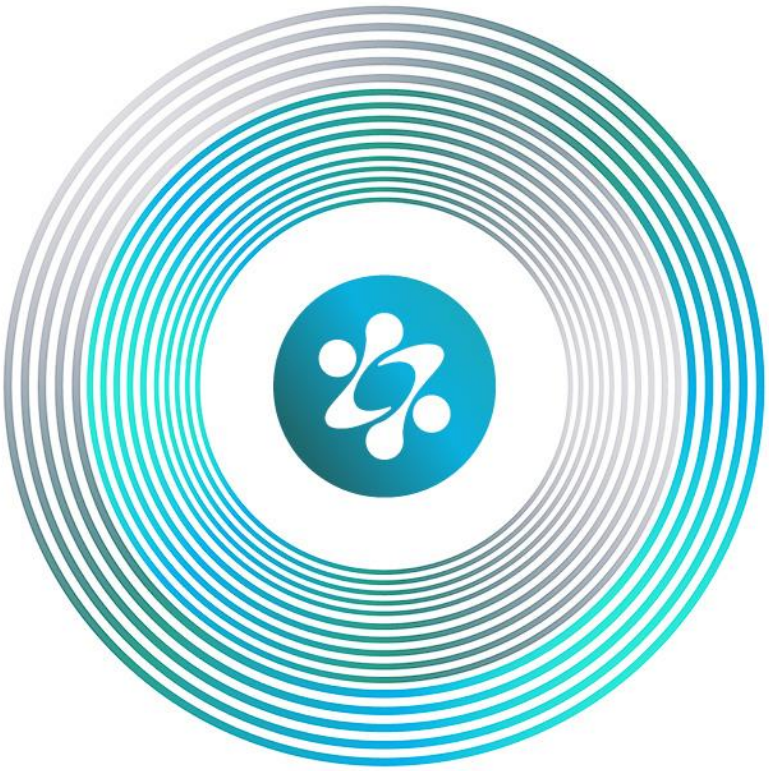


הערכת העלות הכלכלית בגין תקיפות סייבר בישראל

אפריל 2024

שלמה צרפתי, כלכלן ראשי

אלדד שקד, יועץ כלכלי בכיר

מערך הסייבר הלאומי

תוכן עניינים

תקציר מנהלים

1. מערך הסייבר הלאומי רואה חשיבות גדולה לתחום כלכלת הסייבר, והוא כולל בהחלטות השונות שלו את השיקול הכלכלי, מתוך ההבנה שהגנת סייבר בת קיימה תלויה בשקלול המשמעויות הכלכליות הן ברמת המאקרו (מדינה) והן ברמת המיקרו (ארגון עסקי/ממשלתי).
2. בימים אלו מגבש מערך הסייבר צעדי מדיניות נוספים להגברת ההגנה בסייבר, הן בתחום האסדרה (חוק הסייבר) והן ביצירת תמריצים כלכליים לארגונים, כך שניתוח עלות-תועלת הוא משמעותי לתהליך קבלת ההחלטות בנושאים אלו.
3. במסמך זה מבוצעת סקירה בינלאומית של מחקרים, מאמרים ונתונים העוסקים בעלות הכלכלית הנגרמת מתקיפות סייבר והתועלת בהגברת ההגנה.
4. על בסיס ממצאי הסקירה בוצעה הערכה לעלות הכלכלית הנגרמת מתקיפות סייבר בישראל בשנה. הערכה זאת בוצעה בשתי שיטות שונות - top-down ו־bottom-up - על מנת לבסס את הממצאים.
5. הממצאים מראים כי עלות תקיפות סייבר בישראל מוערכת בסכום של כ־**12 מיליארד ₪ בשנה.** ללא מענה הגנתי הולם, עלויות אלו צפויות להמשיך ולגדול מדי שנה במהלך השנים הקרובות עם ההתפתחות הטכנולוגית בכל תחומי החיים והגידול הצפוי בכמות המתקפות ובאיכותן.
6. מחקרים שבוצעו בשנים האחרונות הצביעו על כך שניתן להפחית עלויות אלו באמצעות הגברת ההגנה במרחב הסייבר (בעלות נמוכה יחסית למול הנזק הפוטנציאלי), היות שהיא תורמת לירידה בעלות הממוצעת הנגרמת מתקיפה וכן בהסתברות לתקיפה.
7. בהתאם לכך, מערך הסייבר הלאומי פועל למען הגברת ההגנה במרחב הסייבר האזרחי, ומביא לתועלות כלכליות למשק ולעסקים. צעדים אלו כוללים: הגנה אקטיבית והנחיית גופים קריטיים, מדיניות, ניטור שוטף, הגברת המודעות, התרעות למשק ועוד.
8. ניתוח כלכלי בתחום הסייבר הוא תחום מורכב ממגוון סיבות כפי שיפורט בהמשך, ואחת המרכזיות בהן היא חוסר בנתונים ובמדידה. לפיכך אנו ממליצים על ביצוע

סקרים סדורים להערכת רמת ההגנה בארגונים וכן מדידת כמות מקרי תקיפות הסייבר בישראל ואיכותם.

1. כללי

1.1. מערך הסייבר הלאומי רואה חשיבות גדולה לתחום כלכלת הסייבר וכולל בהחלטות השונות של המערך את השיקול הכלכלי, מתוך ההבנה שהגנת סייבר בת קיימה תלויה בשקלול המשמעויות הכלכליות הן ברמת המאקרו (מדינה) והן ברמת המיקרו (ארגון עסקי/ממשלתי).

1.2. ההערכות והאומדנים מבוססים על מחקרים ודוחות מעודכנים ועל שיטות העבודה המקובלות בעולם בתחום, אשר תומכים בצעדי המדיניות להעלאת רמת ההגנה.

1.3. יש לציין שניתוח כלכלי בתחום הסייבר הוא תחום מורכב ממגוון סיבות, כגון: חוסר בנתונים עקב דיווח נמוך (תמריץ עסקי שלילי לחברות לשתף מידע בנוגע למתקפות); מידע פרטי; אתגר ייחוס התוקף; מגוון רחב של עלויות ישירות ועקיפות; השפעות קצרות טווח וארוכות טווח; גיוון האיומים; הטרוגניות הנתונים ומדדים מגוונים להשפעה.

2. מטרה

ביצוע הערכה להיקף העלויות השנתיות למדינת ישראל כתוצאה ממתקפות סייבר, לטובת ביצוע ניתוחי עלות-תועלת ולתמיכה בקבלת ההחלטות במערך הסייבר הלאומי.

3. מתודולוגיה והנחות עבודה

3.1. מתודולוגיה

3.1.1. מטרתו הראשית של המתכנן המרכזי בישראל בתחום הגנת הסייבר (ממשלת ישראל ומערך הסייבר הלאומי) היא העלאת רמת ההגנה במרחב הסייבר למול האיומים, בשקלול העלות הכלכלית של ההגנה ברמת תקציב המדינה וברמת תקציב הארגונים והאזרחים.

3.1.2. להלן בעיית "המתכנן המרכזי" (הממשלה) בהצגה אלגברית מופשטת:

$$\textbf{Min } D = P(t)*Q(t) + C(t)$$

D - סך העלות הכלכלית השנתית הנובעת מנזקי מתקפות סייבר במדינת ישראל בתוספת העלות הנובעת מצעדי המדיניות להעלאת רמת ההגנה;

t - הצעדים (מדיניות, טכנולוגיה) שמבצע המתכנן המרכזי להעלאת רמת ההגנה בסייבר במדינת ישראל;

P(t) - עלות תקיפה ממוצעת התלוי ב־t;

Q(t) - כמות המתקפות השנתיות התלוי ב־t;

C(t) - סך העלויות ברמת המאקרו למדינה ועלויות ברמת המיקרו לארגונים כתוצאה מצעדי המדיניות הנדרשים להעלאת רמת ההגנה (כוח אדם, רכש ציוד, רישיונות וכו').

