תהליך ה ו BCP ו DRP בניהול סיכוני סייבר

Business Continuity Plan - BCP - המשכיות עסקית בעולם אבטחת המידע

Data Recovery Plan – DRP

ד"ר מיכאל טיבין

המכללה האקדמית רמת גן

התקפה על נמל אשדוד

יו"ר נמל אשדוד: "בתחילת הלחימה ספגנו 134 אלף תקיפות סייבר בחודש"

שאול שניידר סיפר בוועידת "האנשים של המדינה" של ynet ו"ידיעות אחרונות" על אתגרי המלחמה, על העומס בעקבות תקיפות החות'ים שהשביתו את נמל אילת, וגם השותפות עם מערכת הביטחון והזינוק הכלכלי המפתיע של הנמל: "התמודדנו עם ירי, סגרנו פערים, והשקענו בסטארט-אפים ישראליים"

שרון כידון | 07.04.25 | 17:15

קישור לכתבה

המכללה האקדמית רמת גן

שינוי הפרדיגמה: מ-11 בספטמבר ועד היום

הפרדיגמה החדשה: ארכיטקטורה מבוזרת

פיזור גיאוגרפי נרחב של טכנולוגיה והון אנושי (לקחי קריסת התאומים).

תלויות הדדיות חוצות-מגזרים (תקשורת, חשמל, תחבורה).

ההבנה: אי אפשר לסמוך על ניידות עובדים לאתר חלופי סמוך.

התפיסה הישנה (עד 2001): הצלת המבנה

ריכוז משאבים במיקום אחד מטעמי יעילות.

הנחת העבודה: אסון יפגע רק במערכות, לא בסביבה כולה.

תלות מוחלטת בתשתיות מקומיות.

המכללה האקדמית רמת גן

BCP – Business Continuity Planning

https://www.youtube.com/watch?v=cxE940f7iq0

המכללה
האקדמית
רמת גן

מהו BCP בעולם הסייבר?

רציפות עסקית

תהליך המבטיח המשך פעילות ארגונית גם תחת התקפות סייבר . מאפשר התאוששות מהירה מאירועי אבטחה.

תכנון מקדים

מניעת קריסה ארגונית דרך הכנה מראש .זיהוי נקודות כשל אפשריות ופיתוח מענה יעיל.

מענה למצבי חירום

פרוטוקולים מוגדרים לטיפול באירועי סייבר .תגובה מהירה ואפקטיבית להפחתת נזקים.

המכללה האקדמית רמת גן

BCP .....

- פתרונות BCP – BUSINESS CONTINUITY PLANNING – תכנון המשכיות עסקית, נועדו להבטיח שארגון יוכל להמשיך לתפקד גם בעת משבר – כגון מתקפת סייבר, תקלה טכנולוגית, אסון טבע או מגפה.
- לפעמים גם – מתחרים, שינוי בהתנהגות לקוחות, לפעמים שינוי טכנולוגיות לפי תעדוף לקוחות
- אירועים טבעיים – הוריקנים, גלי חום ממושכים, הפסקות חשמל (לא יזומות), פריצות למטרת כופר או סחר במידע.

המכללה האקדמית רמת גן

למה המשכיות עסקית חשובה .....

- רוב העסקים יכולים לעמוד בהאטה או עצירה של הפעילות העסקית שלהם לפרק זמן קצר, אם כי בנקים, שירותי תשתיות, ספקי שירותי בריאות וחברות בתעשיות אחרות אינם זוכים למותרות האלה וחייבים לעמוד בדרישות החוק ולהבטיח שהם יכולים לחדש את הפעילות הרגילה כמעט מייד לאחר הפרעה.

- ברוב המקרים, ללא קשר לדרישות הרגולטוריות, עסקים לא יכולים להרשות לעצמם הפרעה ממושכת לפעילותם, כי אפילו הלקוחות הסבלניים ביותר בסופו של דבר ימצאו ספקים חלופיים. למעשה, אירוע זמן השבתה ממושך אצל מתחרה יכול להעניק לשחקנים אחרים במגזר הזדמנות להשיג נתח שוק.

