







ניהול סיכוני סייבר במפעל תעשייה המכיל חומ"ס



נושאי הלימוד



- מושגי יסוד בניהול סיכונים 
- קבוצות סיכונים 
- מיפוי נכסים 
- גישות שונות לביצוע ניהול סיכונים 
- סקר סיכונים במערכת תעשייתית המכילה חומרים מסוכנים 
- מדריך סייבר לתעשייה 

מה זה סיכון?

הגדרה המילונאית של סיכון:

“חשש או אפשרות לאירוע אשר עלול לגרום לנזק או להפסד”

במקרה של המשרד להגנת הסביבה ההתמקדות היא בסיכונים הבאים:

- ❑ פגיעה ברצפטור הציבורי
- ❑ פגיעה / נזק לאיכות הסביבה בישראל

על-סמך הגדרה זו, יש לאתר את המקומות שבהם ישנה חשיפה לנזקים כפי שהוגדרו בתחום הרגולציה של המשרד



קבוצות סיכונים

סיכונים אסטרטגיים



- פגיעה בתדמית
- פגיעה בלקוחות
- מתחרים
- פיתוח מוצרים

סיכונים פיננסיים



- תזרים מזומנים
- סיכוני אשראי
- סיכוני שער חליפין
- סיכוני ריבית והצמדה
- סיכוני מחיר נירות ערך

קבוצות סיכונים

סיכונים תפעוליים



- תפקוד לקוי של עובדים
- ליקוי במערכות מידע
- ליקוי בתהליכים אחרים בחברה
- **אירוע חומ"ס**

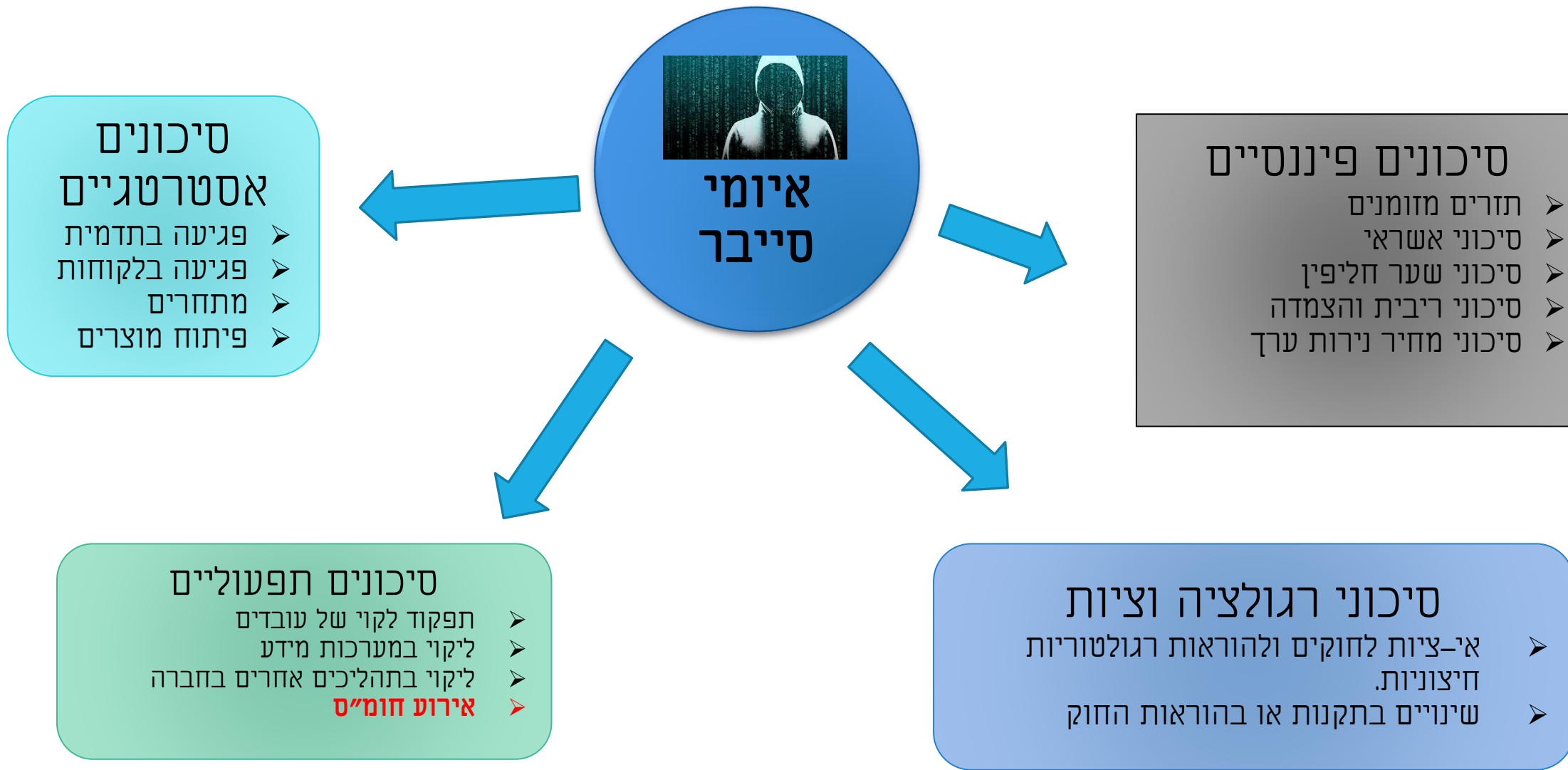
סיכוני רגולציה וציות

- אי ציות לחוקים ולהוראות רגולטוריות חיצוניות
- שינויים בתקנות או בהוראות חוק

חוק
חומרים
מסוכנים



סיכוני אבטחת מידע - הטריגר



שלב טרום - מיפוי נכסים



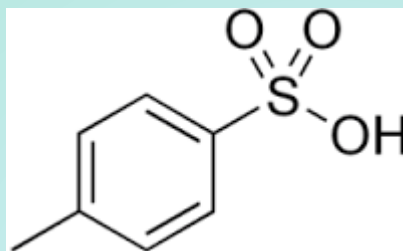
השאלות המרכזיות

- על מה אנחנו רוצים להגן?
- על מה לבצע ניהול סיכונים?