3.1.3. משתנה ההחלטה של המתכנן המרכזי הוא הצעדים שהוא מחיל על המשק, לדוגמה: חקיקה מחייבת; פתרונות טכנולוגיים ממשלתיים; סבסוד הגנה; תמריצים כספיים; קמפיינים להעלאת מודעות; הטבות מיסוי ועוד.

3.1.4. על מנת להביא למינימום את הנזקים והעלויות הנובעים מצעדי המדיניות, על המתכנן המרכזי להבין את הפרמטרים המשפיעים: העלות הכלכלית הקיימת הנובעת מנזקי תקיפות סייבר (P*Q) והעלויות הכרוכות מהעלאת רמת ההגנה (C).

3.1.5. מסמך זה יעסוק בעיקר בהערכת העלות הכלכלית הנוכחית הנובעת מנזקי תקיפות סייבר (P*Q) ויתייחס באופן כללי למשתנים האחרים.

3.1.6. קיימות תועלות נוספות מהעלאת רמת ההגנה ובהן אמון דיגיטלי, חיי אדם וכו'. תועלות אלו לא יפורטו במסמך זה.

3.2. הנחות עבודה

3.2.1. נתונים ופרמטרים לצורך החישוב מבוססים על מחקרים ודוחות מובילים שפורסמו בשנים האחרונות על ידי גורמים ממשלתיים, מכוני מחקר וחברות אבטחת מידע.

3.2.2. ההערכות לגבי היקף העלויות הנגרמות מתקיפות סייבר מתייחסות בדרך כלל לפשעי סייבר (cybercrimes). משרד המשפטים האמריקאי הגדיר וחילק את פשעי הסייבר לשלוש קטגוריות: פשעים כנגד ציוד מחשוב (גישה לרשת); פשעים שהמחשב משמש בהם "כלי נשק" (לדוגמה: מתקפת DDOS) ופשעים שהמחשב משמש בהם כלי עזר לפשע (לדוגמה: שמירה של מידע לא חוקי).[1]

[1] Kim, C. (2012). Computer crimes. *American Criminal Law Review, 49*(2), 443–488. https://law-journals-books.vlex.com/vid/computer-crimes-411848950

3.2.3. הערכות אלו אינן כוללות בהכרח עלויות כתוצאה מפעולות טרור או ממניעים אידאולוגיים. מכיוון שלא ניתן להעריך את היקף העלויות שלא נכללות במסגרת cybercrime, מטעמי שמרנות נתייחס להערכות עלויות ה־cybercrime כאל העלויות המלאות.

3.2.4. את העלויות הנובעות מתקיפות סייבר ניתן לסווג לשתי קטגוריות:[2]

עלויות ישירות - לדוגמה: תשלומים לצוות תגובה ראשוני; שירותי ייעוץ; הודעה ללקוחות; ייעוץ משפטי; הפסד כספי כתוצאה מהשבתת העסק או אובדן הפסד כספי כחלק ממאמצי שחזור נתונים; תיקון או החלפה של ציוד שנפגע ואובדן נכסים בלתי מוחשיים.

עלויות עקיפות - לדוגמה: אובדן הכנסות עתידיות; אובדן הזדמנויות עסקיות; פגיעה במוניטין; עלויות ביטוח; תביעות בגין נזקים שנגרמו לצד שלישי; השקעות נוספות בכלי אבטחה ("הגבהת החומות"); פגיעה באמון משקיעים זרים.

3.3. מתודולוגיה לחישוב אומדן להיקף עלויות בגין תקיפות הסייבר במדינת ישראל

על מנת להגביר את מהימנות המסמך לאור מורכבות הניתוח הכלכלי בתחום כפי שהוסבר לעיל, הערכת העלויות בגין תקיפות סייבר במדינת ישראל תבוצע בשתי שיטות העבודה שלהלן:

top-down - שימוש בנתוני עלויות בגין תקיפות סייבר גלובליות ממחקרים בעולם, והתאמתם לישראל בהתאם לחלקה של ישראל בכלכלת העולם;

bottom-up - חישוב העלויות בגין תקיפות סייבר, בהתאם למכפלת מספר מקרי הסייבר בישראל והעלות הממוצעת למקרה תקיפה ממוצע.

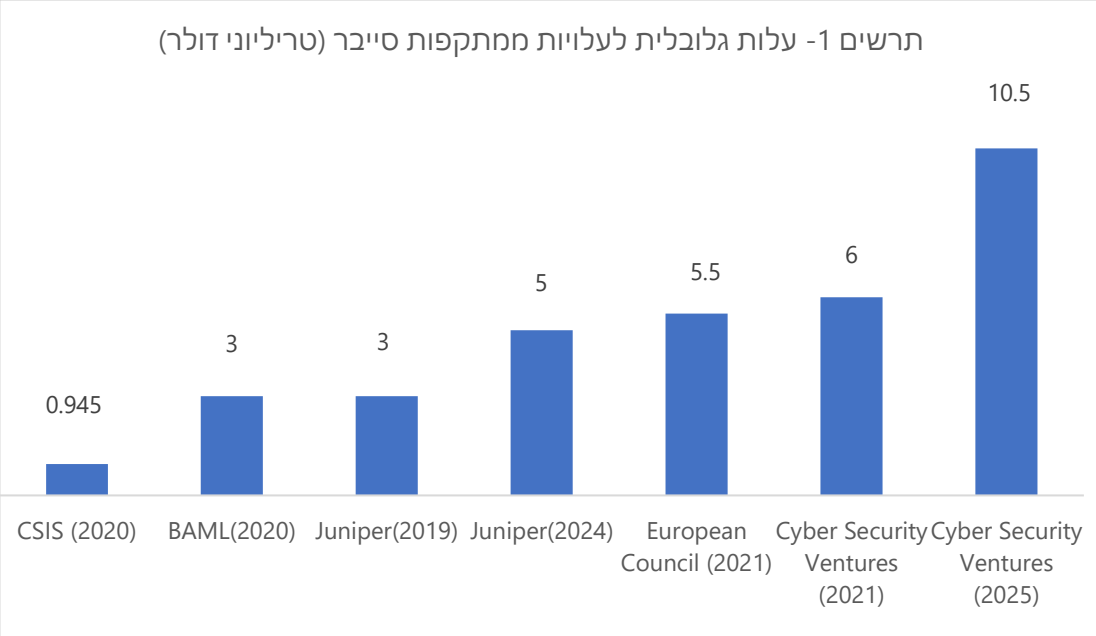
[2] Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economic and Business Review, 5(2), 24–47.https://dx.doi.org/10.18559/ebr.2019.2.2

4. ניתוח top-down

4.1. הערכת העלות העולמית בגין פשיעת סייבר

4.1.1. בשנים האחרונות בוצעו מחקרים והערכות לעלויות העולמיות הנגרמות ממתקפות סייבר. ההערכות בוצעו על ידי מוסדות ממשלתיים, מכוני מחקר, חברות אבטחת מידע וגופים כלכליים נוספים.

4.1.2. להלן גרף המתאר את הערכת העלויות הגלובליות השנתיות מתקיפות סייבר בהתאם למחקרים השונים, כפי שיפורטו בהמשך (השנה בסוגריים היא השנה האחרונה שהערכת העלות של כל מחקר מתייחסת אליה):



4.1.3. כפי שניתן לראות בתרשים 1, הערכת העלות השנתית הגלובלית בגין תקיפות סייבר נעה **בין כטריליון לשישה טריליון דולר** עבור השנים 2020–2021, כאשר בשנת 2025 הצפי הוא שהעלות תעלה מעל עשרה טריליון דולר.