"מה קרה בשעה 12:33?": ספרד חוקרת את הסיבה להפסקת החשמל העצומה

אחרי יממה של כאוס, ספרד ופורטוגל מנסות להתאושש מהפסקת החשמל הגדולה בתולדותיהן – וחוקרות את נסיבות התקלה החריגה. חברת החשמל של ספרד שללה אפשרות של מתקפת סייבר – אך בית המשפט העליון בודק גם אפשרות של חבלה. "אנחנו לא פוסלים אף תרחיש", אמר ראש הממשלה סנצ'ס. במדינה טוענים שהתלות הגדולה באנרגיה מתחדשת הובילה לקריסת החשמל – בתוך 5 שניות

ynet והסוכנויות | 29.04.25 | 18:52

המכללה האקדמית רמת גן

מה כלול בהמשכיות עסקית ?

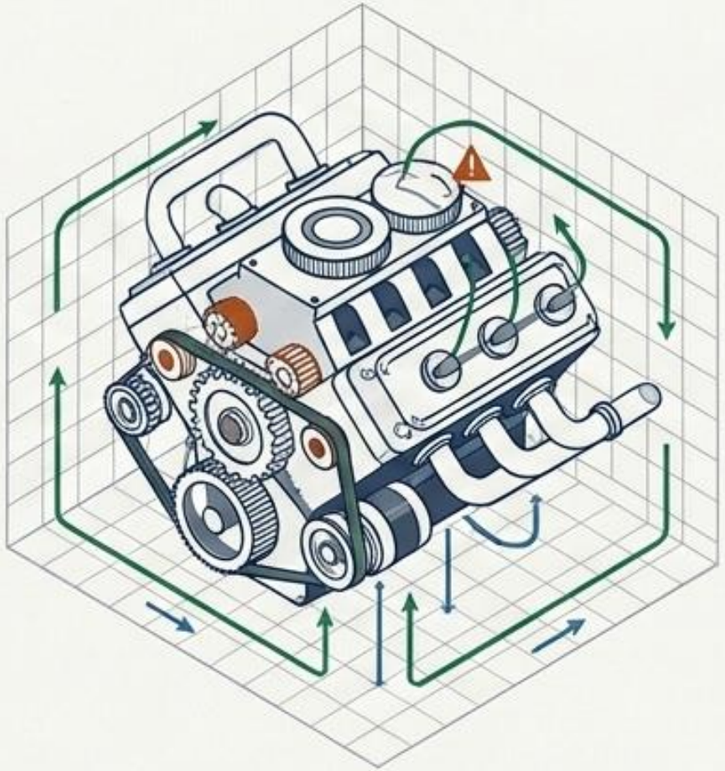
- המשכיות עסקית כוללת את המרכיבים הבאים:

- הערכת פונקציות כגון ייצור, שירות לקוחות, מכירות ושיווק ודירוגן לפי סדר עדיפויות. במקרה חירום
- ייתכן שהארגון שלכם לא יוכל להפעיל את כל הפונקציות שלו באופן מיידי, ולכן, הידעה אילו מהן קריטיות ביותר להצלחתו היא חיוני כדי שיצליח לשרוד את הדקות, השעות והימים הראשונים.
- הערכת יכולת ההסתגלות והגמישות של ספקים וספקי שירות מרכזיים. ודאו שיש להם תוכניות המשכיות עסקית משלהם, ובמקרה של ספקי IT, שיש להם יתירות, שעתוק נתונים ותהליכים אחרים להתאוששות מאסון כדי להבטיח שהעסק שלכם לא יסבול משיבושים בפעילויות שלהם.
- וידוא שהעסק עומד בסטנדרטים מקומיים, לאומיים ובינלאומיים רלוונטיים. זה חשוב במיוחד במגזרי הכספים, הבריאות והתשיות

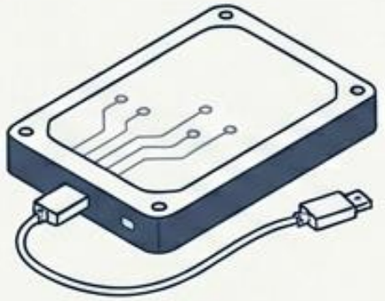
המכללה
האקדמית
רמת גן

אשליית הגיבוי

המציאות: גיבוי אומר שיש לכם עותק של המידע. DRP אומר שאתם יודעים בדיוק מה לעשות כשהכל קורס.



