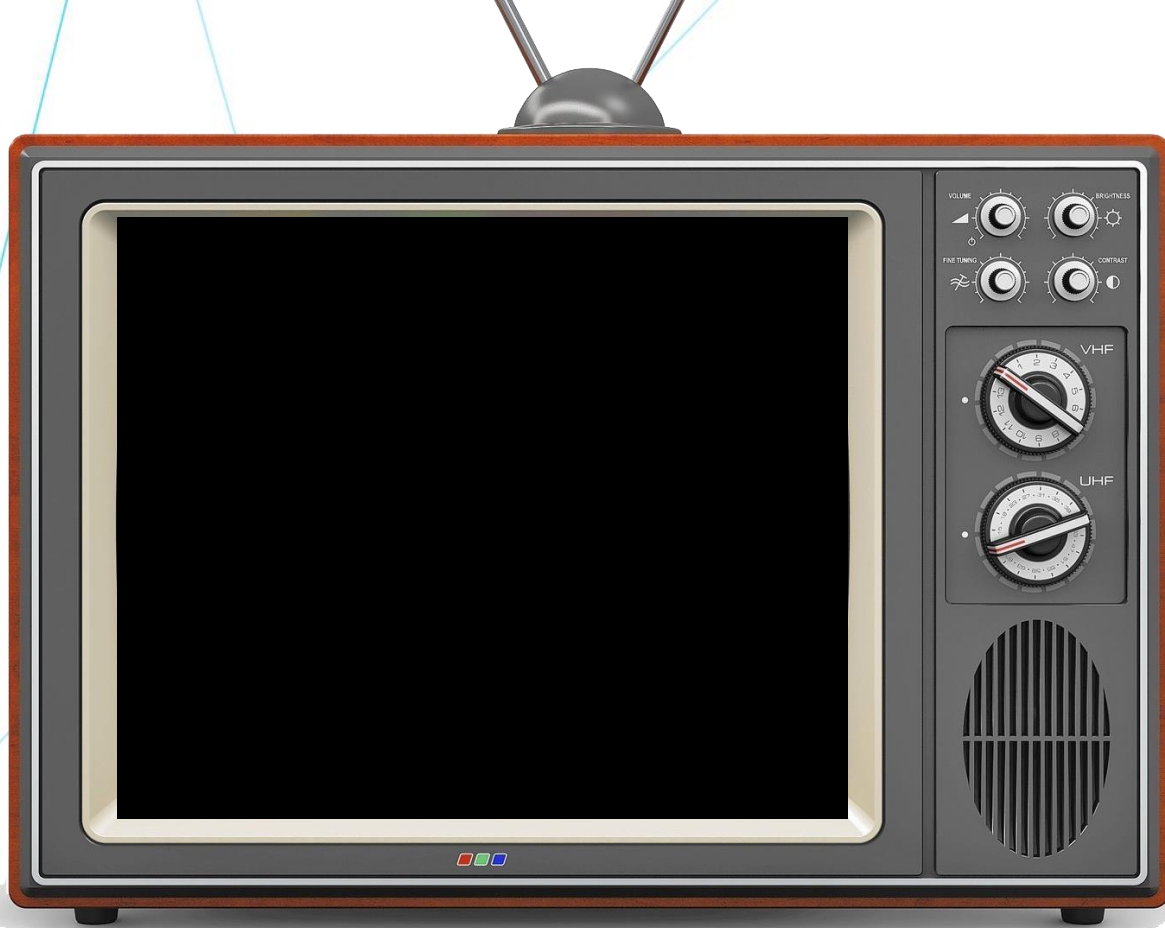
# שאלון קצד

מצב נוכחי - הגנה בסייבר





# תוצאות השאלון



2017

תקנות הגנת  
הפרטיות

1995

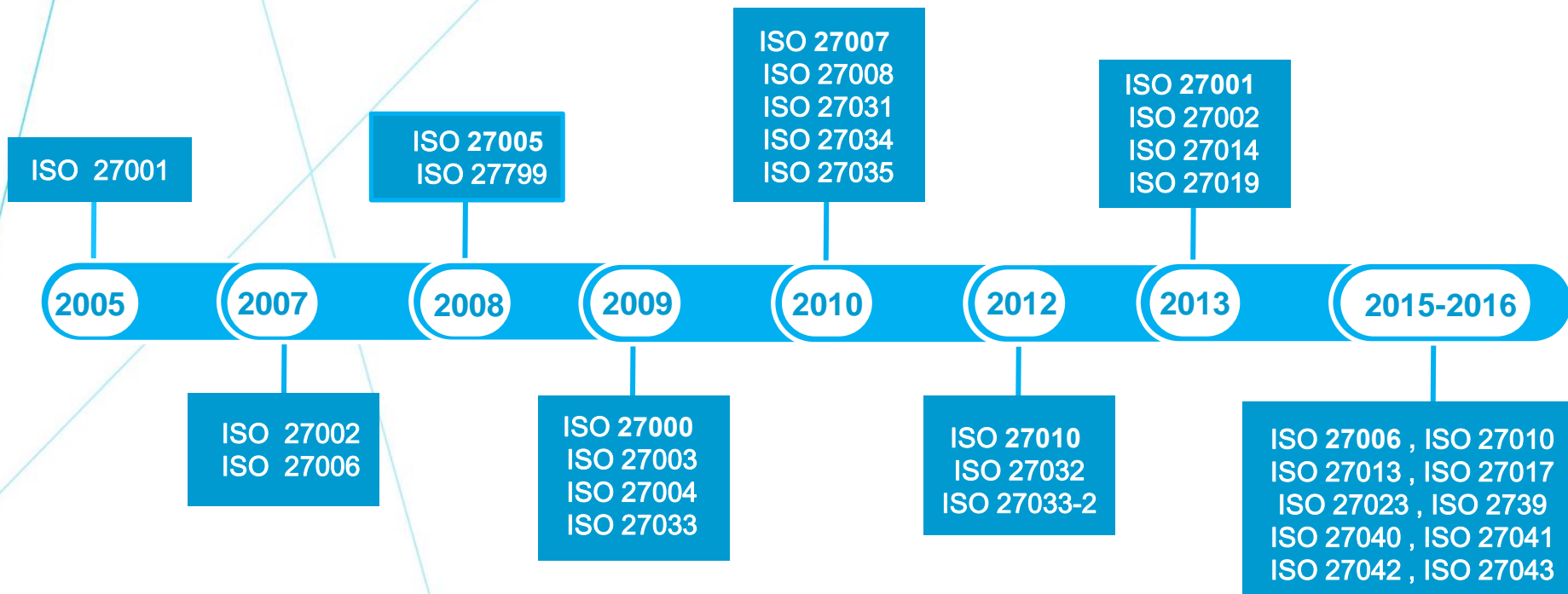
חוק המחשבים

1981

תקנות הגנת  
הפרטיות

# ובינתיים בעולם

משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר







משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר



10-20  
מסמכים בשנה



תורת ההגנה הארגונית  
מגדלור למשק



# מבנה תורת ההגנה

משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר





### מידתיות

תוכנית עבודה  
ארגונית אפקטיבית  
חייבת להישען על  
הערכת סיכונים טובה



### אחריות הנהלה

ההגנה על הארגון  
הינה באחריות של  
הנהלת הארגון



### 3 P's

הגנה על הארגון  
מורכבת משלושה  
נדבכים עיקריים



### ידע וניסיון מקומי

היתרון בהיותנו  
קטנים

# עקרונות תורת ההגנה

# מידתיות תהליך ניהול הסיכונים

משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר



במידה שיתרחש אירוע סייבר בארגוןך,  
האם עלות הטיפול באירוע לארגון  
תהיה גבוהה מ-500,000 ש"ח?

טיפ: עלות הנזק כתוצאה מאירוע  
סייבר כוללת נזקים ישירים  
ועקיפים לעסק. עם עלויות אלה  
נמנים: זמני השבתת שירות, פגיעה  
במוניטין, עלות בנין סנקציות  
שיוטלו לאור הפרת דרישות חוק  
ורגולציה ועוד.

בעת מענה על השאלה שלהלן, יש לקחת בחשבון את העלות הכוללת. ארגונים אשר השיבו בשלילה על השאלה הנ"ל, משויכים לקטגוריה א'. ארגונים אשר השיבו בחיוב, משויכים לקטגוריה ב'.

