

יובל שגב
ראש מחלקת מתודולוגיה
מערך הסייבר הלאומי
ינואר 2019

1956, 5 מגה בייט זכרון של חברת IBM



חוק הביקורת הפנימית, תשנ"ב-1992
נוסח מלא ומעודכן

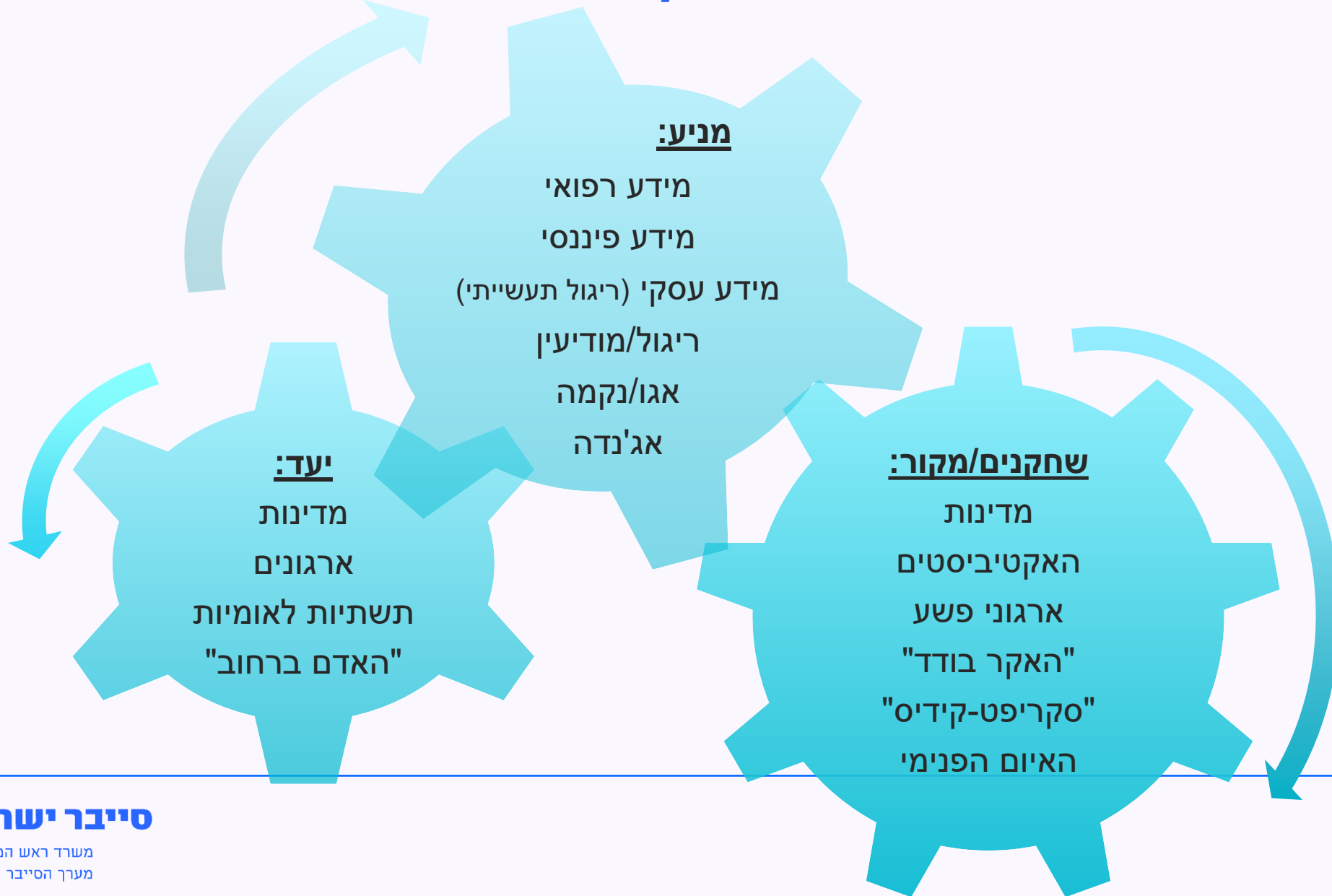
חוק הביקורת הפנימית, תשנ"ב-1992

תפקידים

4.