מיתוס מסוכן: יש לנו גיבוי למידע, אנחנו מוגנים.



המחיר של חוסר מוכנות:

93%

מהחברות שמאבדות את מרכז הנתונים שלהן ל-10 ימים פושטות רגל בתוך שנה.

40%

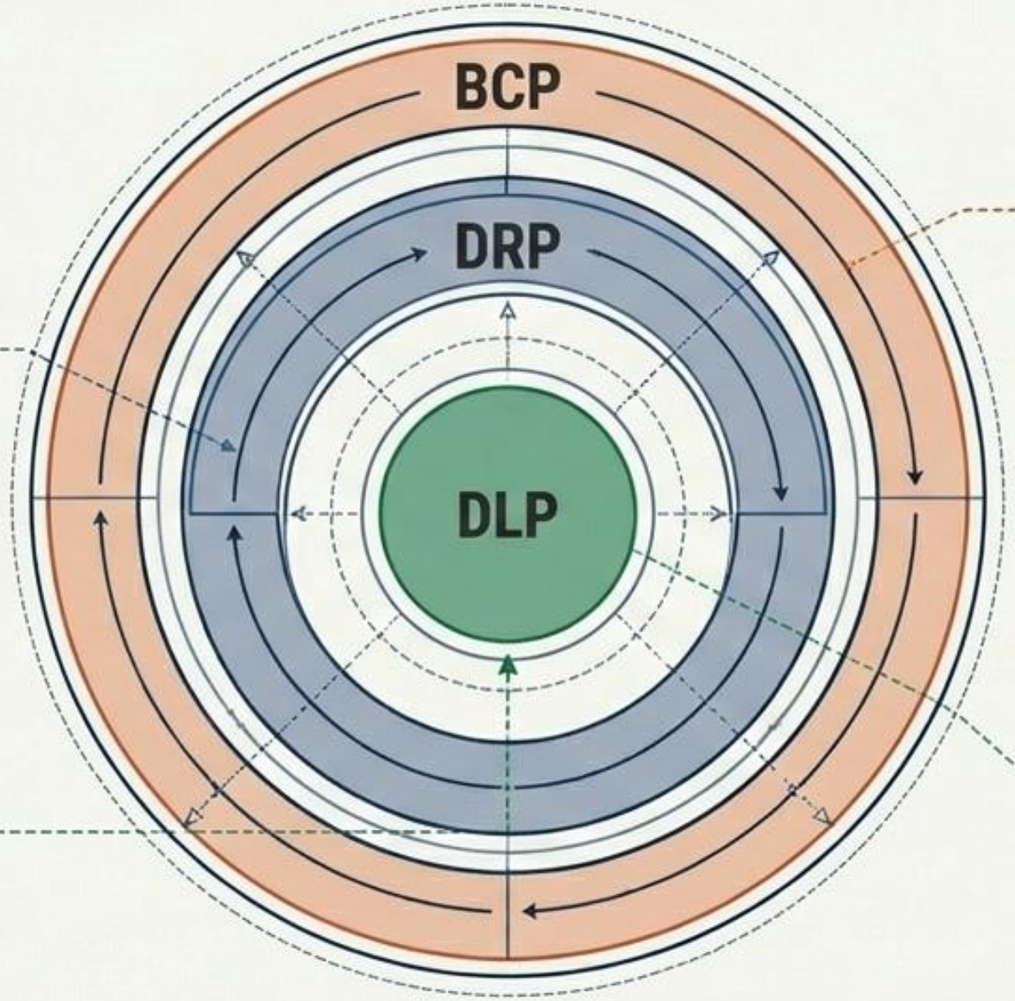
מהעסקים נסגרים לחלוטין בתוך 5 שנים לאחר אסון.

הבדל של שעות בין שחזור מוצלח לשיתוק עסקי מוחלט.

שילוש ההגנה: אנטומיה של חוסן

המשכיות עסקית - המעטפת:
המיקוד הוא בארגון כולו.
כוח אדם, מיקום פיזי,
פיזי, תקשורת עם לקוחות,
וספקי משנה.

התאוששות מאסון - המנוע:
המיקוד הוא בטכנולוגיה.
שחזור מערכות ה-IT, שרתים,
ותשתיות הרשת.



