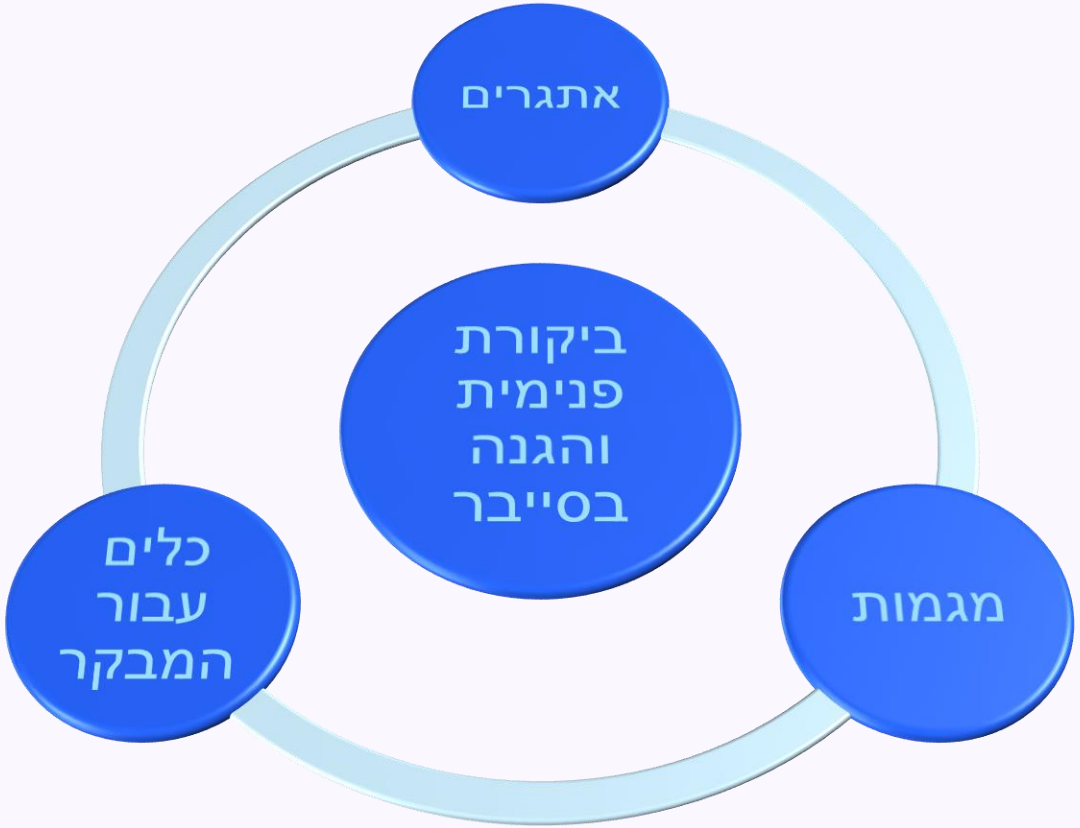
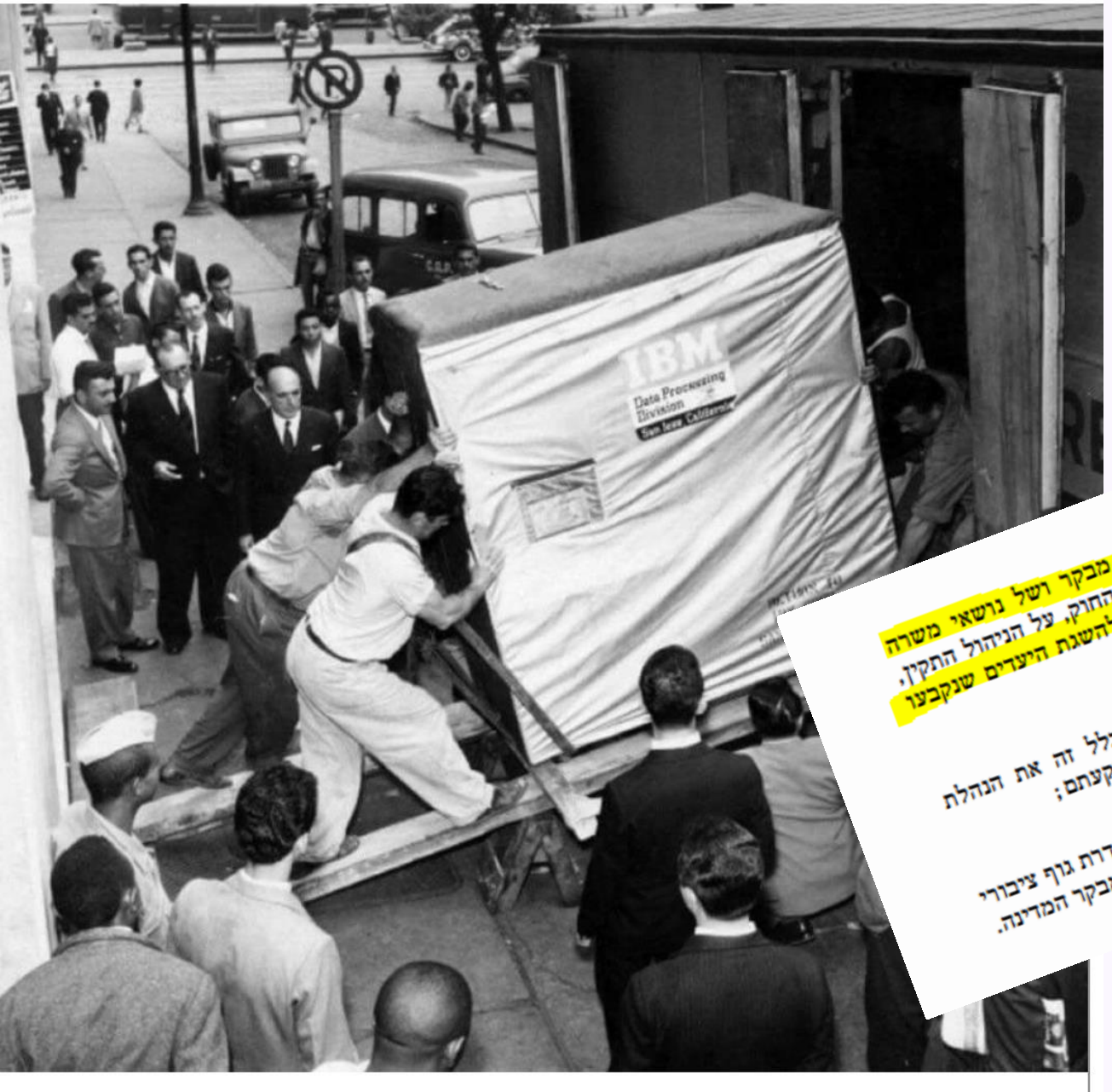
סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי



יובל שגב
ראש מחלקת מתודולוגיה
מערך הסייבר הלאומי
ינואר 2019

5 ,1956 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 רשל 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 יערך את הביקורת על פי תקנים מקצועיים מקובלים.

"בסייבר, זה אחרת"

שליחת
מייל/פקס
לכתובת שגויה
רכיב הזיכרון
שבמדפסת
המדפסת
כחיבור לרשת
חיבור USB
כניסת וירוס דרך
עדכון תוכנה
נתיב להוצאת
מידע מהארגון
הטמנה בחומרה/
תוכנה

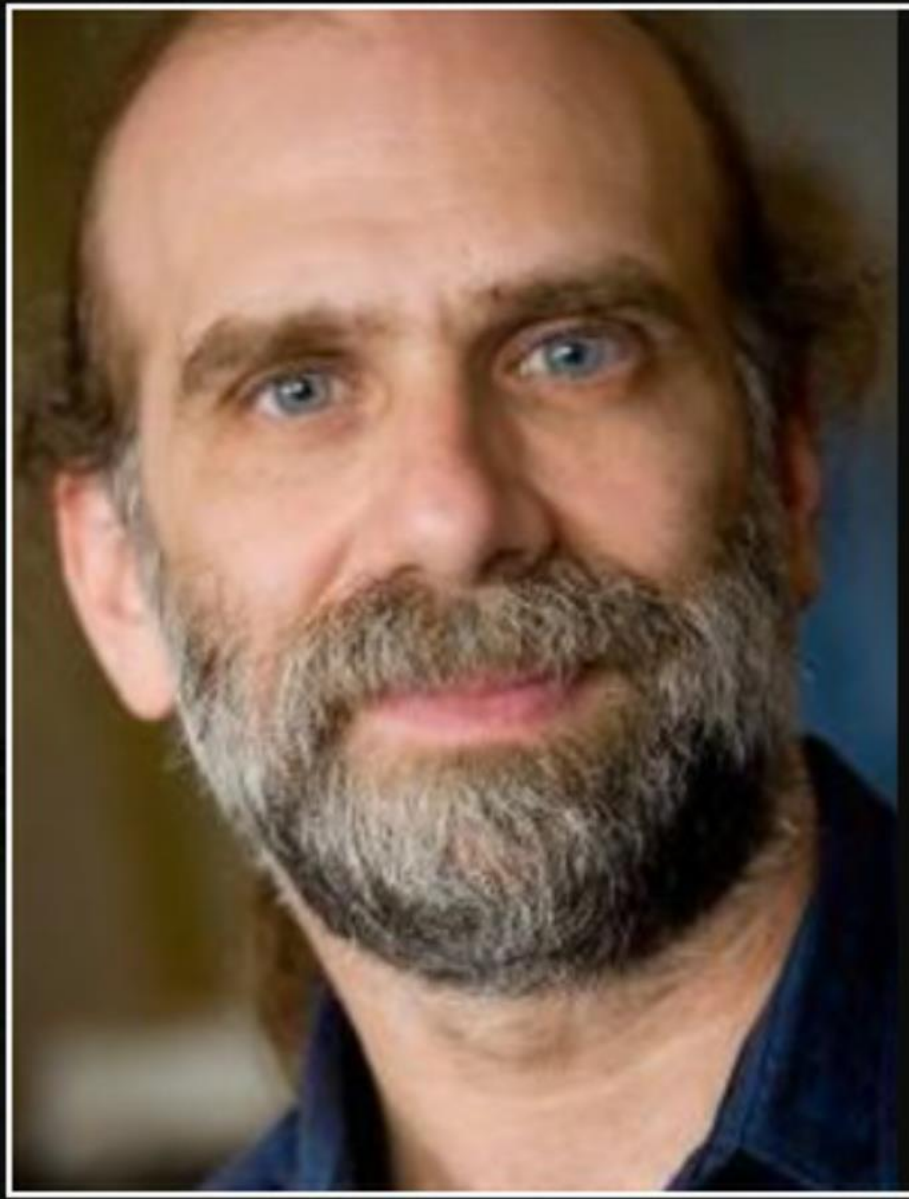
YAHOO!
<AFTERHOURS>
39.95
2.35%
Bloomberg
WHO IS RESPONSIBLE FOR YAHOO BREACH
Bloomberg

97% מאירועי הרשת נגרמים כתוצאה מ - Misconfigurations

88% מהמתקפות הידועות יכולות להימנע באמצעות מימוש 20 "בקרות אב"

50% הציון הממוצע של גופי Enterprise שנבדקו בהיבטי יכולות Detect & Respond

6-8% מתקציב IT מושקע בסייבר.
תקציב IT נגזר לרוב מהמחזור.