- (א) המבקר הפנימי יבדוק, בין היתר -
 - (1) אם הפעולות של הגוף הציבורי שבו הוא משמש מבקר ושל נושאי משרה וממלאי תפקידים באותו גוף תקינות, מבחינת השמירה על החוק, על הניהול התקין, על טוהר המידות ועל החסכון והיעילות, ואם הן מועילות להשגת היעדים שנקבעו להן;
 - (2) אם מקיימות ההוראות המחייבות את הגוף הציבורי;
 - (3) את ניהול הנכסים וההתחייבויות של הגוף הציבורי, ובכלל זה את הנהלת החשבונות שלו, וכן את דרכי שמירת הרכוש, והחזקת הכספים והשקעתם;
 - (4) אם ההחלטות בגוף הציבורי נתקבלו על פי נהלים תקינים;
 - (5) אם הגוף הציבורי הוא גוף מבוקר כאמור בפסקה (1) או (3) להגדרת גוף ציבורי שבסעיף 1 (להלן - גוף מבוקר) - את תיקון הליקויים שעליהם הצביע מבקר המדינה.
- (ב) המבקר הפנימי יערוך את הביקורת על פי תקנים מקצועיים מקובלים.

"בסייבר, זה אחרת"



רכיב הזיכרון
שבמדפסת

המדפסת
כחיבור לרשת

חיבור USB

שליחת
מייל/פקס
לכתובת שגויה

כניסת וירוס דרך
עדכון תוכנה

נתיב להוצאת
מידע מהארגון

הטמנה בחומרה/
תוכנה

Advanta
COPY



YAHOO!
<AFTERHOURS>
39.95 ↓ 2.35%

Bloomberg

WHO IS RESPONSIBLE FOR YAHOO BREACH

Bloomberg

מאירועי הרשת נגרמים כתוצאה
Misconfigurations - מ

97%

מהמתקפות הידועות יכולות להימנע באמצעות
מימוש 20 "בקרות אב"

88%

הציון הממוצע של גופי Enterprise שנבדקו
בהיבטי יכולות Detect & Respond

50%

מתקציב IT מושקע בסייבר.
תקציב IT נגזר לרוב מהמחזור.

6-8%





If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— *Bruce Schneier* —

AZ QUOTES

Risk = Impact X **Likelihood**

NIST 800-30

CobIT

27005

OCTAVE



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי



גברים ממאדים נשים מנוגה גרסת עולם ה Security



לוגים NAC

DLP SIEM



SSDLC

IPS

MDM

EDR

הקשחה

PIM

פאצ'ים



סייבר ישראל

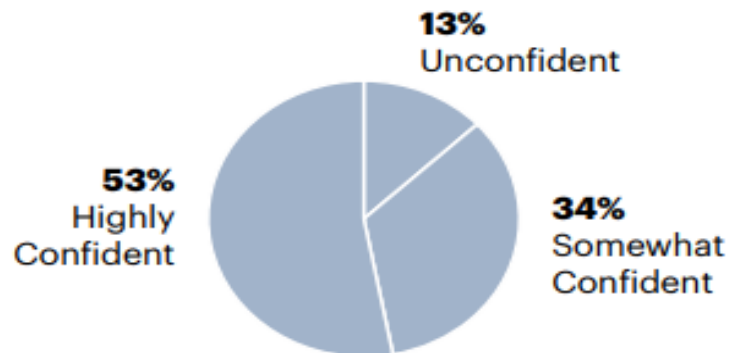
משרד ראש הממשלה
מערך הסייבר הלאומי

2019 Audit Plan Hot Spots Report Excerpt

Five Risk Areas to Watch

Confidence in Audit's Ability to Provide Assurance Over Cybersecurity Detection and Prevention Risks

Percentage of Respondents

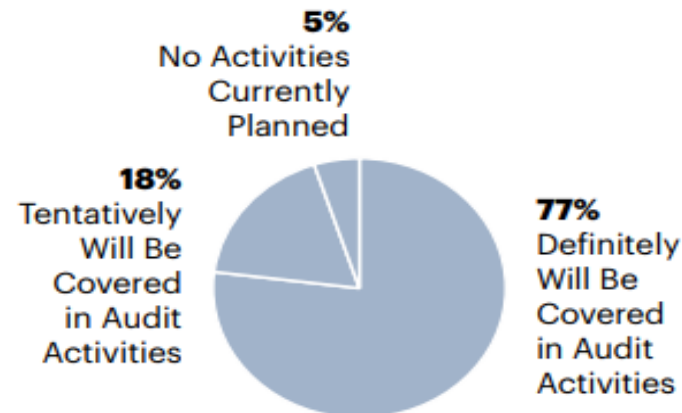


n = 143

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Plans to Cover Cybersecurity Detection and Prevention in Audit Activities in the Next 12-18 Months