4.2. מחקרים בשיטת top-down

4.2.1. במחקר שפורסם על ידי CSIS[3] בשנת 2018[4] ונערך בשיתוף חברת אבטחת המידע McAfee הוצג ניתוח של העלות בגין תקיפות סייבר בעולם כאחוז מהתוצר המקומי הגולמי (להלן: תמ"ג - GDP).[5] המחקר הציג כי בשנת 2017 העלות כתוצאה מתקיפות סייבר הוערכה ב־0.8% מהתוצר העולמי. במחקר שערך המכון בשנת 2020, גם כן בשיתוף McAfee,[6] הוערכה העלות בגין תקיפות הסייבר בעולם ב־945 מיליארד דולר - כ־1.1% מהתוצר העולמי.[7]

4.2.2. במחקר שפורסם על ידי המכון הלאומי לתקנים וטכנולוגיה במחלקת המסחר האמריקאית (NIST),[8] הוערכה העלות בגין תקיפות סייבר בארה"ב בשנת 2016 בין 0.9% ל־4% תוצר. אחוזים אלו גבוהים מההערכה במחקר של CSIS.

4.2.3. חברת המחקר Cybersecurity Ventures[9] העריכה את העלות בגין תקיפות סייבר בשישה טריליון דולר עבור שנת 2021, כאשר הצפי שעלויות אלו יאמירו ליותר מעשרה טריליון דולר עד שנת 2025.[10]

4.2.4. האיחוד האירופי העריך את העלות הגלובלית בגין תקיפות סייבר ב־5.5 טריליון דולר בסוף שנת 2020.[11]

---

[3] Center Of Strategic and International Studies - מכון מחקר מוביל בארצות הברית שהוקם ב־1987. המכון דורג ראשון על ידי אוניברסיטת פנסילבניה בכלל התחומים בארצות הברית ומקום ראשון בעולם בתחום מדיניות ביטחון וביטחון לאומי.

[4] המחקר המעודכן ביותר אשר הציג את רמת הפירוט הגבוהה ביותר הכוללת חתכים שונים שעליהם התבססנו בהמשך.

[5] Lewis, James (2018, February). Economic impact of cybercrime – No slowing down. CSIS & McAfee. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[6] Malekos Smith, Z., & Lostri, E. (2020). The hidden costs of cybercrime. McAfee.https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf

[7] לפי נתוני הבנק העולמי לשנת 2020: GDP עולמי - 85.26 טריליון דולר.

[8] Thomas, Douglas (2020). Cybercrime losses: An examination of U.S. manufacturing and the total economy. National Institute of Standards and Technology. https://www.nist.gov/publications/cybercrime-losses-examination-us-manufacturing-and-total-economy

[9] חברה העוסקת במחקר בתחום הסייבר. החברה מציגה עצמה כחברת מחקר עצמאית, והכנסותיה מפרסום באתר ובפרסומים שלה.

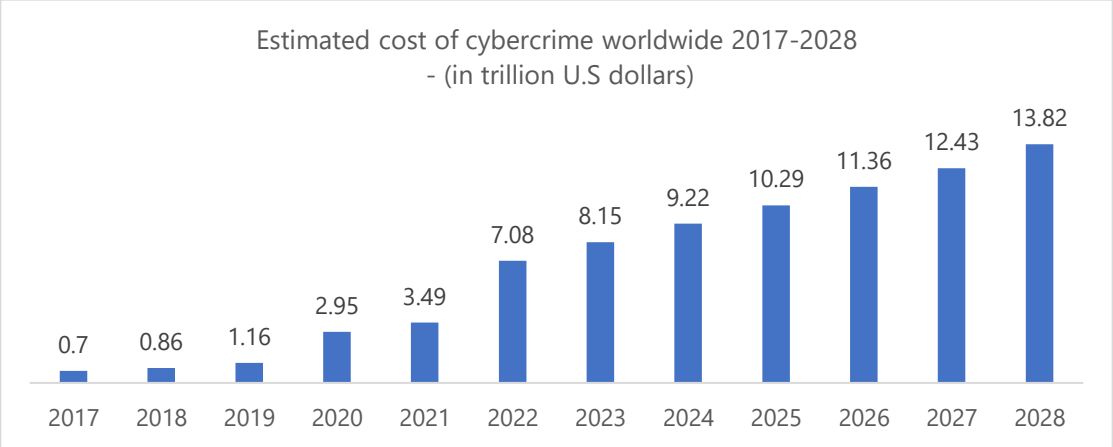
[10] Cybercrime To Cost the World $10.5 Trillion Annually By 2025

[11] A cybersecure digital transformation in a complex threat environment — Brochure

4.2.5. חברת אבטחת המידע Juniper העריכה ב-2019 את העלות הגלובלית מתקיפות סייבר בשלושה טריליון דולר, כאשר עלויות ממתקפות סייבר צפויות להגיע לחמישה טריליון דולר בשנת 2024.[12]

4.2.6. בנק אמריקה ו'מריל לינץ'' העריכו כי העלות העולמית כתוצאה מתקיפות הסייבר בעולם בשנת 2020 תסתכם בשלושה טריליון דולר.[13]

4.2.7. בנוסף לכך, חברת Statista העוסקת בחקר נתונים והצגתם העריכה כי בשנים 2023–2028, העלות העולמית כתוצאה ממתקפות סייבר תגדל כל שנה בכ־10%, ותסתכם ב־13.82 טריליון דולר בשנת 2028.[14]



4.2.8. יצוין כי שיטת החישוב האגרגטיבית הננקטת במחקרים בשיטה זו לוקה במספר חסרונות: שונות גבוהה בין הממצאים, חלק מן ההנחות אינן מבוססות ברמה אמפירית ומושפעות מאינטרסים כלכליים של ממני המחקר. לאור זאת, בחרנו להשתמש בנתונים השמרניים ביותר של שיטה זו, כפי שיתואר בהמשך.

4.3. הערכת העלות בגין תקיפות הסייבר בישראל בשיטת top-down

בתת־פרק זה הערכת העלות השנתית ממתקפות סייבר בישראל מבוססת על מחקרים שבוצעו על ידי מכון המחקר CSIS, שכן ממצאי מחקרים אלו הם השמרניים ביותר ביחס לאחרים ויהוו כחסם תחתון (כפי שניתן לראות בתרשים 1).

[12] Global Breach Costs Set to Top $5 Trillion By 2024
[15] You've Been Hacked! - Global Cybersecurity Primer
[14] Estimated cost of cybercrime worldwide 2017-2028

4.3.1. החוקרים העריכו את העלות כתוצאה מתקיפות סייבר בשנת 2017 בכ־0.8% מהתוצר העולמי והעלויות הוצגו במספר חתכים במחקר לשנה זו:

- <u>חלוקת המדינות בהתאם לרמת ההגנה בסייבר</u> - רמת ההגנה בסייבר נמדדה בהתאם למדד GCI.[15] המדינות חולקו לשלוש קטגוריות: מדינות מובילות (GCI גבוה מ־70); מדינות מתבגרות (GCI בין 30 ל־70); ומדינות בשלב ראשוני (GCI נמוך מ־30). ציון ה־GCI של ישראל הוא 90.93,[16] ולכן מדינת ישראל מסווגת כמדינה מובילה בהגנת הסייבר. בהתאם לכך, המחקר הציג כי העלויות כתוצאה מתקיפות סייבר במדינה מובילה הוא בסדר גודל של כ־0.41%[17] מהתוצר.
- <u>חלוקת המדינות בהתאם לרמת התוצר לנפש</u> - המדינות חולקו לארבע קבוצות בהתאם לרמת התוצר לנפש. הקבוצה הראשונה כללה מדינות מעל תוצר לנפש של 12,236 דולר. במדינת ישראל התוצר לנפש בשנת 2017 עמד על 41,115 דולר[18] והיא נכללה בקבוצה זו. בהתאם לכך, אחוז העלויות בגין תקיפות סייבר מהתוצר הממוצע למדינה בעלת רמת תוצר לנפש גבוהה הוא 0.505%[19] מהתוצר.