מניעת דליפת מידע - הליבה:
המיקוד הוא בנתונים. יצירת
סביבה של Secure Data –
הגנה על מידע רגיש בעת
לאתריים וגישה מרחוק.

מניעת דליפת מידע - הליבה:
המיקוד הוא בנתונים יצירת
Secure Data Movement –
הגנה על מידע רגיש בעת מעבר
לאתרי חירום וגישה מרחוק.

המכללה
האקדמית
רמת גן

מחזור החיים של מצב חירום

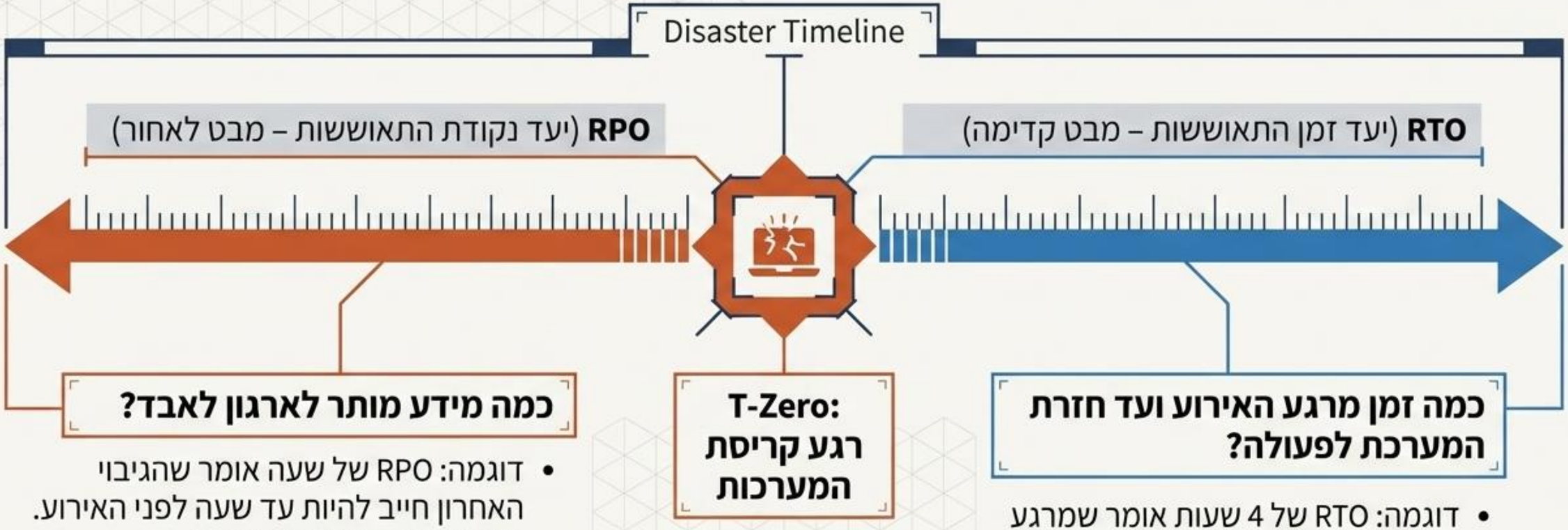
1. שגרה (Routine)
ביצוע פעולות הכנה, תרגולים עתיים, ויצירת מיומנות. המערכות עובדות כסדרן.

2. מעבר לחירום (Transition)
הערכת מצב, הפעלת צוות משבר, הכרזה רשמית על מצב חירום, והחלטה על הפעלת אתר ה-DRP.

3. חירום (Emergency)
ניהול פעילות במתכונת מיוחדת, העברת משתמשים לאתר חלופי, עבודה תחת שיבושים.

4. חזרה לשגרה (Recovery)
שיקום התשתיות הפיזיות, בדיקת תקינות בסביבת הייצור, והחזרת הפעילות באופן מדורג ומבוקר.

מדדי הזהב: RPO מול RTO



- דוגמה: RPO של שעה אומר שהגיבוי האחרון חייב להיות עד שעה לפני האירוע. מעבר לכך – נזק בלתי הפיך.

- דוגמה: RTO של 4 שעות אומר שמרגע האסון, יש חלון של 4 שעות להחזיר את הארגון לאוויר.