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

גברים ממאדים נשים מנוגה גרסת עולם ה Security

NAC

לוגים

SIEM

DLP

SSDLC

IPS

MDM

EDR

הקשחה

פאצ'ים

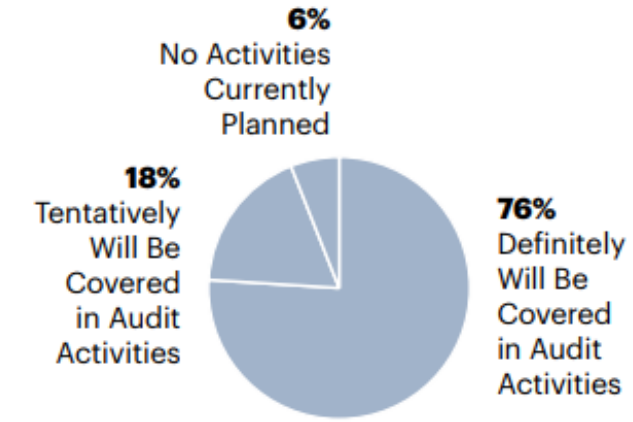
PIM

2019 Audit Plan Hot Spots Report Excerpt

Five Risk Areas to Watch

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

Percentage of Respondents

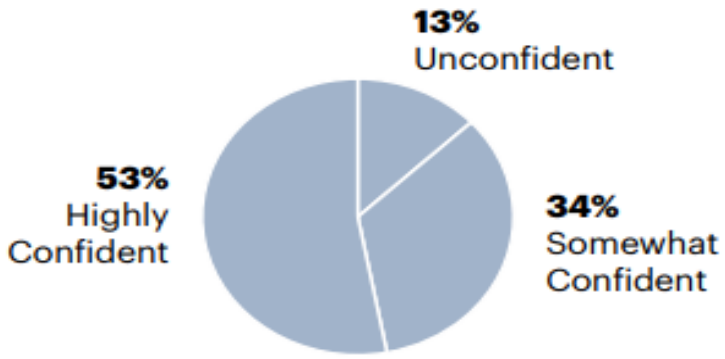


n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

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

Percentage of Respondents

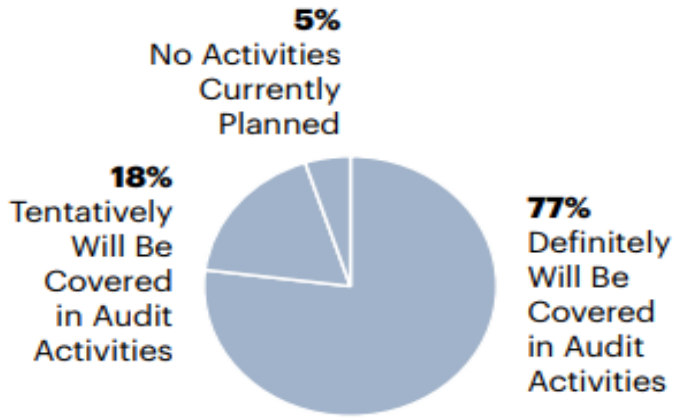