4.3.2. בהתאם לאמור לעיל, לצורך הערכת העלות בגין תקיפות הסייבר בישראל הנחנו כי אחוז עלויות ממתקפות סייבר מהתוצר המקומי של מאפייני מדינה כישראל הוא כ־0.46% מהתוצר (ממוצע של שני הסעיפים שלעיל).

4.3.3. כמפורט לעיל, במחקר מעודכן של המכון (ללא פירוט לחתכים) לשנת 2020 הוערכה העלות העולמית בגין תקיפות סייבר בעולם בכ־1.1% מהתוצר העולמי.[20] הגידול מ־0.8% תוצר ל־1.1% תוצר, מהווה גידול של כ־37% באחוז העלות בגין תקיפות סייבר מהתוצר.

---

[15] The Global Cybersecurity Index (GCI) - מדד שהחל להימדד בשנת 2015 על ידי איגוד התקשורת הבינלאומי (ITU), ומודד את מידת המחויבות של 193 מדינות לאבטחת מידע בסייבר. המדד בוחן היבטי משפט, טכנולוגיה, ארגוניים, פיתוח ושיתוף פעולה.

[16] Global Cybersecurity Index 2020

[17] ממוצע בנטרול חריגים - %GDP (excluding outliers)

[18] https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=IL

[19] ממוצע בנטרול חריגים - %GDP (excluding outliers)

[20] לפי נתוני הבנק העולמי לשנת 2020: GDP עולמי - 85.26 טריליון דולר.

4.3.4. בהתאמה, אנו מעריכים כי אחוז העלות מתקיפות סייבר מהתמ"ג של מאפייני מדינה כישראל גדל מ־0.45% תוצר ל־0.63% תוצר.

4.3.5. נתוני התוצר המקומי הגולמי בישראל (תמ"ג) לשנת 2023 - 1,868 מיליארד ₪.[21]

4.3.6. **בהתאם לאמור לעיל ובפרט תחת מגבלות המחקרים שתוארו, אומדן לעלויות בגין תקיפות סייבר בישראל בשנת 2023, בשיטת top-down, מסתכם בכ־11.8 מיליארד ₪.**

5. ניתוח bottom-up

החישוב בשיטת bottom-up מבוצע בהתאם למכפלת העלות הממוצעת בגין תקיפה בכמות התקיפות המוערכת בישראל. כמות התקיפות תחושב בהתאם לכמות העסקים בישראל מוכפלת בהסתברות לתקיפת סייבר עם נזק, לרבות התייחסות להערכת החסר בדיווחים על תקיפות סייבר עם נזק. העלות הממוצעת לתקיפת סייבר תחושב בהתאם לעלות הישירה לתקיפת סייבר בתוספת אומדן העלות העקיפה לתקיפת סייבר.

5.1. כמות העסקים בישראל

5.1.1. נתונים בדבר כמות העסקים הפעילים בישראל לשנת 2022, בחלוקה לקבוצות גודל של משרות שכיר פורסמו על ידי הלשכה המרכזית לסטטיסטיקה (להלן, הלמ"ס) בינואר 2024.[22]

5.1.2. בהתאם לנתונים בשנת 2022 היו בישראל 684,156 עסקים פעילים.

5.1.3. לצורך ניתוח העלויות הנובעות ממתקפת סייבר בישראל חולקו העסקים הפעילים בישראל לשלוש קבוצות גודל של משרות שכיר, כלהלן:

---

[21] למ"ס - החשבונות הלאומיים לשנת 2023 : אומדן שני - מרץ 2024- לוח 1 - הוצאה על התוצר המקומי הגולמי.
https://www.cbs.gov.il/he/mediarelease/pages/2024/%D7%94%D7%97%D7%A9%D7%91%D7%95%D7%A0%D7%95%D7%AA-%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99%D7%99%D7%9D-%D7%9C%D7%A9%D7%A0%D7%AA-2023-%D7%90%D7%95%D7%9E%D7%93%D7%9F-%D7%A9%D7%A0%D7%99.aspx

[22] פרסום זה כולל מידע בנושא דמוגרפיה של עסקים ומכיל מאגר נתונים שנתיים על אודות עסקים ומאפייניהם ממרשם העסקים. הפקת הנתונים לפרסום נעשתה באגף עסקים-כלכלה של הלשכה המרכזית לסטטיסטיקה, על פי ההנחיות החדשות של ארגוני Eurostat (הלשכה הסטטיסטית של האיחוד האירופי) וה־OECD (הארגון לפיתוח ושיתוף פעולה). לצורך הערכת העלויות השתמשנו בלוח 1: עסקים פעילים לפי ענף סדר וקבוצת גודל משרות שכיר ישראלים וזרים, 2022.
https://www.cbs.gov.il/he/publications/Pages/2023/%D7%93%D7%9E%D7%95%D7%92%D7%A8%D7%A4%D7%99%D7%94-%D7%A9%D7%9C-%D7%A2%D7%A1%D7%A7%D7%99%D7%9D-%D7%9E%D7%A7%D7%91%D7%A5-%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D-%D7%A1%D7%98%D7%98%D7%99%D7%A1%D7%98%D7%99%D7%99%D7%9D-%D7%9E%D7%9E%D7%A8%D7%A9%D7%9D-%D7%94%D7%A2%D7%A1%D7%A7%D7%99%D7%9D-2011-2021.aspx

קבוצת גודל (משרות שכיר)	כמות עסקים בשנת 2022
0-9	634,242
10-200	47,755
+200	2,159
סה"כ	684,156

5.1.4. החלוקה בוצעה לקבוצות גודל משרות שכיר כאמור, תוך התאמה לסקרים שבוצעו בישראל בשנים האחרונות על ידי הלמ"ס ועל ידי הסוכנות לעסקים קטנים ובינוניים. פירוט לגבי הסקרים ואופן השימוש בהם לצורך הערכת העלויות מתקיפות סייבר יפורט בהמשך.

5.2. ההסתברות לתקיפה

5.2.1. הנתונים בפרק זה הסתמכו על שני הסקרים המעודכנים ביותר שבוצעו בישראל:

- נתוני סקר שימושים בטכנולוגיית מידע ותקשורת והגנת סייבר בעסקים, שנערך על ידי הלמ"ס בשנת 2020.[23] **סקר זה בוצע על עסקים המעסיקים מעל עשרה עובדים.**
- סקר עסקים קטנים ובינוניים, שכיחות מתקפות סייבר בעסקים ואופני ההתגוננות 2023, שנערך על ידי הסוכנות לעסקים קטנים ובינוניים במשרד הכלכלה והתעשייה.[24] **בסקר זה ניתן דגש לעסקים המעסיקים עד עשרה עובדים.**

5.2.2. סקר הלמ"ס הוא סקר מקיף המתמקד בעסקים שמעסיקים מעל עשרה עובדים, ומבוצע על ידי גוף סטטוטורי שאחראי על עיבוד ניתוח ופרסום מידע סטטיסטי בישראל. נתוני ההסתברות לתקיפת סייבר בעלת נזק עבור עסקים המעסיקים מעל עשרה עובדים נלקחו מסקר זה.