המכללה האקדמית רמת גן

אסטרטגיית אתר חלופי:
מטריצת החלטות

סוג אתר	זמן התאוששות (RTO)	עלות	שימוש אידיאלי
אתר חם (Hot Site)	דקות עד שעה	גבוהה מאוד	מערכות קריטיות, בנקים, תשתיות לאומיות הפועלות 24/7 (שכפול בזמן אמת).
אתר חמים (Warm Site)	מספר שעות	בינונית	המודל המומלץ לרוב העסקים. תשתיית קיימת, מצריכה הפעלה וטעינת נתונים.
אתר קר (Cold Site)	ימים עד שבועות	נמוכה	שטח פיזי עם חשמל ורשת, ללא שרתים. מיועד למערכות לא קריטיות או כגיבוי של גיבוי.

הפיזיקה של השכפול:
מגבלות המרחק

שכפול סינכרוני (Synchronous):

- המידע נכתב בשני האתרים במקביל. כתיבה לא מאושרת עד ששני האתרים התעדכנו.
- **היתרון:** אפס אובדן נתונים.

⚠ **החיסרון:** מוגבל על ידי הפיזיקה (מהירות האור / Latency). מחייב מרחק פיזי קצר בין האתרים – חושף את הארגון לאסון אזורי.

שכפול אסינכרוני (Asynchronous):

- המידע מאושר מיד, והשכפול לאתר המרוחק מתבצע ברקע.

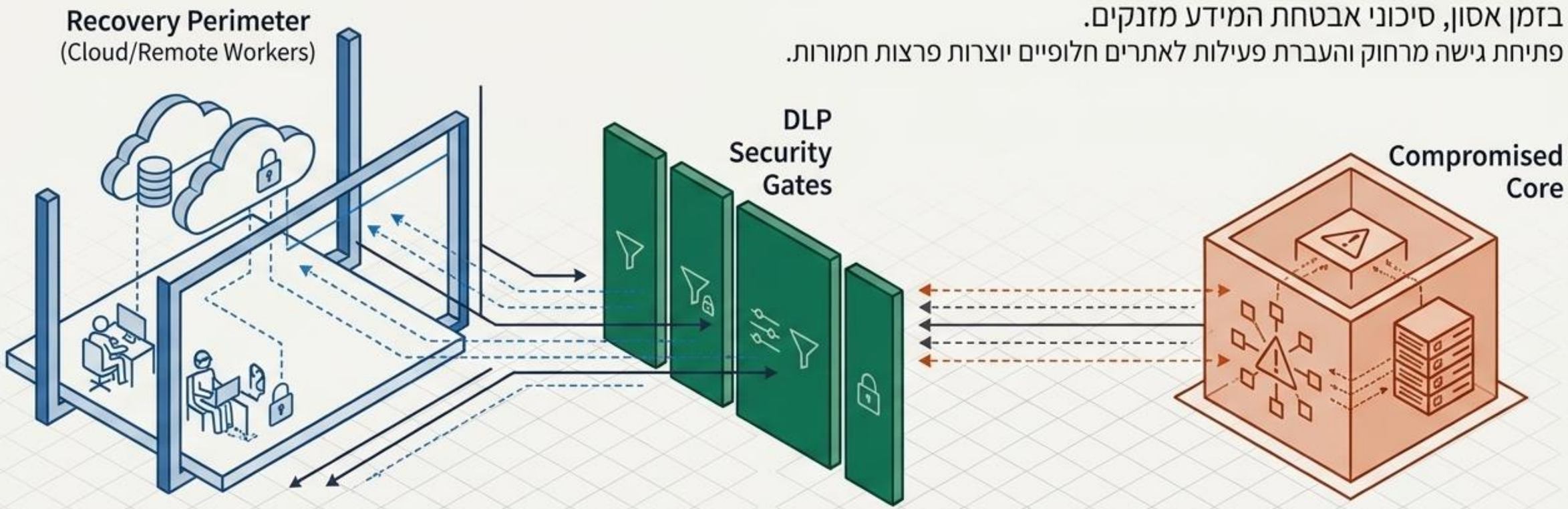
היתרון: מאפשר פיזור גיאוגרפי אמיתי (מאות קילומטרים), חיוני לעמידות בפני אסונות רחבי היקף.