n = 143

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

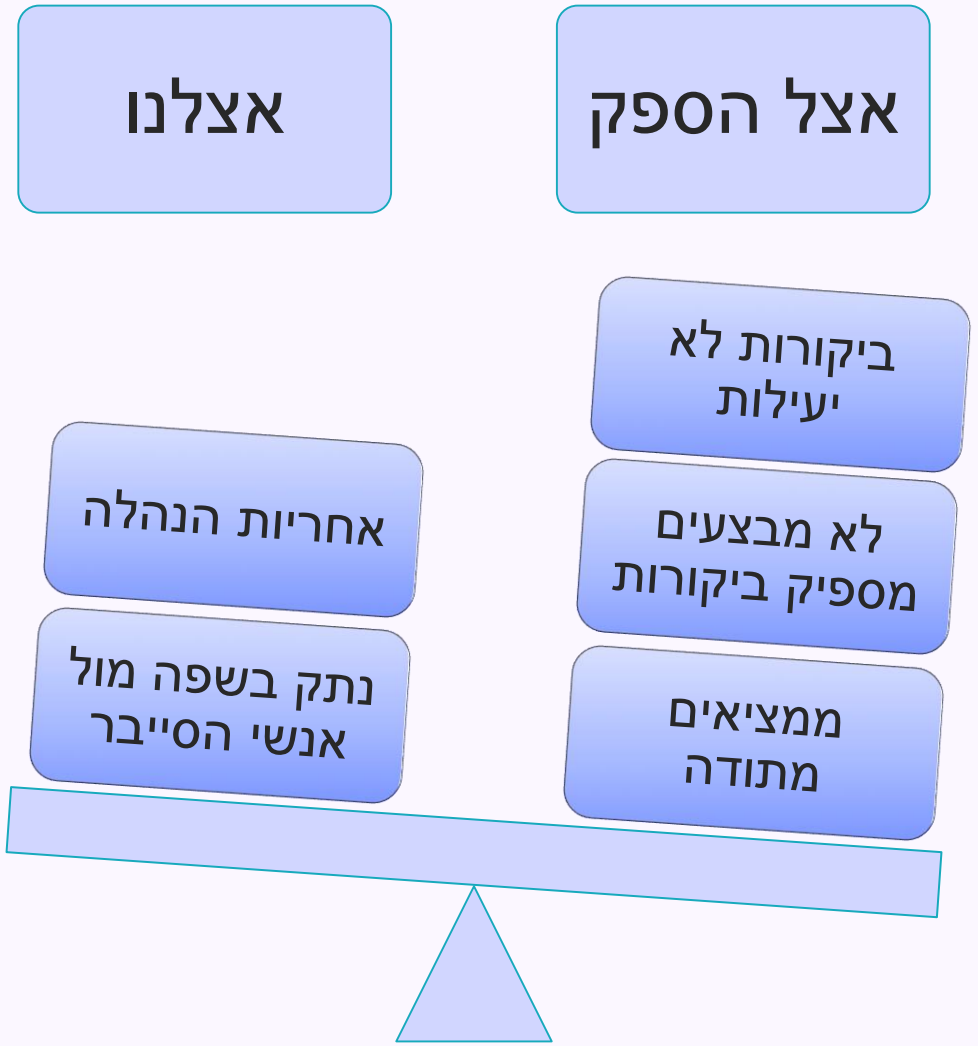


n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Gartner

חלוקת האתגרים

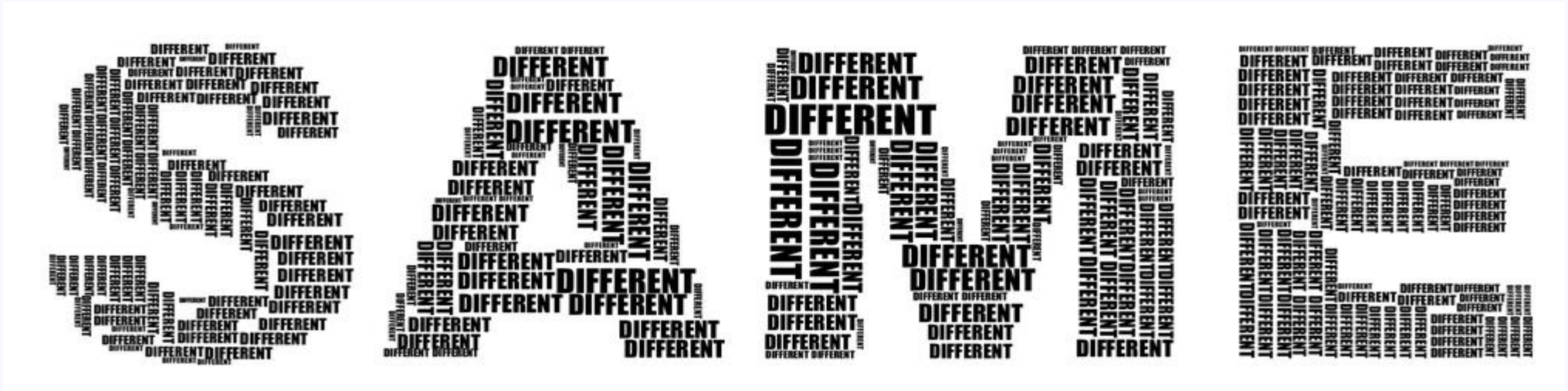


שרשרת אספקה
מחזקים את החוליה החלשה בשרשרת
דברים שלמדתי בקבוצת המיקוד

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



Ports

MEMEPIX.COM

דרישות
הגנה
מהספק
ארגון X
גישה מרחוק
תו"ל רימון
הסרת
משתמשים
בסיום העסקה
תקנות הגנת
הפרטיות
ניהול פאצ'ים
תוה"ג
חומת אש
ניטור
פיתוח מאובטח
27001
ליווי
הצפנת קבצים

ואיך זה נראה בעיני הספק?