[23] על בסיס מדגם של כ־2,500 עסקים. סך האוכלוסייה כוללת את כל העסקים עם עשרה מועסקים - כ־31,000 עסקים. הסקר לא כלל את כל הענפים במשק. ענפים שלא נכללו בסקר: חקלאות, יהלומים, שירותים פיננסיים וביטוח, מינהל ציבורי ומקומי, ביטחון, שירותי בריאות וסעד, אומנות בידור ופנאי. הסקר התייחס לחתכי כמות עובדים בלבד.
[24] סקר טלפוני שנערך בחודשים יוני–יולי 2023 בקרב 902 עסקים בישראל בגודל של עד מאה מועסקים.

5.2.3. להלן ההסתברויות לתקיפת סייבר עם נזק על פי הסקר עבור קבוצות גודל משרות שכיר שהוגדרו בסעיף הקודם, של **עסקים המעסיקים מעל עשרה עובדים**:

קבוצת גודל (משרות שכיר)	אחוז העסקים שחוו תקיפת סייבר עם נזק
10-200	[25]3.4%
+200	[26]4.5%

5.2.4. הסקר לא כלל את כל הענפים במשק.[27] לצורך פשטות התחשיב נלקחה הנחה שאחוז העסקים שחוו תקיפת סייבר עם נזק גם בענפים שלא נכללו בסקר זהה.

5.2.5. עבור עסקים **המעסיקים פחות מעשרה עובדים** נסתמך על סקר עסקים קטנים ובינוניים, שבוצע על ידי הסוכנות לעסקים קטנים ובינוניים. בהתאם לסקר **1%** מסך העסקים חוו תקיפת סייבר עם נזק.

5.3. אי־דיווח על תקיפות סייבר

5.3.1. עקב התמריץ השלילי לדיווח על תקיפת סייבר (פגיעה במוניטין וכו'), כמות התקיפות בפועל גבוהה מכמות התקיפות המדווחות. לצורך החישוב שיובהר בהמשך, נגדיר את היחס בין מספר התקיפות המדווחות למספר התקיפות בפועל כ"מקדם אי הדיווח".

5.3.2. תופעת אי־דיווח על תקיפות סייבר על ידי נתקפים באה לידי ביטוי במחקרים ובנתונים המפורסמים על ידי רשויות ברחבי העולם:

- דוח של הסנאט האמריקאי מ־2022 העריך כי 75% מתקיפות הכופרה לא מדווחות.[28]
- מחלקת המשפטים האמריקאית העריכה כי 85% מהתקיפות אינן מדווחות.[29]

---

[25] התאמה למול סקר הלמ"ס - קבוצה של 10–250 עובדים.
[26] התאמה למול סקר הלמ"ס - קבוצה של 250 עובדים ומעלה.
[27] ענפים שלא נכללו בסקר: חקלאות, יהלומים, שירותים פיננסיים וביטוח, מינהל ציבורי ומקומי, ביטחון, שירותי בריאות וסעד, אומנות בידור ופנאי.
[28] United States Senate Committee on Homeland Security and Governmental Affairs (2022). *Use of cryptocurrency in ransomware attacks, available data, and national security concerns.*
[29] https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud.

- בדוח השנתי לשנת 2023[30] של ה- FBI צוין כי תקיפות כופרה רבות לא מדווחות.
- דוח של 'ברקליס' עם המוסד למנהלים בבריטניה (IOD) העריך כי שיעור התקיפות אשר אינן מדווחות הוא 72%.[31]
- משטרת לונדון מעריכה כי 85% ממקרי הסייבר לא מדווחים.[32]
- דו"ח של משרד רו"ח וייעוץ RSM מצא באמצעות סקר במדינות אירופה כי 77% ממתקפות הסייבר אינן מדווחות לרשויות.[33]

5.3.3. בהתאם לאמור ועל פי המקורות שצוינו לעיל, יחס אי־הדיווח הוא בין 4 ל־5, קרי: על כל תקיפה מדווחת, מספר המקרים בפועל **גבוה פי ארבעה–חמישה.**

5.3.4. לצורך הערכת הנזק בישראל באופן שמרני, נגדיר כי **מקדם אי־הדיווח הוא 4**, כלומר 75% מהמקרים אינם מדווחים לרשויות או במסגרת הסקרים.

5.4. עלות ישירה ממוצעת למקרה תקיפת סייבר

5.4.1. העלות הממוצעת לתקיפת סייבר מתבססת על מחקר של חברת סיכוני סייבר NetDiligence.[34]

5.4.2. המחקר בחן 9,000 תביעות סייבר של חברות ביטוח לאורך השנים 2018–2022 בארצות הברית ובמדינות נוספות. מחקר זה מבוסס על תביעות בפועל, ולכן אמינות הנתונים שבו גבוהה יותר לעומת מחקרים אחרים המתבססים על סקרים וראיונות.

5.4.3. העלות הממוצעת במחקר כוללת מספר מרכיבי עלות ישירים ספציפיים המוגדרים במחקר שנוגעים בעיקר לטווח הקצר:

<u>עלויות הקשורות לניהול האירוע</u> - לדוגמה: עלויות ייעוץ והדרכה באירוע, IR, זיהוי, הודעה, יחסי ציבור;

---

[30] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[31] U.K. study reveals serious underreporting of cyber attacks by business

[32] Kennedy, Lindsey (2015, March 23). 85% of fraud and cybercrime unreported. The Global Treasurer. https://www.theglobaltreasurer.com/2015/03/23/85-of-fraud-and-cybercrime-unreported/

[33] Catch-22: Digital transformation and its impact on cybersecurity
הסקר בוצע ב־33 מדינות באירופה, ונסקרו בו כ־600 חברות.

[34] Cyber claims study 2023 report
NetDiligence עוסקת בסיכוני סייבר. העלות כוללת עלויות ניהול המשבר מעת שקרה, עלות טיפול בנזקי התקיפה וכו'.

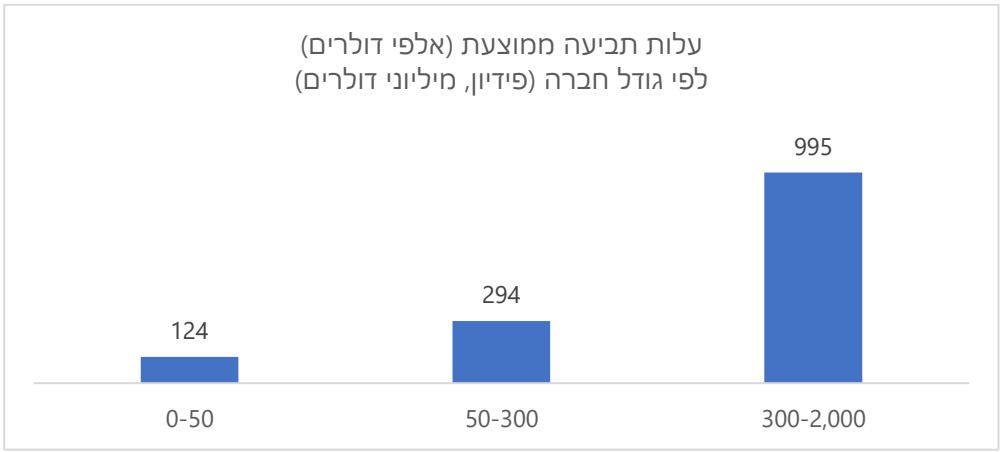
<u>עלויות משפטיות</u> - לדוגמה: ייעוץ משפטי, ייעוץ מול רגולטורים, התמודדות עם תביעות וקנסות;

<u>עלויות הנובעות מאובדן הכנסה ישיר</u> - אובדן הכנסות הנובעות מהשבתת העסק ועלויות התאוששות.