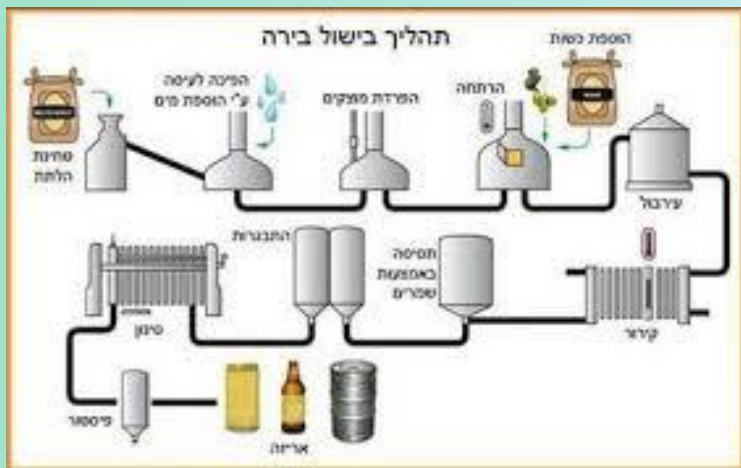
יש לבצע מיפוי על:

1. נכסים קריטיים
2. תהליכים קריטיים

**במפעל חומרים מסוכנים: חומרים מסוכנים המנוהלים / מבוקרים
ע"ח מערכות מיחשוב**



❖ **נוסחת** ייצור קוקה קולה



❖ **תהליך** ייצור בירה

Facts on Amazon



Amazon Company Overview	Values	Statistic
Net sales of Amazon in 2016	136bn USD	Details →
Net income of Amazon in 2016	2.371bn USD	Details →
Number of Amzon.com employees as in 2016	341,400	Details →
Biggest revenue segment of Amazon in 2016	Retail products	Details →
Year-over-year revenue growth of Amazon as of 2016	27%	Details →
Amazon's outbound shipping costs in 2016	16.2bn USD	Details →
Amazon's fulfillment expenses in 2016	17.6bn USD	Details →

Benchmark	Values	Statistic
Most popular online store in the United States in 2016	Amazon	Details →
Amazon's brand value in 2016	98.99bn USD	Details →
Unique monthly U.S. visitors to Amazon sites as of November 2016	184m	Details →
Share of direct traffic to Amazon.com as of April 2017	41.47%	Details →

אתר המכירות AMAZON

אתר מושבת



הפסד רווח ליום:
 $2.37B / 365 = 6.5M$

הפסד לשעה:
 $\$270,000$

הפסד לדקה: **$\$4500$**



❖ תהליך קירור באמוניה

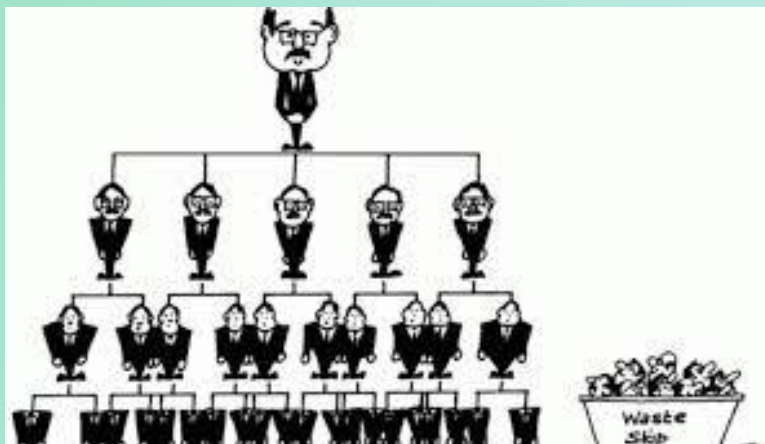
❖ תהליך עיקור ציוד רפואי

❖ תהליך ייצור תרופות

❖ תהליך ייצור חומר מסוכן (דשנים, חומרי ניקוי, חומרי הדברה)

❖ תהליך טיפול בשפכים, או טיפול במי התפלה

איד לבצע מיפוי נכסים



TOP DOWN



BOTTOM UP

מה עדיף?

TOP-DOWN

BOTTOM-UP

יתרונות	<ul style="list-style-type: none">• Starts with the needs of the organization• Provides a "big picture" to the customer and the designer	<ul style="list-style-type: none">• Quick• Leverages previous experience
חסרונות	<ul style="list-style-type: none">• Time consuming	<ul style="list-style-type: none">• Might miss some organizational requirements• High probability of failure



1. דחיית הסיכון

2. קבלת הסיכון

3. מזעור הסיכון

4. העברת הסיכון לצד ג'

1. דחיית הסיכון

דחיית סיכון = ביטול הפרויקט



דוגמא מהחיים:

הימנעות מרכיבה על אופנוע
הימנעות מעישון

דוגמא מעולם הסייבר:

ארגון לא מאפשר לעובדיו גישה לאינטרנט
ארגון לא מאפשר גישה מרחוק אל הארגון

בעולם החומרים המסוכנים

מפעל מפסיק לעבוד עם אמוניה לצורך קרור ומיישם קירור בצורות אחרות (אתילן גליקול)

2: קבלת הסיכון מודעים לסיכון ומקבלים אותו



סיבות:

עלות תועלת

הסיכוי להתממשות נמוך

דוגמא מהחיים:

שותים ונוהגים בתקווה שלא נתפס ולא נעשה תאונה במידה והסיכוי לתאונה יתממש, נקבל את הסיכון במלא עוצמתו

דוגמא מעולם אבטחת המידע

תיתכן החלטה בארגון גדול שלא מתקינים אנטי-וירוס במחשבים במידה ויגיע וירוס – הוא יכנס בוודאות לארגון השאלה כמה נזק יגרום.

בעולם החומרים המסוכנים

לא נוכל להרשות לעצמינו את קבלת הסיכון – מדובר בחיי אדם ופגיעה חמורה בסביבה – יציאה משליטה של המפעל.

הנחת יסוד: לא ניתן לבטל סיכון אלא למזער עד לסיכון שיוורי



הסיכון	מזעור הסיכון	האם מבטל את הסיכון?? לא!!
וירוסים	התקנת אנטי-וירוס	וירוס ZERO DAY
חדירה לאפליקציה	התקנת מוצר הגנה אפליקטיבית	חדירת המוצר
דליפת מידע חיוני לארגון	התקנת מוצר המונע דלף מידע	צילום המידע ממסך המחשב והוצאתו
פריצה פיסיית	מצלמות, מאבטחים	הנדסה חברתית

4. העברת הסיכון לצד ג' (TRANSFER)



חברת ביטוח

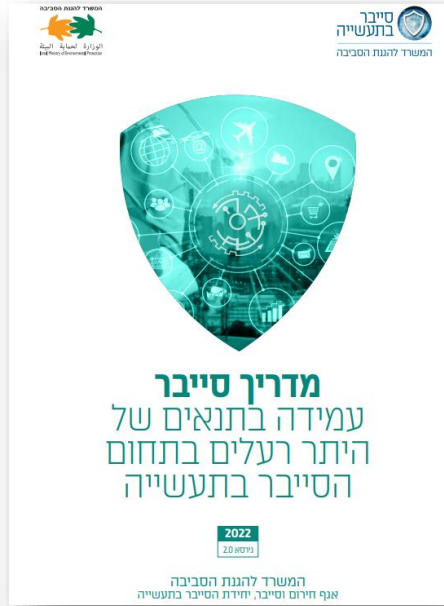
במקרה של התממשות האיום חברת הביטוח תכסה את הנזק

במפעלי חומרים מסוכנים האם ביטוח יכסה חיי אדם??