Percentage of Respondents

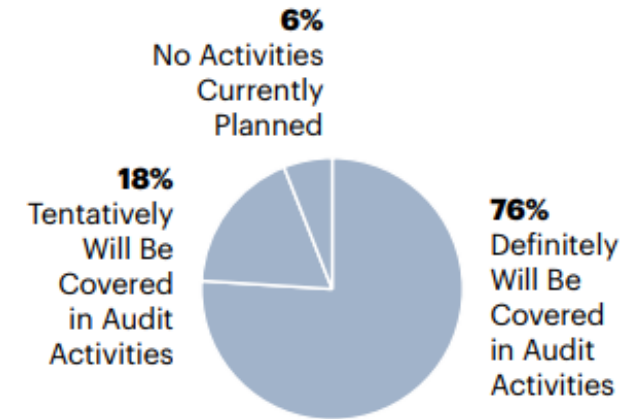


n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Plans to Cover Third-Party Risk in Audit Activities in the Next 12-18 Months

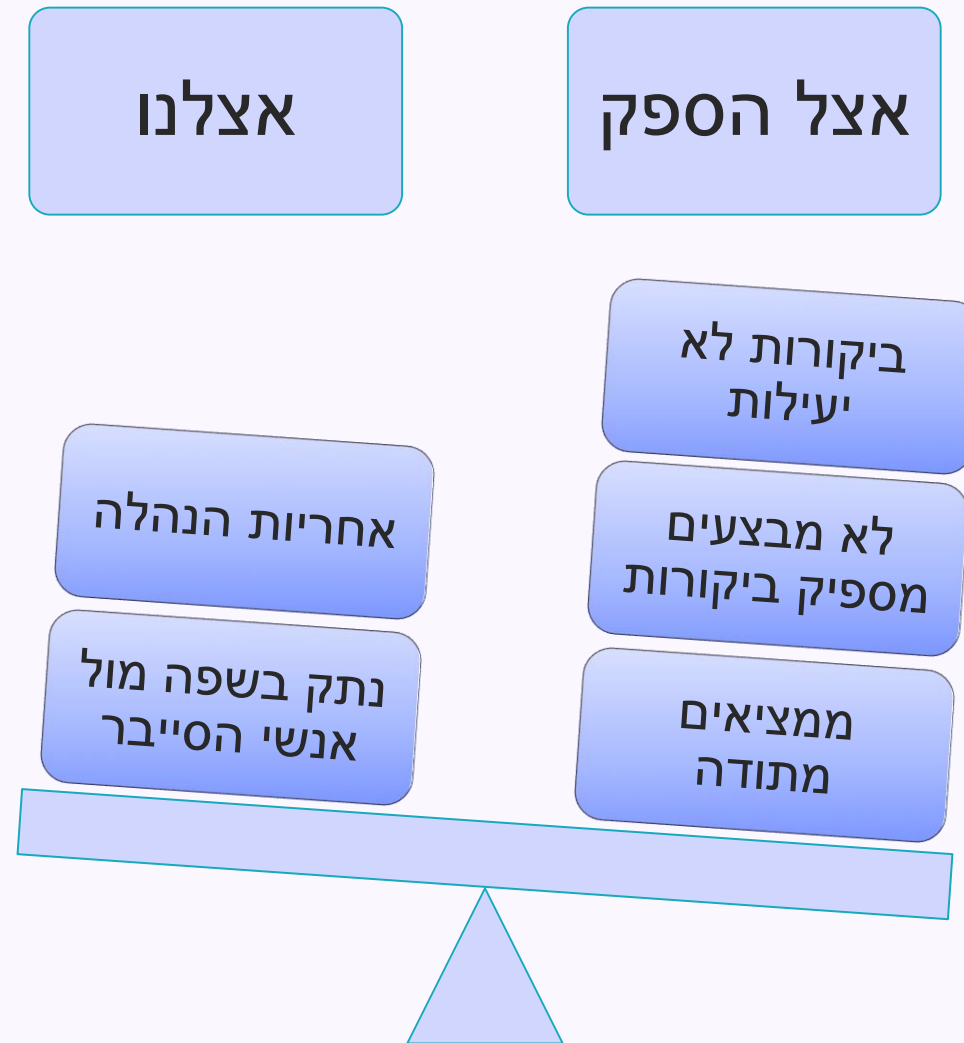
Percentage of Respondents




n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

חלוקת האתגרים



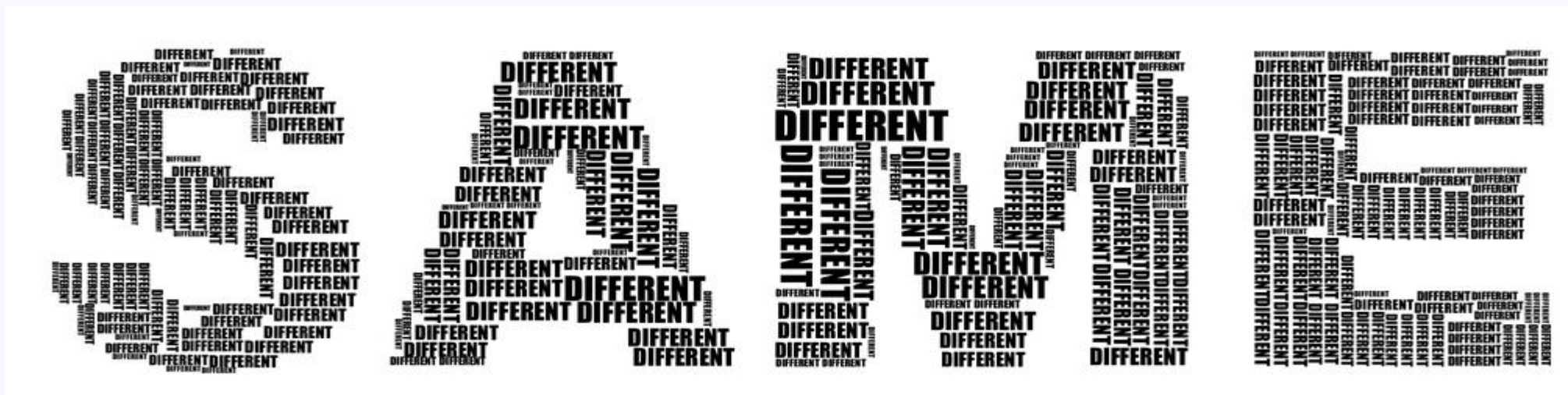
An aerial photograph of a city skyline at sunset. The sun is low on the horizon, casting a bright orange glow over the city. A prominent skyscraper stands out in the center. A river or lake is visible in the lower-left corner. The text is overlaid in the center of the image.

**שרשרת אספקה
מחזקים את החוליה החלשה בשרשרת
דברים שלמדתי בקבוצת המיקוד**

רמת סיכון זהה – הגנה שונה

שרשרת האספקה, משמשת פעמים רבות כאמצעי לתקיפת ארגון היעד. היא משפיעה על הרציפות העסקית, על אמינות ועל סודיות המידע של הלקוחות.

ארגונים רבים במשק עוסקים בהגנה בסייבר על הנכסים השונים שלהם, שעה **שאותו המידע** נגיש דרך שרשרת האספקה שלהם בצורה שאיננה מאובטחת כראוי.