远程访问

Rimon方法论

完成后删除
用户

保护隐私条
例

管理修补程序

组织防御理论

火墙

监控

确保发展

27001

陪伴供应商

加密文件

10%

כמות הספקים "הרגישים"
מתוך סך הספקים

15,000 – 5,000

כמות הספקים שיש
לארגון אנטרפרייז

2-20 שעות

משך הזמן שמוקצה
לבדיקת ספק

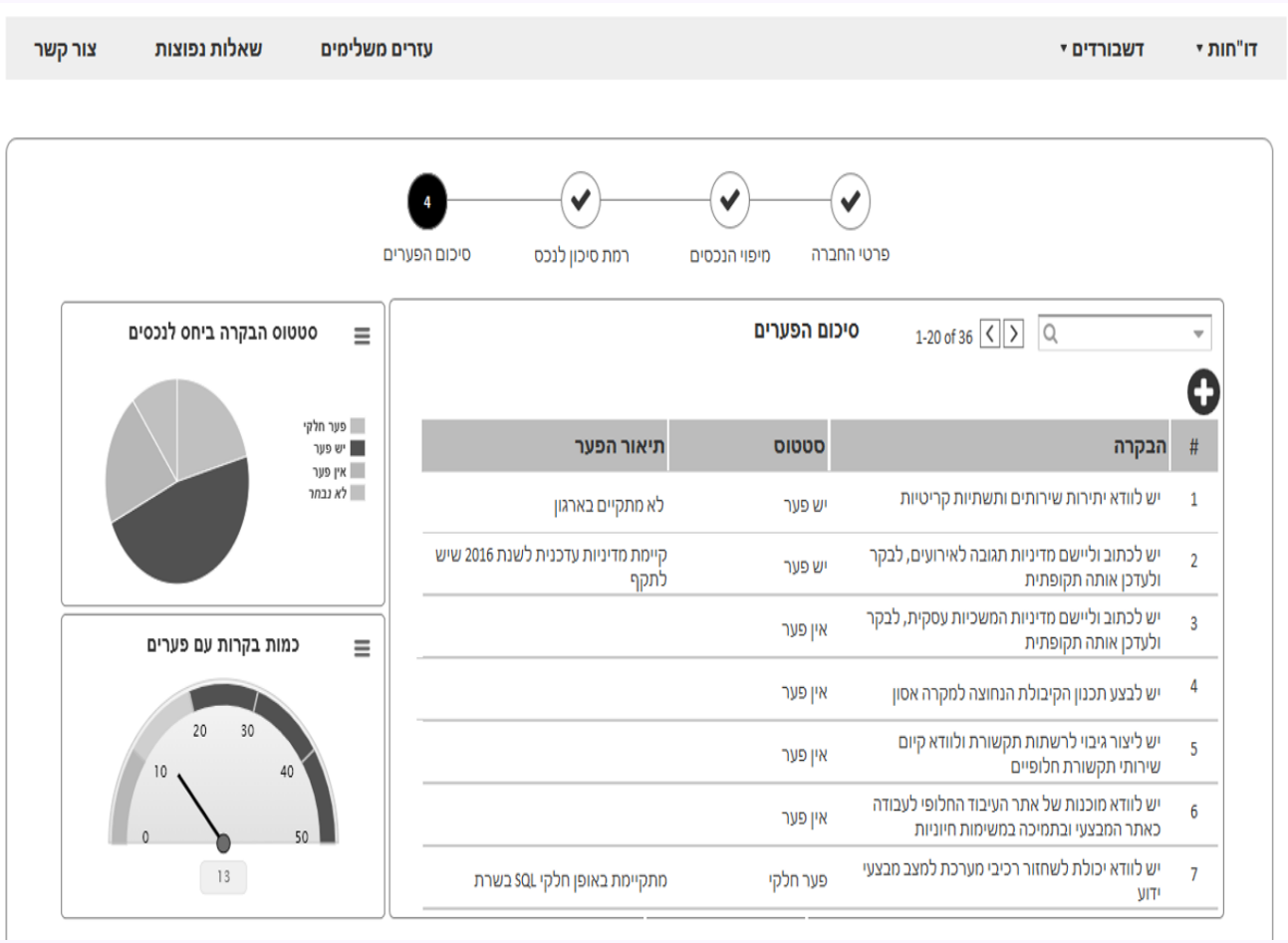
פחות מ – 1%

מספר הארגונים
שמקצים FTE לנושא

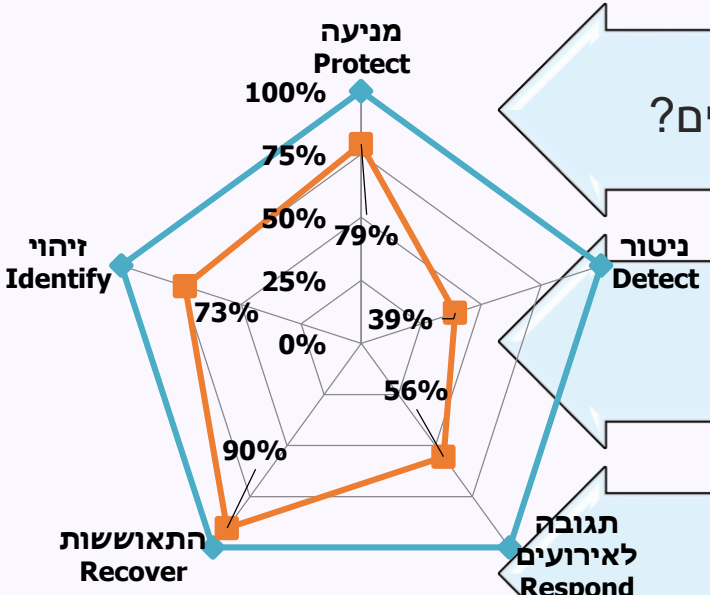
2%

היכולת של ארגון לבצע ביקורת
בחצרות הספק

לשימוש המשק: שפה + פלטפורמה + מוסמכים



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

שנת 2017 - האתגר