איך לבצע סקר סיכונים במערכות בקרה תעשייתיות המכילות חומרים מסוכנים ?



מדריכי הסייבר גירסא 1.3 וגירסא 2.0



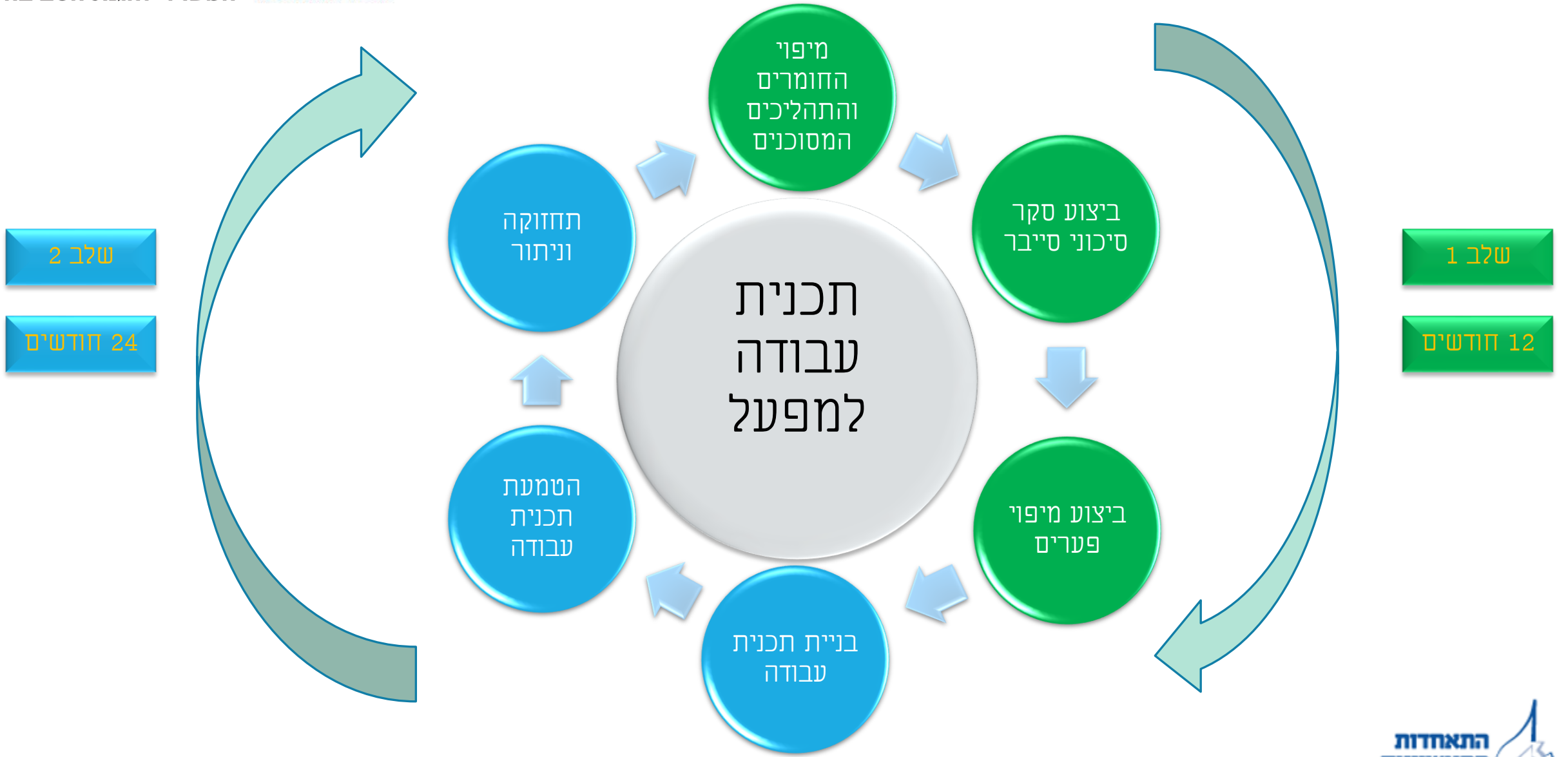
מדריך סייבר 2.0

- חל על מפעלי A , B
- חל על כל מערכת בקרה שמנהלת / מבקרת חומ"ס
- מכיל 99 בקרות

מדריך סייבר 1.3

- חל על מפעלי סבסו בלבד (עליון ותחתון)
- מיפוי תהליך מסוכן ע"פ נספח י"א
- מכיל כ-91 בקרות

תכנית עבודה למפעל לעמידה בדרישות סייבר בהיתר הרעלים



לפני תחילת הפעילות – מינוי ממונה סייבר במפעל 1. מסמך מדיניות הנהלה



- הממונה חייב להיות איש המפעל (לא גורם חיצוני)
- מינוי יתבצע תוך 60 יום ממתן תנאי סייבר
- כתב המינוי בנספח ה' במדריך הסייבר לתעשייה גרסא 2.0

יש להגיש למשרד נספח ה' חתום תוך 60 יום

מסמך מדיניות הנהלה – נשאר במפעל לביקורת עתידית

לפני תחילת הפעילות – מסמך מדיניות הנהלה

מדיניות הנהלה תכלול:

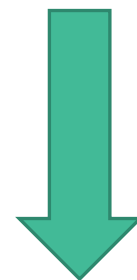
- ✓ הצהרת מחוייבות ההנהלה להגנת סייבר בעסק
- ✓ התחייבות להקצאת המשאבים הנדרשים להגנת סייבר בעסק



מסמך מדיניות הנהלה – נשאר במפעל לביקורת עתידית

שלב 1 - מיפוי

מיפוי החומרים המסוכנים



החומרים המסוכנים אשר מנוהלים / מבוקרים ע"י מערכות מיחשוב

טופס מיפוי נספח ו' - נשאר במפעל לביקורת עתידית

מיפוי החומרים המנוהלים / מבוקרים ע"י מערכות ממוחשבות

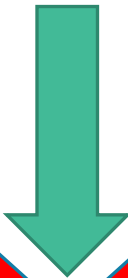
דוגמא למערכות ממוחשבות

- עמדות HMI
- בקרים מכל הסוגים
- סנסורים המחברים בתקשורת ETHERNET
- רכיבי שטח המחברים בתקשורת ETHERNET
- רכיבי נוספים כלשהם המחברים בתקשורת ETHERNET
- מערכות ERP