סייבר ישראל

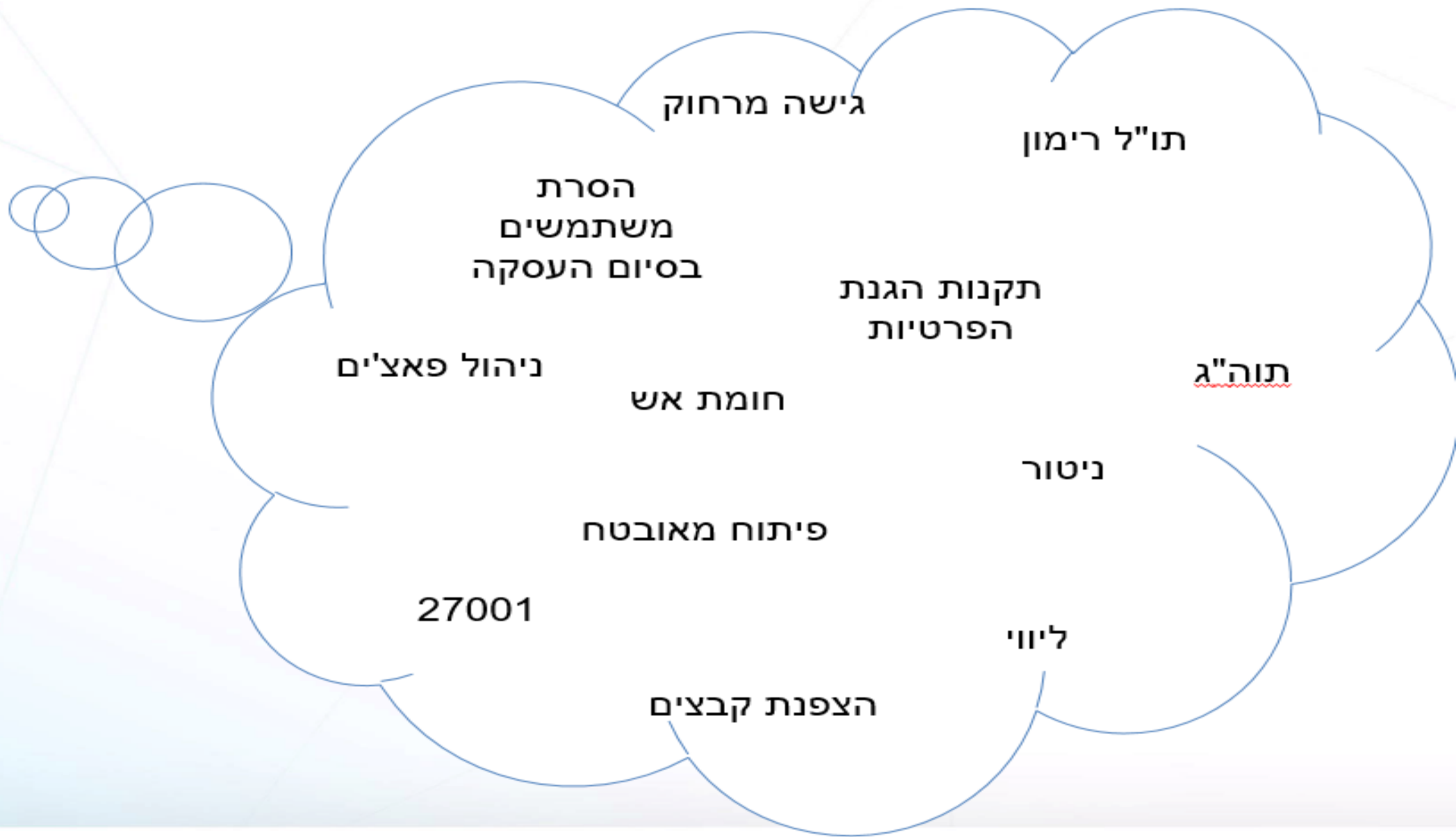
משרד ראש הממשלה
מערך הסייבר הלאומי



Ports

Optical Audio "Toslink"	USB A 1.0/1.1/2.0	Firewire 4 pin iLink	Firewire 400 1394a	Firewire 800/3200 1394b/c	Ethernet 8P8C common:RJ-45	Modem RJ-11	Apple Desktop Bus - ADB	Mac Serial
PS/2	USB A 3.0	DE-9F	DB-25 Serial/Com Port	DE-9 Serial RS232	e-SATA			
Centronics Parallel 36pin	Centronics SCSI 50pin	AT Keyboard						
50 pin SCSI 2	Surround sound	stereo/Headphones	Line In	Mic	Digital Audio RCA plug style			
AAUI	Composite Audio/Video	S-Video	Component Video	F-Connector RF/COAX				
Parallel Port/SCSI 1/DB-25F	Mac Video/MIDI /gameport/AUI/DA-15	Mini DisplayPort	Mini-DVI	Mini-VGA				
Apple Hi-Density Video HDI-45	Apple Display Connector - ADC	LFH60 (dual DVI-D)	DMS59 (dual DVI-D)					
HDMI	Micro-DVI	DisplayPort	DVI Video	DE-15/HD-15 VGA/SVGA				