5.4.4. העלות הממוצעת מושפעת מאירועים גדולים הכרוכים בעלויות גבוהות ואינה מהווה אינדיקציה לעלות השכיחה של תקיפת סייבר לעסק. לצורך ניתוח העלות השכיחה לעסק, החציון מהווה מדד טוב יותר. עם זאת, לצורך ניתוח אגרגטיבי, כפי שמבוצע במסמך זה, נכון להשתמש בעלות הממוצעת.

5.4.5. יודגש כי עלות זאת בחסר משמעותי, כיוון שהיא כוללת את תביעת העסק מחברת הביטוח בלבד, ואינה כוללת עלויות כגון: פגיעה בהכנסות עתידיות, "הגבהת חומות", אמון הלקוחות, מוניטין. כיוון שנרצה לתת ביטוי מלא לכלל העלויות הכרוכות במתקפת הסייבר, נעריך עלויות אלו בהמשך הסקירה.

5.4.6. להלן עלות תקיפת סייבר ממוצעת בהתאם למחזור החברה, כאשר ממצאי המחקר מצביעים על קשר ישיר בין גודל החברה במונחי פדיון לעלות הממוצעת למקרה:



5.4.7. מאחר שההסתברויות לתקיפה נותחו על בסיס גודל החברה במונחי עובדים, והעלות לתקיפה מנותחת על בסיס גודל החברה במונחי פדיון ולא קיימים נתונים מהימנים אחרים, נדרש לבצע התאמה לנתונים אלו כלהלן.

5.4.8. תחת ההנחה הסבירה[35] כי קיים מתאם בין כמות העובדים בעסק למחזור, נעריך כי עבור עסקים עם יותר מ־200 עובדים הסתמכנו על העלות הממוצעת לתקיפה עבור עסקים עם מחזור שבין 50–300 מיליון דולר. עבור עסקים עם 10–200 עובדים הסתמכנו על העלות הממוצעת לתקיפה עבור עסקים עם מחזור עד 50 מיליון דולר.

5.4.9. ייתכן, כי העלות הממוצעת עבור העסקים הגדולים שמעסיקים יותר מ־200 עובדים שכירים היא הערכת חסר, כיוון שאינה מביאה לידי ביטוי בממוצע את העלות בגין תקיפת הסייבר לעסקים עם מחזור של יותר מ־300 מיליון דולר. נדרש לבצע ניתוח נוסף בעתיד על מנת לדייק נתונים אלו.

5.4.10. לחישוב העלות הממוצעת בגין לתקיפה של עסקים עד תשעה עובדים הסתמכנו על מחקר של חברת הביטוח HISCOX.[36] בהתאם למחקר, העלות החציונית לנזק כלכלי של חברות עם 0–9 עובדים **נמוך בכ־50%** מהנזק החציוני של חברות עם 10–250 עובדים. לפיכך הערכנו את העלות הממוצעת לחברות עם 0–9 עובדים במחצית מהעלות של עסקים בעלי 10–200 עובדים שכירים (124 אלף דולר).

5.4.11. בהתאם לכל האמור לעיל, אנו מעריכים את העלות הממוצעת בגין תקיפת סייבר על קבוצות גודל העסקים שהגדרנו כלהלן:

קבוצת גודל (משרות שכיר)	עלות ממוצעת לתקיפה (אלפי דולר)
0-9	62
10-200	124
+200	294

[35] בהתאם לסקר הלמ"ס (עוסקים ופדיון בענפי כלכלה לפי מס ערך מוסף 2020–2022) ישנם כ־3,800 עסקים בישראל שמחזורם השנתי מעל 100 מש"ח, כאשר המחזור הממוצע לעסקים אלו הוא כ־440 מש"ח (115 מיליון דולר). בקבוצת העסקים המעסיקים מעל 200 עובדים ישנם כ־2,160 עסקים אשר סביר להניח שרובם נכללים בקבוצה זאת. על כן ניתן לשייך את העלויות בגין התקיפה לעסקים בעלי מחזור של 50–300 מיליון דולר לקבוצת העסקים שמעסיקים 200+ עובדים, כפי שמתואר בפסקה.

[36] Hiscox Cyber Readiness Report 2023 - נתונים מבוססים על סקר של 5,000 משתתפים בארצות הברית ואירופה. מתוך הסקר יותר מרבע הם עסקים קטנים עם פחות מעשרה עובדים.

5.5. המחיר המלא בנוגע לתקיפת סייבר - אומדן העלויות העקיפות

5.5.1. העלויות שפורטו הן בחסר היות שהן אינן כוללות עלויות עקיפות בטווח הבינוני-ארוך שלאחר המקרה.

5.5.2. העלויות העקיפות כוללות אובדן הכנסות עתידיות, איבוד הזדמנויות עסקיות, התמגנות מחודשת ומשופרת, איבוד אמון של לקוחות ועובדים ופגיעה במוניטין החברה.

5.5.3. לעלויות העקיפות, מעצם טבען, יכולות להיות השלכות כלכליות משמעותיות, הן נמשכות לאורך תקופת זמן ארוכה יותר מהעלויות הישירות, מורכבות למדידה ולהערכה והן קשות יותר לתיקון על ידי העסק שנפגע מתקיפת סייבר.[37]

5.5.4. מורכבות המדידה והערכה של העלויות העקיפות מהווה אתגר ביצירת אומדן לעלויות אלו. בחרנו להתמודד עם אתגר זה באמצעות ממצאים שעלו במחקר של חברת IBM, כפי שיפורט בהמשך. על אף שהממצאים במחקר של חברת IBM הנוגעים לעלויות העקיפות הם ברמת סמך שאינה גבוהה בהקשר העלויות העקיפות, אנו רואים חשיבות במתן ביטוי לעלויות העקיפות במחיר התקיפה וכנגזרת בסך עלויות התקיפה בישראל. אנו מצפים כי מחקרים בתחום יאפשרו שיפור האומדנים בעתיד.

5.5.5. כאמור, לצורך אומדן העלויות העקיפות השתמשנו בנתונים שפורסמו במחקר העדכני של חברת IBM[38], שכלל מדגם של 553 חברות. מחקר זה כלל במסגרת העלויות גם עלויות עקיפות כגון איבוד לקוחות, פגיעה במוניטין ואובדן הכנסות, עלויות שלא באו לידי ביטוי בנתוני תביעות הביטוח שהוצגו בפרק הקודם.

5.5.6. בהתאם למחקר IBM, העלויות בשנה הראשונה שלאחר התקיפה מהוות 51% מסך עלויות התקיפה. ניתן להעריך כי עלויות אלו מהוות את העלויות המיידיות והישירות שחווה העסק בעקבות האירוע ושאותן ניתן לקשר באופן חד משמעי

[37] Cyberattacks on critical infrastructure: An economic perspective.

[38] Cost of a data breach report 2023 - מבוסס על מחקר של 553 חברות מ־16 מדינות (כולל מזרח תיכון) ומ־17 סקטורים. עלויות הנזק כוללות עלויות ישירות ועקיפות הקשורות למקרה התקיפה כגון: איתור התקיפה דיווח לגורמים רלוונטיים, טיפול בפגיעה לאחר התקיפה, הפסדים לעסק (אובדן הכנסות, איבוד לקוחות, פגיעה במוניטין).

לאירוע לצורכי תביעת הביטוח. יתרת העלויות מהוות בראייתנו עלויות עקיפות שסביר להניח שאינן נכללות במסגרת תביעות הביטוח.

5.5.7. בהתאם לכך נעריך כי העלויות העקיפות זהות בשווין לעלויות הישירות.