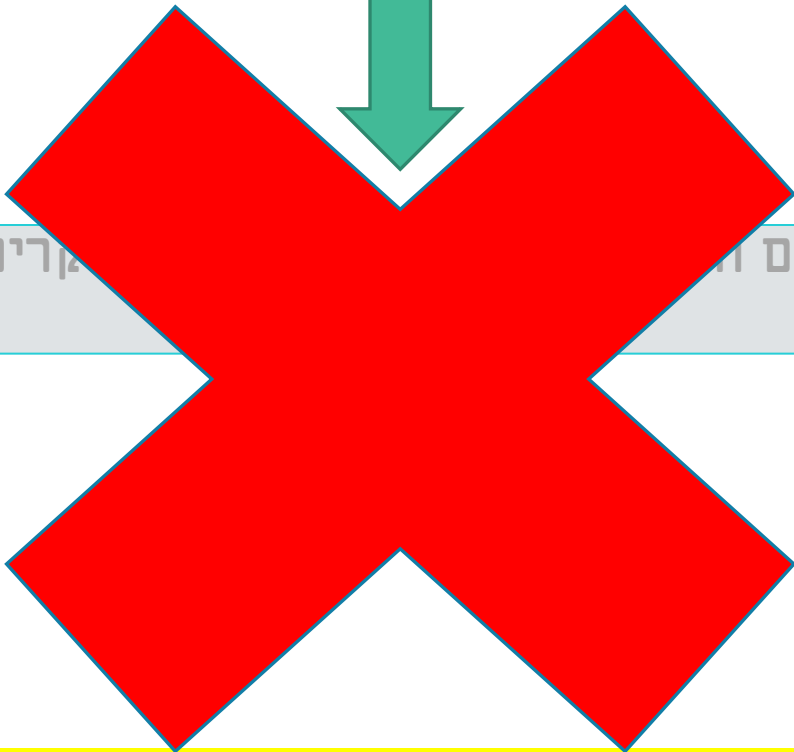


נספח י' – פטור מכניסה לרגולציית סייבר

מיפוי החומרים המסוכנים



החומרים המסוכנים / מקרים ע"י



נספח י' – תצהיר המפעל על העדר מערכות ממוחשבות המנהלות / מבקרות חומרים מסוכנים

נספח י – תצהיר בעל היתר רעלים על היעדר מערכות ממוחשבות המחבורות לחומרים מסוכנים

אני החתום/ה מטה _____, מס' זהות _____, לאחר שהוזהרתי כי עלי לומר את האמת, וכי אם לא אעשה כן אהיה צפוי/ה לעונשים הקבועים בחוק, מצהיר/ה בזה כדלקמן:

1. הריני משמש/ת כ _____, בעבור _____ (שם העסק), מס' היתר רעלים _____.

2. בצעתי הליך הערכת סיכונים כנדרש בהיתר הרעלים ומצאתי כי כלל המערכות המכילות חומרים מסוכנים אינן מתופעלות או מבוקרות ע"י מערכות ממוחשבות, וכי לא קיימות במפעל מערכות ממוחשבות אשר פגיעה בהן עלולה לגרום לאירוע חומרים מסוכנים.

3. הליך הערכת הסיכונים האמור בסעיף 2 לעיל הסתיים, לרבות עריכת תוצאותיו, ביום _____.

4. ידוע לי כי אם תתווסף מערכת ממוחשבת אשר תנהל או תבקר מערכות המכילות חומרים מסוכנים בעסק, אדרש לבצע הליך הערכת סיכונים מחדש ולפעול בהתאם לממצאי ההליך על פי תנאי היתר הרעלים.

5. הנני מצהיר כי כל האמור אמת.

חתימת המצהיר _____

אישור עו"ד

אני הח"מ, _____, מספר רישיון _____,

_____ מאשר בזה,

כי ביום _____, הופיעה בפניי במשרדי ברחוב _____, מר/גב'

_____ שזיהה/זיהתה עצמו/ה בפני לפי ת"ז: _____ / המוכר/ת לי באופן אישי,

ולאחר שהזהרתי/ה כי עליו/ה להצהיר את האמת, וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, אישר/ה את נכונות ההצהרה הנ"ל וחתם/ה עליה.

תאריך: _____ חתימה וחותמת: _____

הסיכון הוא תמיד פונקציה של ההסתברות והאימפקט:

$$\text{Risk} = f(P, I)$$

I חישוב הנזק = IMPACT מסומן באות

P חישוב הסיכוי להתממשות הנזק (או רמת חשיפה) = Probability מסומן באות

הנזק מחושב לפי **WCS** – WORST CASE SCENARIO

סוגי נזקים:

○ פגיעה בבריאות הציבור עקב התרחישים הבאים:

- פיזור גאזים רעילים – יחושב על פי ערכי PAC
- פוטנציאל לפיצוץ (UVCE) – יחושב על פי ערכי לחץ (הדף) ביחידות BAR
- אפקט דליקה / כדור אש (BLEVE) – יחושב על פי ערכי קרינה יחידות קילוואט למטר רבוע במשך 60 שניות

○ פגיעה בסביבה :

- זיהום מי תהום
- זיהום ים ונחלים
- זיהום קרקעות

טבלת חישוב הנזק

נספח א' במדריך הסייבר לתעשייה

שאלה	1	2	3	4	ציון (1-4)
	הנזק מוערך באחד או יותר מהקריטריונים להלן:				
S (Safety)	1.1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי	1.1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי	1.1. בריאות הציבור: פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 3	1.1. בריאות הציבור: פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 3	
מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב פגיעה בבטיחות המערכת שבבעלות העסק?	2.2. סביבה: ללא פגיעה בסביבה	2.2. סביבה: פוטנציאל לאירוע חומרים מסוכנים שעלול לגרום לפגיעה בסביבה	2.2. סביבה: פוטנציאל לפיצוץ ברמת PAC 2	2.2. סביבה: פוטנציאל לפיצוץ ברמת PAC 2	
C (Confidentiality)			3.3. פוטנציאל לאירוע של 0.28 באר	3.3. פוטנציאל לאירוע של 0.28 באר	
מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב חשיפת מידע על מערכת ממוחשבת המנהלת/מבקרת חומרים מסוכנים שבבעלות העסק?			3.3. פוטנציאל לאירוע של 0.1 באר	3.3. פוטנציאל לאירוע של 0.1 באר	
I (Integrity)			3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	
מהי מידת הנזק שייגרם לבריאות הציבור או לסביבה עקב שיבוש המידע ברכיב התעשייתי או עקב שיבוש התהליך שהרכיב התעשייתי הוא חלק בלתי נפרד ממנו?			3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	
A (Availability)			3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	
מהי מידת הנזק שיגרם לבריאות הציבור או לסביבה עקב השבתת הרכיב התעשייתי או תהליך ממוחשב?			3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	3.3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	