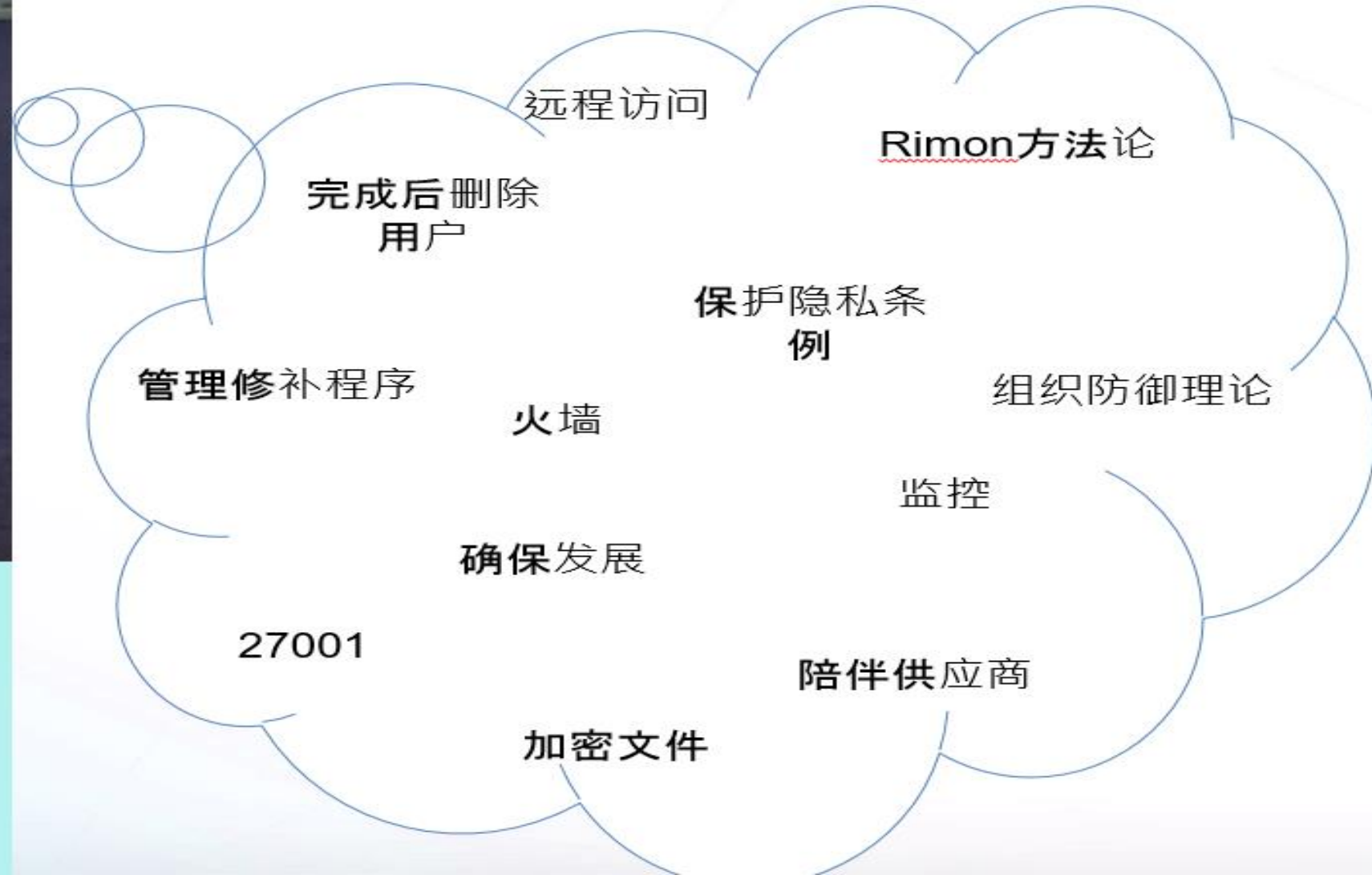
דרישות
הגנה
מהספק
ארגון X



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

ואיך זה נראה בעיני הספק?