5.6. סיכום עלויות שנתיות הנובעות מתקיפות סייבר בישראל בשיטת bottom-up

5.6.1. להלן סיכום הניתוח בהתאם לפרמטרים שהוצגו לעיל:

כמות עסקים לפי קבוצות משרות שכיר	כמות עסקים (אלפים) (1)	עלות ישירה ממוצעת למקרה (אש"ח) (2)	אחוז תקיפות עם נזק (3)	מקדם אי דיווח (4)	סה"כ עלויות ישירות (מש"ח) (5)	סה"כ עלויות ישירות ועקיפות (מש"ח) (6)
0-9	634,242	223	1.00%	4	5,663	11,325
10-200	47,755	446	3.40%	4	2,899	5,798
+200	2,159	1,058	4.50%	4	411	823
סה"כ	**684,156**				**8,973**	**17,946**

(1) בהתאם לפרק 5.1 - כמות העסקים בישראל לפי קבוצות משרות שכיר

(2) בהתאם לפרק 5.4- עלות ממוצעת למקרה סייבר[39]

(3) בהתאם לפרק 5.3 - הסתברות לתקיפה עם נזק

(4) בהתאם לפרק 5.4 - אי דיווח והערכת חסר בסקרים

(5) מכפלה של כלל הגורמים (1) עד (4)

(6) סך העלות הישירה בתוספת העלויות העקיפות כפי שבאות לידי ביטוי בפרק 5.5.

5.6.2. **בהתאם לניתוח שבוצע בשיטת bottom-up, העלויות ממתקפות סייבר בישראל מסתכמות בכ־18 מיליארד ₪ בשנה.**

5.6.3. יצוין כי בהתאם לנתונים שהתקבלו, חלק עיקרי מהעלויות בגין תקיפות הסייבר נובע מהעסקים הקטנים והבינוניים, עסקים אשר חלקם בתמ"ג מהווה יותר מ־50%.[40] ייתכן כי נתון זה נובע מהערכת חסר של העלויות בגין תקיפות הסייבר לעסקים גדולים שתואר לעיל. בכל מקרה, נדרש מחקר נוסף בנושא על מנת לבסס ממצאים אלו.

[39] המרה לש"ח ביחס 1:3.6.

[40] משרד הכלכלה והתעשיה, הסוכנות לעסקים קטנים ובינוניים (2023, ינואר). **דוח תקופתי: מצב העסקים הקטנים והבינוניים 2023**. https://www.sba.org.il/hb/PolicyAndInformation/Researches/Pages/SR77.aspx
בהתאם לממצאי הדו"ח 55% מהתמ"ג מקורם בעסקים קטנים ובינוניים (עסק עד 100 עובדים).

6. השפעת התועלת מהעלאת רמת ההגנה והפחתת התקיפות

בפרקים הקודמים בוצעה הערכה לעלות השנתית בגין תקיפות סייבר בישראל. בפרק זה נסקור מחקרים מובילים העוסקים בהעלאת רמת ההגנה והפחתת התקיפות.

6.1. הפחתת כמות מקרי התקיפה כתוצאה מהעלאת רמת ההגנה

6.1.1. מחקר שבוצע על ידי פרופסורים מאוניברסיטאות תל אביב, קולומביה וטולסה ופורסם בכתב העת Computer and Security,[41] **הראה שיישום צעדי הגנה בתחום הגנה בסייבר יכול להביא לירידה משמעותית של בין 30%–50% בהסתברות לתקיפות סייבר.**

6.1.2. המחקר התבסס על נתוני סקר חברות שבוצע **בישראל** על ידי הלשכה המרכזית לסטטיסטיקה. הסקר כלל מענה מ־993 חברות בישראל. במסגרת המחקר חושבה ההסתברות לתקיפת סייבר באמצעות שיטת הרגרסיה, כאשר המשתנה התלוי הוא ההסתברות לתקיפת סייבר. המשתנים המסבירים כללו את פעולות ההגנה שנקטה החברה, גודל החברה, היקף ההכנסות השנתי, הסקטור שבו פעלה החברה ומאפיינים נוספים.

6.1.3. מחקר נוסף[42], שביצעו במשותף אוניברסיטת קיימברידג' וחברת BitSight, חשף את המשמעות הגדולה של נקיטת אמצעי הגנה בתחום הסייבר על ירידת הסיכויים להיתקל בתקיפות סייבר. המחקר התבצע באמצעות סימולציה של שלושה סוגי מתקפות (כופר, תקלה בשירותי ענן ודליפת מידע) על פי רמת הגנת סייבר בארבע קטגוריות שונות. **התוצאות הראו כי יישום של בקרת הגנת סייבר <u>בודדת</u> יכול לצמצם את ההסתברות למתקפת סייבר בין 7%–35%,** תלוי בסוג הבקרה. לעומת זאת, הפעלת שילוב של כל ארבע הבקרות בו־זמנית עשויה להביא לירידה עוד יותר משמעותית בהסתברות לתקיפה.

[41] Gandal, N., Moore, T., Riordan, M., & Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incident. Computer and Security, 133, Article 103380. https://doi.org/10.1016/j.cose.2023.103380

[42] Cambridge Centre for Risk Studies, BitSight Technologies (2022), Cyber Security Cost Effectiveness for Business Risk Reduction.

6.2. הפחתת עלות נזק התקיפה כתוצאה מהעלאת רמת ההגנה

6.2.1. לפי סקר עדכני שערכה חברת IBM שתואר לעיל, ההוצאה הממוצעת הנלווית למתקפת סייבר עם רמה נמוכה של מנגנוני הגנה מסתכמת ב־5.36 מיליון דולר. לעומת זאת, ארגונים עם רמת אבטחה גבוהה נתונים להוצאה ממוצעת נמוכה יותר של 3.78 מיליון דולר.

6.2.2. רמות האבטחה מורכבות בהתאם למחקר מ־27 מנגנוני הגנה כגון: הכשרת עובדים, תוכנית תגובה, צוות תגובה, ביטוח סייבר, כלי הגנה, שימוש ב־AI ועוד. מנגנונים אלו נבחנו במסגרת הסקר על מנת לגבש תמונת מצב של רמת ההגנה בארגונים וההקשר לגובה הנזק.

6.2.3. **בהתאם לכך, ניתן לראות כי יכולות אבטחה מתקדמות יכולות להוריד את העלות הממוצעת בגין תקיפה בכ־30%.**

6.3. סיכום ממצאים

6.3.1. מהנתונים המרוכזים במחקרים שהוצגו לעיל עולה כי אמצעי הגנה מתקדמים בסייבר עשויים להפחית את ההיתכנות של אירועי תקיפה ב־30%–50%, וכן לצמצם את העלות המוערכת בגין לתקיפה שכזו, אם תתרחש, בכ־30%.

6.3.2. איחוד פשטני של שני הפרמטרים הללו, במקרה של יכולות אבטחה מתקדמות, ירידה בהסתברות לתקיפה (30%) וירידה בעלות הממוצעת בגין תקיפה (30%), יכול להוביל להערכה כי תוצאת ההשקעה באמצעי הגנה מתקדמים תהיה הורדה של עד 50% בתוחלת העלויות הצפויות כתוצאה מתקיפות סייבר.

6.3.3. לשם המחשה, אם נתבונן בתוחלת הנזק הכלכלי מתקיפות סייבר בישראל בהתאם לניתוח top-down, שהוערכה בכ12 מיליארד ₪ בשנה, נמצא כי ירידה של רק 10% בסיכוי למתקפת סייבר ורק 10% בעלויות הממוצעות של כל תקיפה עשויה לתרום לחיסכון המשמעותי של יותר משני מיליארד ₪ לכלכלה הישראלית ברמת המאקרו וכן לעסקים ברמת המיקרו.