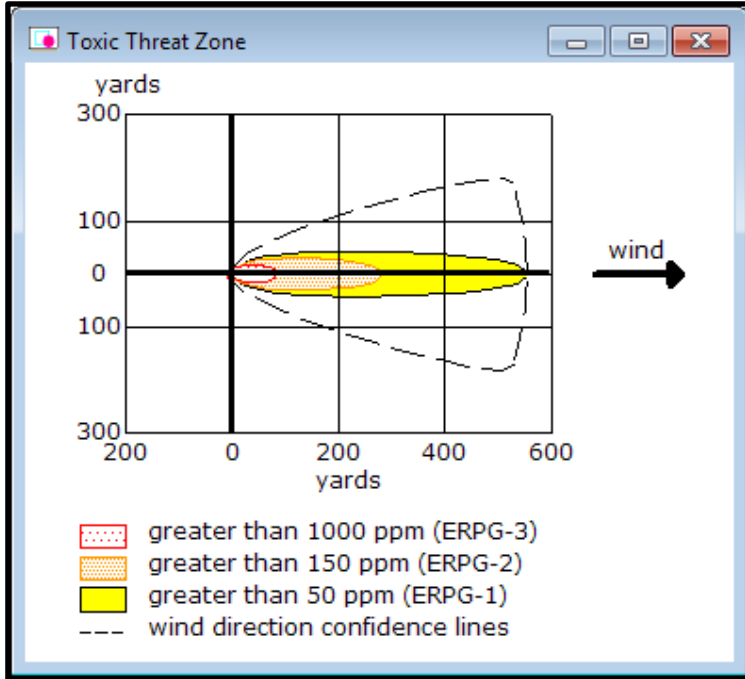
$$I = \text{Max} (1-4) = 1 \text{ to } 4$$

הנתונים לקוחים מתוך חוזר מנכ"ל - מדיניות מרחקי הפרדה במקורות סיכון נייחים - מהדורה מעודכנת
<http://www.sviva.gov.il/subjectsenv/hazardousmaterials/riskmanagement/documents/hm-distance-polcy.pdf>

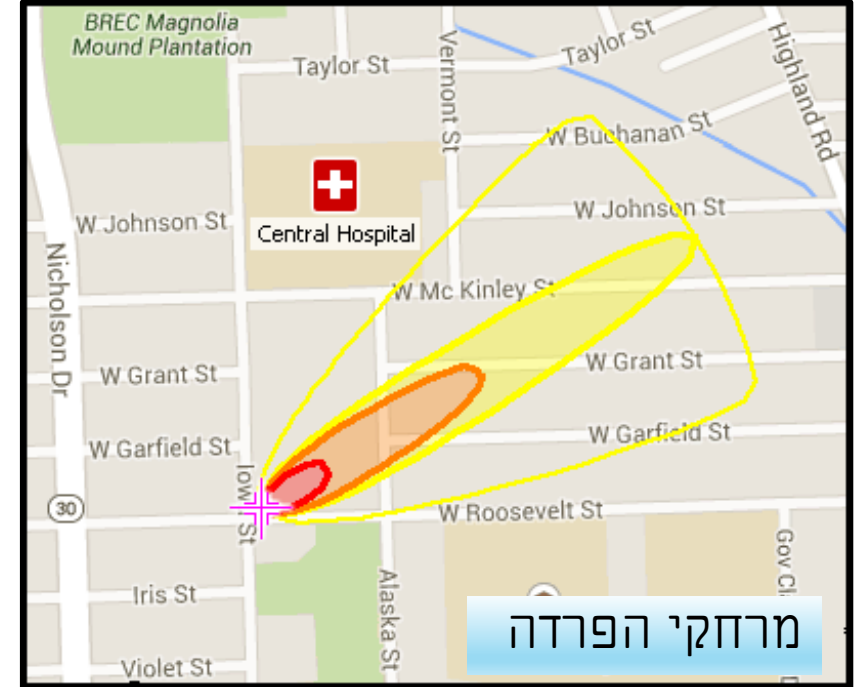


PAC Software

ALOHA 5.4.7



MARPLOT 5.1.1



נתוני INPUT:

- תנאים אטמוספריים: מהירות וכיוון הרוח
- מיקום: נצ מדוייק, כולל גובה מעל פני הים, תכסית, תבליט
- מיכל: צורה, מידות, מצב (שכיבה, עמידה)
- מודל הפיזור: מודל גאוסיאני, גאזים כבדים

ייצוא הנתונים אל המפה



נספח ב' - טבלה לקביעת מידת החשיפה (P) של עסק המחזיק חומרים מסוכנים

בטבלה זו יש לענות על כל 36 השאלות שבעמודת "פרמטר נבדק" על ידי מתן ציון מ-1 עד 4. לאחר מתן ציונים לכל השאלות, יש לחשב את מידת החשיפה על ידי סיכום כל הציונים וחישוב ממוצע לכל הטבלה. התוצאה המתקבלת היא רמת החשיפה – P.

יש לבצע את הניתוח לפי טבלה זו בנוגע לכל התהליך המצוין במיפוי התהליכים המסוכנים ובנוגע לכל מערכת ממוחשבת בכל אחד מתהליכים אלה.

רמת חשיפה / פרמטר נבדק	1	2	3	4	ציון (4-1)
1. מספר עובדים החשופים למערכות אדם-מכונה (HMI) המנהלות/מבקרות חומרים מסוכנים	עד 5	6 - 10	11 - 50	יותר מ-50	
2. מספר עובדים בעלי גישה לבקרים המנהלים/מבקרים מערכת חומרים מסוכנים	עד 10	11 - 25	26 - 50	יותר מ-50	
3. אחריות הטיפול במערכות אדם-מכונה (HMI) רק עובדים פנימיים	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות לגורמים נוספים	
4. אחריות הטיפול בבקרים המשפיעים על מערכת חומרים מסוכנים רק עובדים פנימיים	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות לגורמים נוספים	
5. מספר עמדות אדם-מכונה (HMI) שיש בעסק	1	2 - 5	6 - 10	יותר מ-10	
6. מספר בקרים הקשורים לחומרים מסוכנים בעסק	עד 5	6 - 10	11 - 50	יותר מ-50	
7. תקשורת בין רשת מנהלית לרשת תפעולית	אין – קיים ניתוק פיזי ברמת כבילה בין הרשתות	יש באמצעות חומת אש ודיודה חד-כיוונית	יש באמצעות חומת אש בלבד	יש ללא אמצעי בקרה	
8. האם מתאפשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים?	לא	יש חיבור, אבל בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק	כן, אך עם בקרת חומת אש וסינון תוכן או רכיבי אבטחה נוספים	כן	

חִישׁוּב ההסתברות לאירוע סייבר = PROBABILITY יסומן מעתה באות P

ערך ההסתברות מייצג גם את משטח החשיפה (Attack Surface)

$$P = \text{Average (1-36)} = 1 \text{ to } 4$$



קובץ אקסל לחישוב רמת החשיפה לארוע סייבר (P)

באתר המשרד להגנ"ס :

https://www.gov.il/he/departments/publications/reports/cyber_industrytoxins_permit