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

10%

**כמות הספקים "הרגישים"
מתוך סך הספקים**

2-20 שעות

**משך הזמן שמוקצה
לבדיקת ספק**



15,000 – 5,000

**כמות הספקים שיש
לארגון אנטרפרייז**

פחות מ- 1%

**מספר הארגונים
שמקצים FTE לנושא**

2%

**היכולת של ארגון לבצע ביקורת
בחצרות הספק**



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

לשימוש המשק: שפה + פלטפורמה + מוסמכים



דו"חות דשבורדים עדרים משלימים שאלות נפוצות צור קשר

4 סיכום הפערים רמת סיכון לנכס מיפוי הנכסים פרטי החברה

סיכום הפערים 1-20 of 36

סטטוס הבקרה ביחס לנכסים

פער חלקי יש פער אין פער לא נבחר

כמות בקרות עם פערים 13

#	הבקרה	סטטוס	תיאור הפער
1	יש לוודא יתירות שירותים ותשתיות קריטיות	יש פער	לא מתקיים בארגון
2	יש לכתוב וליישם מדיניות תגובה לאירועים, לבקר ולעדכן אותה תקופתית	יש פער	קיימת מדיניות עדכנית לשנת 2016 שיש לתקף
3	יש לכתוב וליישם מדיניות המשכיות עסקית, לבקר ולעדכן אותה תקופתית	אין פער	
4	יש לבצע תכנון הקיבולת הנחוצה למקרה אסון	אין פער	
5	יש ליצור גיבוי לרשתות תקשורת ולוודא קיום שירותי תקשורת חלופיים	אין פער	
6	יש לוודא מוכנות של אתר העיבוד החלופי לעבודה כאתר המבצעי ובתמיכה במשימות חיוניות	אין פער	
7	יש לוודא יכולת לשחזור רכיבי מערכת למצב מבצעי ידוע	פער חלקי	מתקיימת באופן חלקי SQL בשרת



נושאים לבדיקה "בתוך הבית"

- מהם הנכסים הרגישים ביותר עבורכם?
- האם ההנהלה אישרה את מפת הסיכונים?

Identify

- כיצד מוודאים מיצוי שימוש בכלים קיימים?
- האם הכלים תומכים את מפת הסיכונים ואת הנכסים הקריטיים?

Protect

- אילו כלי איתור קיימים בארגון?
- מהו שיעור התראות השווא בארגון?

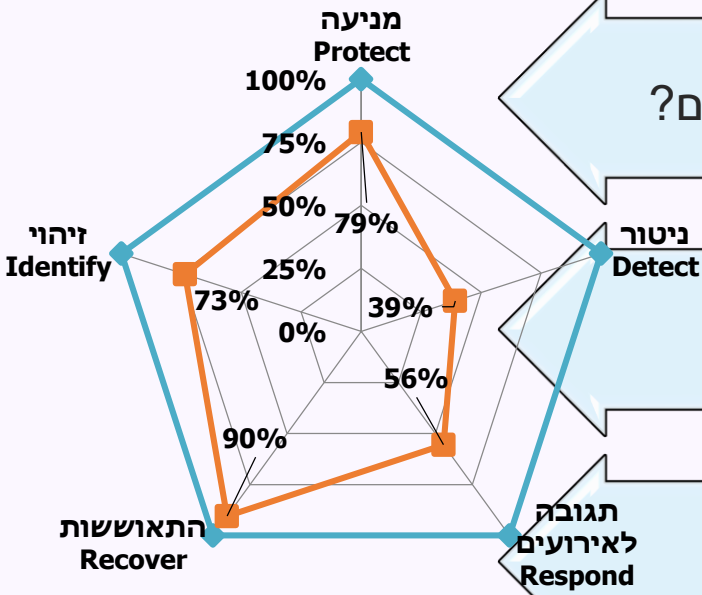
Detect

- האם ישנו חוזה התקשרות למקרי חירום/צוותי התערבות?
- האם צוות התגובה כולל בעל עניין מורחבים?

Respond

- מהם התהליכים העסקיים שאינם חלק מתכנית ה-DR?