כיצד ראוי להגן על ארגון בישראל?

שנת 2018 – האתגר

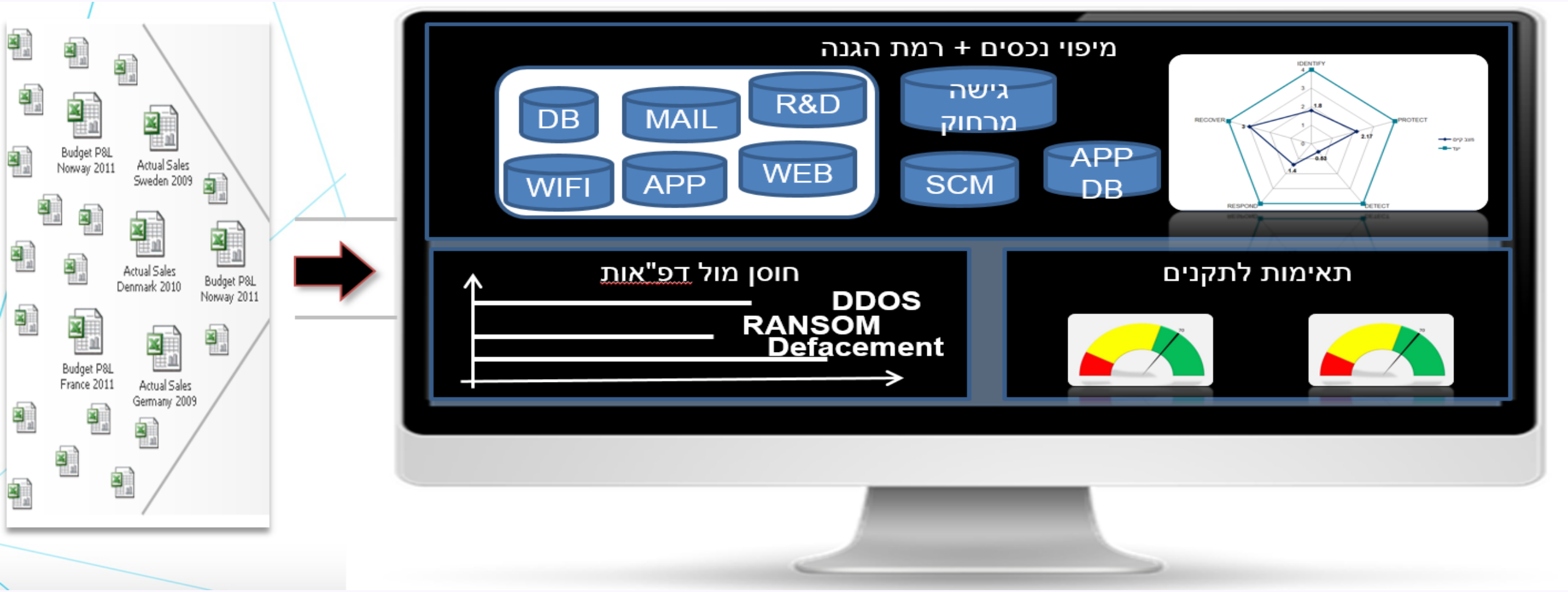
העלאת החוסן בארגונים באמצעות העמקה והטמעת תוה"ג

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

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

רתימה באמצעות כנסים, פורומים, הנגשה ועוד

2019 – הערכת מצב ובנצ'מרק בפשטות ובחינם



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

משרד ראש הממשלה
מערך הסייבר הלאומי
יובל שגב
ראש מחלקת מתודולוגיה
yuvals@cyber.gov.il
050:8885732
מחלקת מתודולוגיה
מפתחים מתודה לאומית בסייבר