ציון	4	3	2	1	רמת חשיפה ← פרמטר נבדק ↓	
1	מעל 50	10-50	5-10	עד 5	מספר עובדים החשופים למערכות אדם-מכונה (HMI) הקשורות לחומרים מסוכנים	1
3	מעל 50	25-50	10-25	עד 10	מספר עובדים בעלי גישה לבקרים המשפיעים על מערכת חומרים מסוכנים	2
2	נגישות גם לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	אחריות הטיפול במערכות אדם - מכונה (HMI)	3
2	נגישות גם לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	אחריות הטיפול בבקרים המשפיעים על מערכת חומרים מסוכנים	4
4	מעל 10	5-10	1-5	1	מספר עמדות אדם – מכונה (HMI) שיש בעסק	5
1	מעל 50	5-10	1-5	1	מספר בקרים הקשורים לחומרים מסוכנים בעסק	6
2	קיימת ללא אמצעי בקרה	קיימת באמצעות חומת אש בלבד	קיימת באמצעות חומת אש ודיודה חד כוונת	לא קיימת	תקשורת בין רשת מנהלית לרשת תפעולית	7
3	ק	ק אך עם בקרת חומת אש וסינון תסק או רכיב אבטחה נוספים	חיבור קיים, אבל בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק	לא	האם מתאפשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים?	8
1	לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	עדכון קושחה בבקרים	9
1	לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	עדכון תוכנה בבקרים ובמערכת ICS נלוות.	10
2	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית למערכות אדם - מכונה (HMI)	11
4	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית לבקרים הקשורים לחומרים מסוכנים	12
4	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית לרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)	13

ציון החשיפה לכל נכס הינו הציון הממוצע שהתקבל ל-36 השאלות

$$P = \text{Average (1-36)}$$

שלב 2 - ביצוע סקר סיכונים: חישוב הסיכון

1	2	3	4	רמת נזק (I) הסתברות (P)
7	10	13	16	4
6	9	12	15	3
5	8	11	14	2
4	7	10	13	1

$$\text{Risk} = P + 3 * I$$
 INCD (Israel National Cyber Directorate)

שאלה	1	2	3	4	ציון (1-4)
S (Safety) מיד מידת הפגיעה ללא מניעה או סכנה ששולטת בסיכונים שניתנת במצבא כבעלת תפקיד	1. כריאות הציבור: ללא מניעה ציבורי	1. כריאות הציבור: ללא מניעה ציבורי	1. כריאות הציבור: ללא מניעה ציבורי	1. כריאות הציבור: ללא מניעה ציבורי	S (Safety)
C (Confidentiality) מיד מידת הפגיעה ללא מניעה או סכנה ששולטת בסיכונים שניתנת במצבא כבעלת תפקיד	2. סביבה: ללא מניעה	2. סביבה: ללא מניעה	2. סביבה: ללא מניעה	2. סביבה: ללא מניעה	C (Confidentiality)
I (Integrity) מיד מידת הפגיעה ללא מניעה או סכנה ששולטת בסיכונים שניתנת במצבא כבעלת תפקיד	3. כריאות הציבור: ללא מניעה ציבורי	3. כריאות הציבור: ללא מניעה ציבורי	3. כריאות הציבור: ללא מניעה ציבורי	3. כריאות הציבור: ללא מניעה ציבורי	I (Integrity)
A (Availability) מיד מידת הפגיעה ללא מניעה או סכנה ששולטת בסיכונים שניתנת במצבא כבעלת תפקיד	4. כריאות הציבור: ללא מניעה ציבורי	4. כריאות הציבור: ללא מניעה ציבורי	4. כריאות הציבור: ללא מניעה ציבורי	4. כריאות הציבור: ללא מניעה ציבורי	A (Availability)
ציון					Max(1-4)
שם הבודק	תפקיד	תאריך	ציון	חתימה	

רמת חשיפה < V	1	2	3	4	ציון (1-4)
1. מספר עובדים החשופים למערכות אדם-מכונה (HMI) הקשורות לחומרים	עד 5	6-10	11-50	מעל 50	
2. מספר עובדים לוקרים המשפיעים על מערכת חומרים	עד 10	11-25	26-50	מעל 50	
3. אחריות במערכות אדם-מכונה (HMI)	רק עובדים פנימיים	קבועים חיצוניים	ספקים חיצוניים מודדמים	ספקים חיצוניים מודדמים	נגישות גם לזרים
4. אחריות בקבצים המשפיעים על מערכת חומרים	רק עובדים פנימיים	קבועים חיצוניים	ספקים חיצוניים מודדמים	ספקים חיצוניים מודדמים	נגישות גם לזרים
5. מספר עבודות אדם-מכונה (HMI) הקיימות במפעל	1	2-5	6-10	מעל 10	
6. מספר בקרים חשופים לחומרים במפעל	עד 5	6-10	11-50	מעל 50	

חישוב רמת הסיכון של המערכת

$P + 3 * I$	$P * I$	ערך הסתברות P	ערך אימפקט I
4	1	1	1
5	2	2	1
6	3	3	1
7	4	4	1
7	2	1	2
8	4	2	2
9	6	3	2
10	8	4	2
10	3	1	3
11	6	2	3
12	9	3	3
13	12	4	3
13	4	1	4
14	8	2	4
15	12	3	4
16	16	4	4

$P * I$ vs $P + 3 * I$

איזה בקרות להטמיע ?

נתון: נניח שקיבלנו בחישובים $P=2.6$, $I=3$

חישוב הסיכון: $RISK = P + 3*I = 2.6 + 3*3 = 11.6$
מעגלים כלפי מעלה - Risk = 12

הערה: קיימת אופציה לנסות להוריד את רמת החשיפה P ולהגיע לרמה יותר נמוכה

אם $RISK=12$ אנו בחבילת בקרות 3

כמות בקרות להטמעה: 81

יתכן שחלק מהבקרות כבר קיימות נניח 50

יש להטמיע את הדלתא: $81-50 = 31$

יש לנו 31 בקרות להטמעה

הערה: במידה ובקרה מסויימת קשה להטמעה מבחינת לוחות זמנים, עלויות, חוסר במשאבים אחרים על העסק להציע בקרה מפצה אשר נותנת מענה ראשוני עד להטמעה מלאה של הבקרה הנדרשת - כל זאת באישור יחידת הסייבר בתעשייה

פוטנציאל הסיכון	חבילת הבקרות בהתאם לפוטנציאל הסיכון	כמות הבקרות לחבילה זו
4-7	1	41
8-11	2	59
12-14	3	81
15-16	4	92