Recover



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

שנת 2018 – האתגר

העלאת החוסן בארגונים באמצעות העמקה והטמעת תוה"ג

רתימה באמצעות הסרת חסמים (מיכון, תאימות לתקנים, עזרים, ערך מוסף חדש) + פעילות מגזרית

חיזוק באמצעות ידע "מתקדם" (כתיבת מסמכי BP's ודפ"אות)

אימוץ חלקי/אי ההגנה במודע אימוץ תורת

ההגנה (יודע ועושה) אימוץ תורת

אימוץ מחוסר היכרות/ידע

רתימה באמצעות כנסים, פורומים, הנגשה ועוד

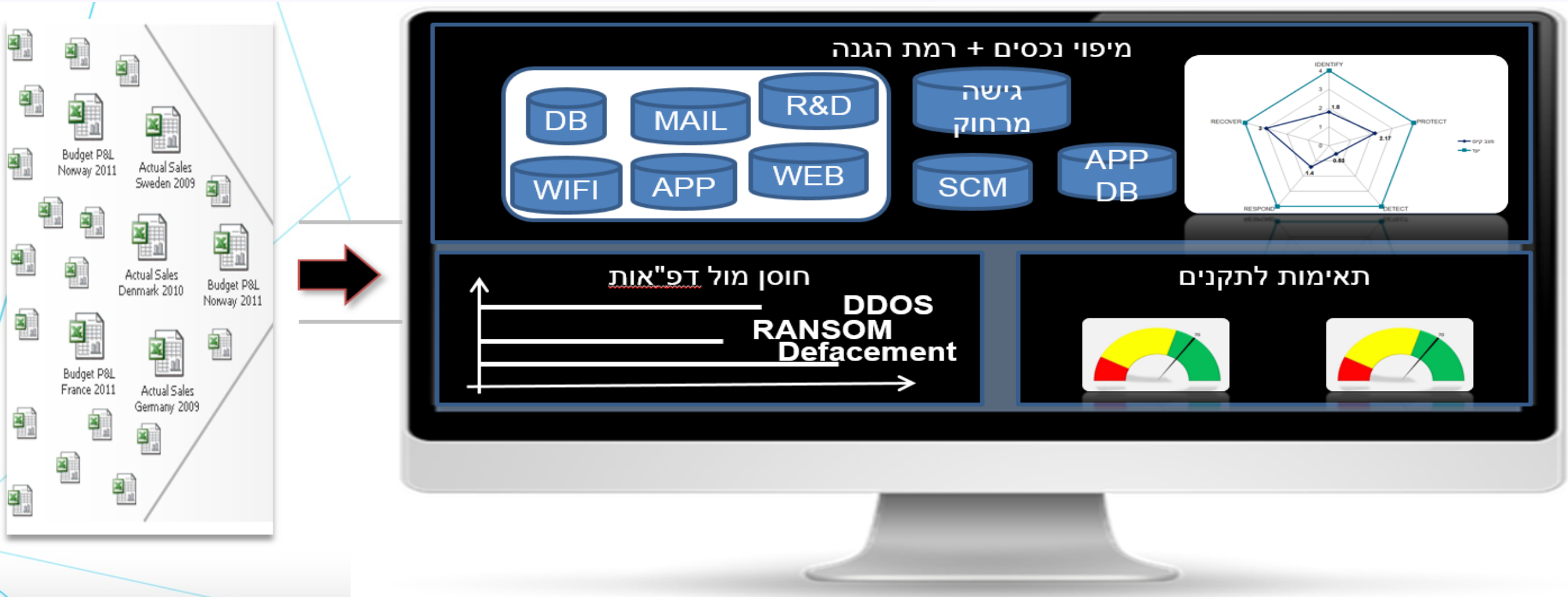
2018



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

2019 – הערכת מצב ובנוצ'מרק בפשטות ובחינם



סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

1. להוסיף לתכנית הביקורת את נושא שרשרת האספקה (שפה/מערכת/רמת הסוקר)
2. לא לעבוד מהבטן – יש מסמך מקיף שהותאם למשק הישראלי
3. היכנסו למערכת יוב"ל – קבלת תמונת מצב מזוויות שונות
4. לא לשכוח בתכנית העבודה לבחון יכולת איתור ותגובה
5. התחילו עם ה KRI's ובצעו העמקה/התאמה לצרכים שלכם
6. מערך הסייבר זמין וישמח לסייע – Team@cert.gov.il



יובל שגב

ראש מחלקת מתודולוגיה

yuvals@cyber.gov.il

050:8885732

**מחלקת מתודולוגיה
מפתחים מתודה לאומית בסייבר**