# פרקי הבקרות

משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר



**שלב:**  
זהוי (IDENTIFY)

**משפחת בקרות:**  
- אחריות דירקטוריון והנהלה  
- ניהול סיכונים והערכת סיכונים  
- בקרה, ביקורת ותאימות

**שלב:** הגנה (PROTECT)

**משפחת בקרות:**  
- בקרת גישה  
- הגנה על המידע  
- הגנה על שרתים ותחנות עבודה  
- מניעת קוד זדוני  
- הצפנה  
- אבטחת רשת  
- הפרדת סביבות  
- אבטחה בענן  
- הגנה על בקרים תעשייתיים  
- אבטחת סלפונים סלולריים  
- ניהול שוניים

- אבטחת מדיה  
- אבטחת שרשרת אספקה ומיקרו-חץ  
- אבטחה ברכש ופיתוח  
- הגנה פיזית וסביבתית  
- משאבי אנוש ומודעות עובדים  
- הדרכות

**שלב:**  
איתור (DETECT)

**משפחת בקרות:**  
- תיעוד וניטור  
- סקרי הערכה של בקרות אבטחה  
- הגנת סייבר פרואקטיבית

**שלב:**  
תגובה (RESPOND)

**משפחת בקרות:**  
- ניהול אירועים ודיווח

**שלב:**  
התאוששות (RECOVER)

**משפחת בקרות:**  
- המשכות עסקית



# יתרונות תורת הגנה תועלות בעיני הארגון

התאמה למידות המשק

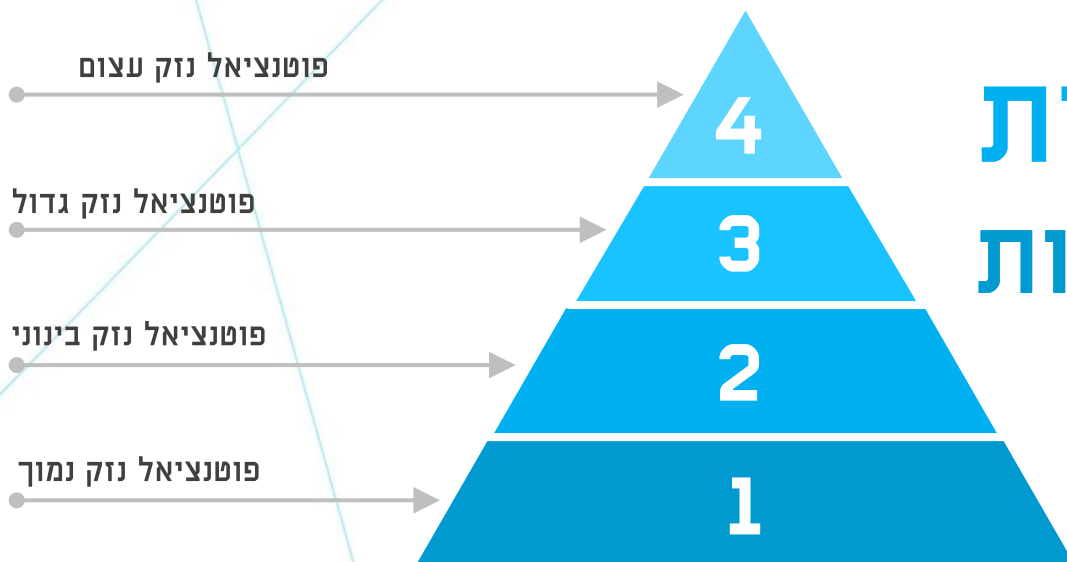
הפריה מצד ראיית התוקף והמודיעין

עזרים נלווים

יכולת להשפיע על תוכן תורת ההגנה

שפה מותאמת ללקוח

תאימות מול תקינה ורגולציה מקומית



# 1 מידתיות

## התאמה למידות המשק

# שיח מגן תוקף ומודיעין

2



יכולת להשפיע

3





# תאימות לתקנים ורגולציות

5



# רגע לפני שרצים ליישם



# תכנית דו-שנתית

משרד ראש הממשלה  
מערך הסייבר הלאומי  
הרשות הלאומית להגנת הסייבר



- הדרכות וכנסים
- גיבוש צרכים (כלים ותכנים)

2017

2018

2019

- מטריצת תאימות
- קבוצות עבודה
- טיוטות ומעגלי התייחסות

- ריכוז התייחסויות
- גיבוש נושאים לגרסה 2.0
- הפצת נספחים ומסמכי הרחבה

- הפצת גרסה 2.0 להתייחסויות

20 July 1969







מיכאל



יאיר

# Feedback





**יובל שגב**  
ראש תחום תורה  
**yuvalse@pmo.gov.il**

**תודה רבה**