קביעת רשימת הבקורות להטמעה

רשימת הבקורות

מס' הבקורות בפרק זה	בדיקה	רמה	המלצות / הערות	פירוט	בקרה נדרשת	סעיף
3	1.1 האם בוצע מיפוי חומרים מסוכנים. 1.2 האם בוצע מיפוי מערכות המחשוב והבקרה.	1	1.2 ב. מומלץ להיוועץ באנשי מקצוע בתחום החומים על מנת לברר אם מערכת ממוחשבת שאינה מטפלת בחומרים אבל עשויה להתלקח או להתפוצץ עקב התקפת סייבר (למשל דוד קיטור בעל בקר מתוכנת) - מסכנת חומרים בסביבתה.	1.2 המיפוי יכול: רשימת המחשבים - בציון תפקידים והמערכות המותקנות עליהם לצורך תפקידים; עמדות HMI/אוטומציה/ייעודיות/משולבות מכונה - בציון דגם וגרסת תוכנה; בקרים ומרכזות גלאים - בציון דגם, גרסת קושחה/תוכנה וסוג התקשורת (Ethernet, WiFi, טלפון, אחר); רכיבי IoT/IIoT ונלאים בציון דגם, מקום וסוג התקשורת אליהם; רכיבי הרשת (מתנים, נתבים, נקודות גישה אלחוטיות, חומת אש) בציון דגם וחיבורם לרשתות אחרות/אינטרנט.	מיפוי מערכות וכתובת מדיניות אבטחת מידע למערכות מחשוב ובקרת חומ"ס 1.1 בעל העסק יבצע מיפוי כל החומרים המסוכנים אשר מטופלים במערכות ממוחשבות. 1.2 בעל העסק יבצע מיפוי כל מערכות המחשוב, הרשת, הבקרה, החישה והאוטומציה בעסק ואלה הן: א. הנוגעות לאחסון, שימוש, זרימה, ייצור, שינוע, השמדה וגילוי חריגות ודליפות של חומרים מסוכנים. ב. העוללות לגרום או לתרום לפריצת חומרים מסוכנים בפעולה זדונית או לא תקינה בהם. ג. הנוגעות לרישום מלאי ולוגיסטיקה של חומרים מסוכנים.	1
1	1.6 הבדיקה מספק.	4			בדיקת חדרות (Penetration Test) 1.6 יש לבצע אחת לשנתיים בדיקת חדרות בעזרת מומחה אבטחת מידע, אשר תכלול לפחות: א. בדיקת עמידות מערכות המחשוב ובקרת החומרים להתקפה מחוץ לעסק. ב. בדיקת עמידות מערכות המחשוב ובקרת החומרים להתקפה מרשת ה-IT בעסק. ג. בדיקת עמידות מערכות המחשוב ובקרת החומרים לתוקף בעל גישה פיזית לעמדות תפעול ולארונות התקשורת והבקרים.	1



נספח ג' במדריך הסייבר לתעשייה

פוטנציאל הסיכון	חבילת הבקורות בהתאם לפוטנציאל הסיכון	כמות הבקורות לחבילה זו
4-7	1	41
8-11	2	59
12-14	3	81
15-16	4	92

במדריך סייבר 2.0 עלו מספר הבקורות ל-99 בקורות



נספח ז' - תצהיר בעל היתר הרעלים אודות ביצוע הערכת סיכוני סייבר וסיווג העסק

אני החתום מטה, _____, מס' זהות _____, לאחר שהזרתי כי עליו לומר את כל האמת, וכי אם לא אעשה כן אהיה צפוי לעונשים הקבועים בחוק, מצהיר בזה לאמור:

1. החז"מ משמש כ- _____, בעבור _____ (שם העסק), מס' היתר רעלים _____.
2. תהליך סיווג העסק בעניין הגנת סייבר הסתיים ביום _____.
3. מצורף בזאת מסמך המפרט את עיקרי תוצאות הליך הסיווג של העסק והערכת סיכוני סייבר.
4. ערכתי בעצמי/נעזרתי בשירותי חברת ייעוץ _____ (מחק את המיותר) את הערכת הסיכונים ואת מסמך עיקרי תוצאות הליך סיווג העסק והערכת הסיכונים, ולמיטב ידיעתי והבנתי מסמכים אלה הם מלאים, שלמים ונכונים, ונערכו לפי מסמך ההנחיות, ומציגים תמונת מצב מדויקת של העסק.
5. תהליך הערכת סיכונים ועריכת תוצאותיו בעניין הגנת סייבר הסתיימו ביום _____.
6. להלן תקציר תוצאות הערכת סיכונים:

שם המערכת	רמת החשיפה (4-1)	רמת הנזק (4-1)	רמת הסיכון	חבילת בקורות להנמעה (4-1)

7. ערכתי בעצמי/בדקתי (מחק את המיותר) את טבלת תקציר הערכת סיכונים המוגש למשרד להגנת הסביבה כנדרש בהנחיות, ולמיטב ידיעתי והבנתי התקציר מלא, שלם ונכון ומציג תמונת מצב מדויקת של העסק.

8. הנני מצהיר כי כל האמור אמת. חתימת המצהיר: _____

אישור ע"ד

אני החתום מטה _____ עורך דין, מאשר בזה כי ביום _____ הופיע לפני _____ המוכר לי אישית/ שזיהיתו על פי תעודת זהות מס' _____ ולאחר שהזרתי כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר נכונות הצהרתו לעיל וחתם עליה בפני:

חתימה וחותמת: _____

מילוי טבלה בנספח ז'

- ✓ שם המערכת
- ✓ רמת חשיפה P
- ✓ רמת הנזק ו
- ✓ רמת הסיכון
- ✓ חבילת בקורות להטמעה

יש להגיש למשרד נספח ז' חתום תוך שנה



<http://www.robi-steiner.co.il/why-there-is-a-gap>

שלב 3 – ביצוע אנליזת פערים

בשלב זה יש לבצע אנליזת פערים (GAP ANALYSIS)

- ✓ מניהול הסיכונים, ידוע לנו איזה בקרות נדרשות
- ✓ יש לבצע השוואה מול הבקרות הקיימות
- ✓ יש לכתוב מסמך המתאר את אנליזת הפערים