6.3.4. נדרש ניתוח נוסף להערכת ההגנה הנוכחית במשק הישראלי על מנת להעריך באופן מדויק את התועלת הפוטנציאלית למשק הישראלי משיפור ברמת ההגנה. אף על פי כן, בהתבסס על הנתונים הזמינים למערך הסייבר הלאומי,

ניתן להעריך כי התועלת הכלכלית מהעלאת רמת ההגנה היא בהחלט משמעותית.

6.3.5. חשוב לציין כי היתרונות המשמעותיים של שיפור אמצעי ההגנה בסייבר, המוזכרים בפסקאות הקודמות, חלים במיוחד על ארגונים שבמצב הנוכחי נחשבים לפחות מוגנים, על בסיס עקרון התועלת השולית הפוחתת בהגנה בסייבר.

6.3.6. כמו כן, קיימות תועלות כבדות משקל נוספות להגנה בסייבר שלא נותחו במסמך זה, בין היתר: שמירה על חיי אדם, רציפות תפקודית, שמירה על פרטיות וכו'.

7. עלויות העלאת רמת ההגנה

7.1.1. בהתאם למודל גורדון–לוב,[43] שמהווה את המודל הבסיסי לראייתנו בחקר התיאורטי של כלכלת סייבר, ארגון ישקיע בהעלאת רמת ההגנה בסייבר את השקל השולי, כל עוד הפחתת תוחלת העלות ממתקפת סייבר תהיה גבוהה מההשקעה.

7.1.2. המתכנן המרכזי (הממשלה) צריך לקחת בחשבון את עלויות העלאת רמת ההגנה בקביעת צעדי המדיניות שהוא מחיל על המשק. בנוסף, המתכנן המרכזי צריך להעריך את רמת ההגנה הקיימת במשק וכמות העסקים שיצטרכו להגביר את רמת ההגנה שלהם בעקבות המדיניות.

7.1.3. מחקר של CIS[44] בחן את עלויות הגנת הסייבר השנתיות בארגון לפי מאפייני הארגון, וחילק את הארגונים לשלוש שכבות (tiers) בהתאם לכמות העובדים, מספר המערכות ופרמטרים נוספים.

7.1.4. המחקר הציג לכל שכבה את העלות השנתית להגנת סייבר בחלוקה לעשרה תחומי פעילות בסיסיים בתחום הגנת הסייבר (לדוגמה: ניהול נכסים, ניהול מידע, גישה).

---

[43] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment, *ACM Transactions on Information and Systems Security, 5*(4), 438–457,

44 Center for Internet Security - ארגון ללא כוונת רווח שפועל החל משנת 2000 למרחב בטוח באינטרנט, תומך בעזרה לפרטים, ארגונים וממשלות בהתמודדות עם איומי סייבר.
Center for Internet Security (2023, August).The cost of cyber defense: CIS controls implementation group 1.

7.1.5. בכל אחת מהשכבות צוין כי לכל תחום פעילות קיים היום בשוק פתרון חינמי המבוסס על קוד פתוח (Open Source) או המהווה אחוז נמוך מתקציב ה־IT של הארגון, כך שלמעשה ניתן לבצע את העלאת רמת ההגנה ללא עלות לכאורה או בעלויות נמוכות למול הנזקים הפוטנציאליים.

8. סיכום וכיוונים להמשך

8.1.1. האתגר של המתכנן המרכזי במדינת ישראל הוא למקסם את התועלת הכלכלית מהפחתת עלויות בגין תקיפות סייבר לצד התועלות הנוספות, תוך שקלול עלויות העלאת רמת ההגנה. לפיכך, קיימת חשיבות רבה למחקר כלכלי העוסק בתחום עלויות בגין תקיפות הסייבר והדרכים להפחית עלויות אלו.

8.1.2. במסמך זה בוצעה סקירה בין-לאומית של מחקרים, מאמרים ונתונים העוסקים בעלות הכלכלית הנובעת ממתקפות הסייבר והתועלות בהעלאת רמת ההגנה.

8.1.3. ממצאי הסקירה אפשרו לנו לבצע הערכה לעלות הכלכלית הנובעת ממתקפות הסייבר בישראל בשנה. הערכה זאת בוצעה הן בגישת top-down והן בגישת bottom up.

8.1.4. בניתוח bottom-up העלות בגין תקיפות סייבר בישראל לשנה היא כ־18 מיליארד ₪ בשנה. בניתוח top-down הערכת העלות בגין תקיפות סייבר בישראל היא כ־12 מיליארד ₪.

8.1.5. בהתאם לממצאים, אנו מעריכים כי העלות בגין תקיפות הסייבר בישראל היא לפחות **12 מיליארד ₪ בשנה.**

8.1.6. מחקרים שבוצעו בשנים האחרונות הצביעו שניתן להפחית עלויות אלו באמצעות העלאת רמת ההגנה במרחב הסייבר, והיא תורמת לירידה בעלות הממוצעת בגין תקיפה וכן בהסתברות לתקיפה. פתרונות אבטחת סייבר ללא עלות, או בעלויות נמוכות, שקיימים בשנים האחרונות מאפשרים גם לעסקים קטנים ובינוניים להגביר את רמת ההגנה.

8.1.7. פעילות מערך הסייבר הלאומי תורמת להעלאת רמת ההגנה במרחב הסייבר וכפועל יוצא הגדלת התועלת הכלכלית. פעילויות אלו כוללות, בין היתר: הגנה אקטיבית והנחיית גופים קריטיים; מדיניות; ניטור שוטף; העלאת רמת המודעות; התרעות למשק; יצירת שותפויות מקומיות ובין-לאומיות ועוד.

8.1.8. בימים אלו מגבש מערך הסייבר צעדי מדיניות נוספים להעלאת רמת ההגנה במרחב בסייבר, הן בתחום האסדרה (חוק הסייבר) והן ביצירת תמריצים כלכליים לארגונים ("שיטת הגזרים").

8.1.9. המשך מחקר כלכלי, הנוגע להערכת עלויות בגין תקיפות סייבר והעלאת רמת ההגנה בסייבר, הוא חיוני במטרה לבסס צעדי מדיניות יעילים אשר יגבירו את התועלת הכלכלית. להלן מספר עבודות רלוונטיות המקודמות במערך הסייבר הלאומי במטרה לשפר את ההערכות והאומדנים במסגרת מחקר עתידי וכן על מנת לייצר בסיסי נתונים מהימנים עבור מדינת ישראל בתחומים הבאים:

ניתוח כמות מקרי הסייבר בישראל ומדידתם - איסוף נתונים על כמות מקרי מתקפות הסייבר בישראל בחתכים שונים כגון: גודל חברה, תחום עיסוק, ובמידת האפשר גם נזק כספי. יצוין, כי במסגרת חקיקת חוק הסייבר העתידית קיימת חובת דיווח על אירועי סייבר (על פי המוגדר בטיוטת החוק). איסוף נתונים סדור יאפשר הערכה מהימנה יותר של מקרי מתקפות הסייבר בישראל.

ביצוע סקרים סדורים- ביצוע סקרים סדורים לאמידת רמת ההגנה של הארגונים בישראל, וכמות מתקפות הסייבר השנתית. סקרים אלו יבוצעו על ידי מגוון גופים כגון: הלשכה המרכזית לסטטיסטיקה, ארגון התעשיינים או הסוכנות לעסקים קטנים ובינוניים ובהכוונת מערך הסייבר הלאומי.

ניתוח עלויות למקרי סייבר מרכזיים שהתרחשו בישראל- ניתוח עומק של ההשפעות הכלכליות באירועי סייבר נבחרים. כאמור, ניתוח יאפשר להבין בצורה טובה יותר את מחוללי העלות המרכזיים בתקיפות סייבר.