מסמך אנליזת פערים – נשאר במפעל לביקורת עתידית



<https://www.pexels.com/>

שלב 4 – תכנית עבודה

בשלב זה יש לכתוב תכנית עבודה

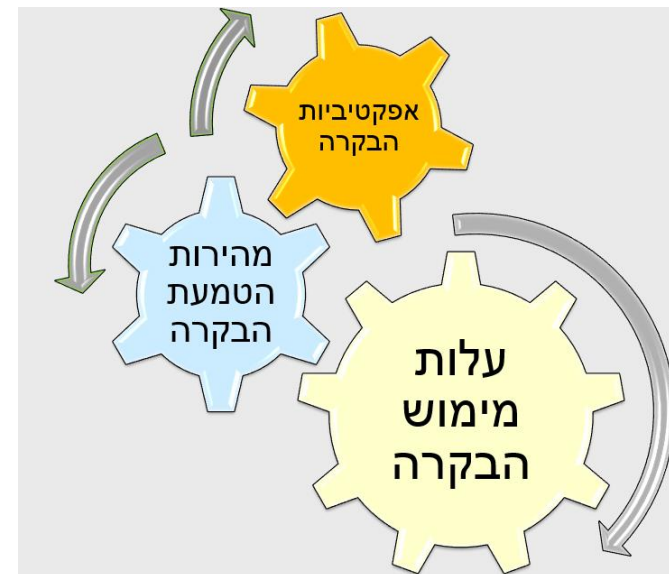
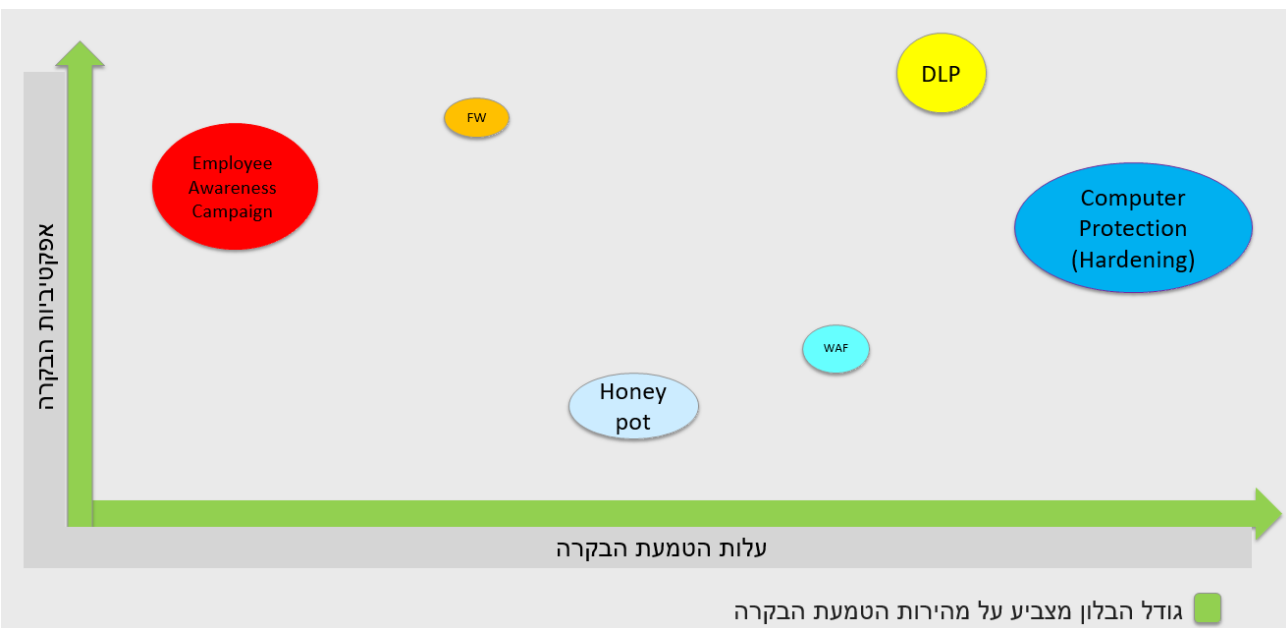
מומלץ כי תכנית העבודה תכלול את הדברים הבאים:

- ✓ שם המערכת
- ✓ בקרות נדרשות להטמעה על פי תכנית מיפוי פערים
- ✓ פירוט שלבי ביצוע להטמעת כל בקרה ובקרה
- ✓ אחראי ביצוע לכל בקרה ובקרה
- ✓ משאבים נדרשים לכל בקרה ובקרה
- ✓ לוח לסיים כל בקרה ובקרה
- ✓ נושאים נוספים לפי שיקול דעת העסק

מסמך תכנית העבודה – נשאר במפעל לביקורת עתידית

שלב 5 – ביצוע תכנית עבודה

המשאבים בארגון מצומצמים – במה לטפל קודם???



שלב 5 – סיום ביצוע תכנית עבודה

נספח ח' - תצהיר בעל היתר רעלים על השלמת תוכנית למזעור סיכוני הסייבר

אני החתום מטה _____, מס' זהות _____, לאחר שהוזהרתי כי עלי לומר את כל האמת, וכי אם לא אעשה כן אהיה צפוי לעונשים הקבועים בחוק, מצהיר בזה לאמור:

1. הח"מ משמש כמנהל כללי / בעלים (מחק את המיותר), עבור _____ (שם המפעל), מס' היתר רעלים _____.

2. תהליך יישום תוכנית למניעת הסיכון לבריאות הציבור ולסביבה עקב אירוע סייבר, הושלם ביום _____.

3. להלן תקציר הטמעת בקורות למזעור סיכוני סייבר:

שם המערכת	חבילת בקורות נדרשת (4-1)	רשימת הבקורות שהוטמנו	הערות

4. בדקתי את מסמך הסיכום המוגש למשרד להגנת הסביבה כנדרש בהנחיות, ולמיטב ידיעתי והבנתי המסמך מלא, שלם ונכון.

5. הנני מצהיר כי כל האמור אמת. חתימת המצהיר: _____.

אישור עו"ד

אני החתום מטה _____ עורך דין, מאשר בזה כי ביום _____ הופיע לפני _____ המוכר לי אישית / שזיהיתיו על פי תעודת זהות מס' _____ ולאחר שהוזהרתי כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר נכונות הצהרתו לעיל וחתם עליה בפני:

_____ חתימה וחותמת:

סיום תכנית העבודה:

- ✓ מילוי נספח ח' במדריך הסייבר
- ✓ שם מערכת
- ✓ חבית בקורות נדרשת
- ✓ רשימת הבקורות שהוטמנו

שלב 6 בקרה וניטור



<https://www.pexels.com/>

לאורך כל התהליך יש לבצע בקרה וניטור על:

- ✓ שלבי התהליך
- ✓ סיום כל שלב ושלב בלויז
- ✓ מילוי דרישות הרגולטור:
 - מינוי ממונה הגנת סייבר
 - השלמת מסמך מדיניות הנהלה
 - תצהיר לסיום סקר סיכונים
 - תצהיר לסיום הטמעת בקרות.

הנחיות למבחן :

- המבחן בנוי מ 20 שאלות אמריקאיות שלכל שאלה תשובה אחת נכונה בלבד. משקל כל שאלה 5 נקודות.
- המבחן יועבר בלינק לכולכם דרך הצי'אט אותו יש לפתוח באקספלורר (פתיחת הלינק בכרום קצת משבש ולכן מומלץ ועדיף לפתוח באקספלורר)
- המבחן עם מצלמות פתוחות ומיקרופונים סגורים, אין להתייעץ אחד עם השני בשעת המבחן, מותר להיעזר בכל חומר כתוב כולל מצגות ואינטרנט.
- לאורך כל המבחן ניתן לשאול שאלות בצי'ט ויוסי יענה.
- קבלת תעודות גמר - ישירות מהתאחדות התעשיינים למייל האישי שלכם