⚠ **החיסרון:** יוצר פער זמן קקטן (RPO גדול מאפס) המהווה סיכון לאובדן חלקיק נתונים.

המכללה האקדמית רמת גן

תנועת נתונים מאובטחת (Secure Data Movement)

בזמן אסון, סיכוני אבטחת המידע מזנקים.
פתיחת גישה מרחוק והעברת פעילות לאתרים חלופיים יוצרות פרצות חמורות.



שילוב DLP בתוכנית ההתאוששות:

ניטור בזמן אמת: שליטה
על העתקת מידע לכונני USB, הדפסות ושימוש בלוח הגזירים (Clipboard) בעת עבודה מאתר חלופי או מהבית.

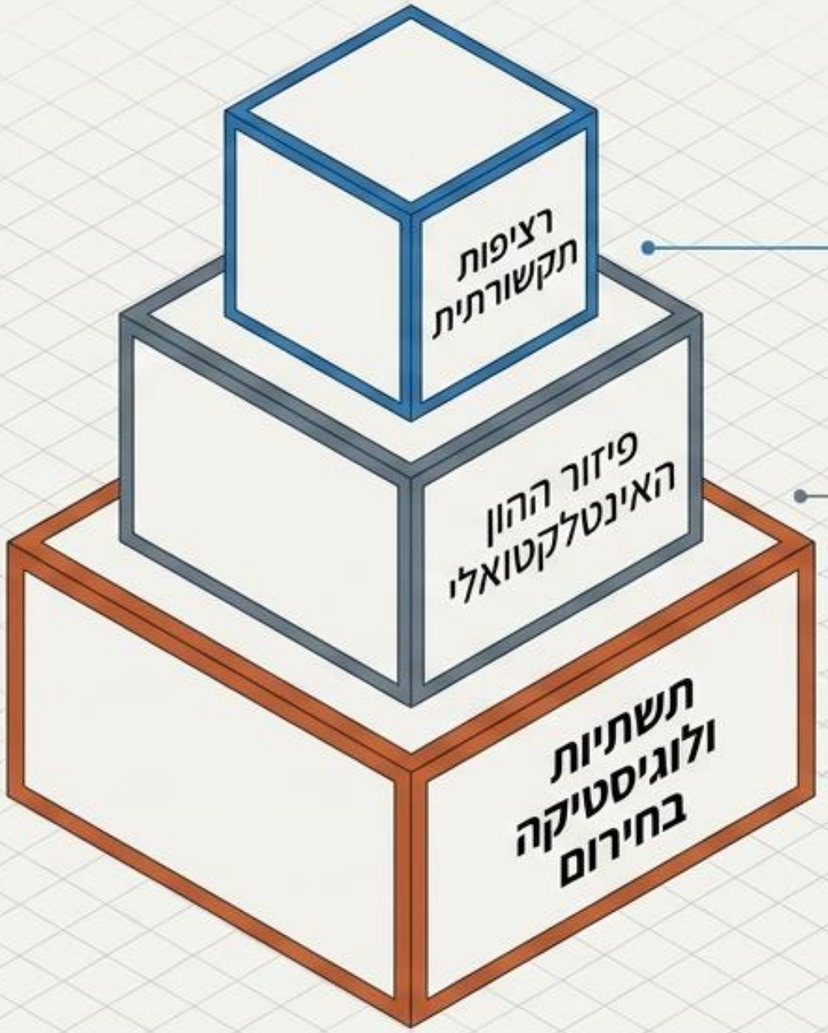
הגנה על רשומות (PII/PHI):
מניעת זליגת מידע אישי ופיננסי גם מחוץ לרשת הארגונית השגרתית.

אכיפת מדיניות אוטומטית:
סיווג רגישות המידע חוסם דליפה החוצה, בלי לעצור את עבודת השיקום.

המכללה
האקדמית
רמת גן

הגורם האנושי המוזנח

תוכנית התאוששות מושלמת קורסת אם למהנדס הראשי אין היכן לישון או תקשורת לעבוד איתה.



תולות מוחלטת ברשתות סלולר ציבוריות מהווה סיכון. יש להגדיר חלופות לזיפות קריסה (למשל, תקשורת לוויינית או קווי עדיפות TSP).

האם הארגון שמר את כל הידע בבניין אחד? חובה לפזר מנהלים ואנשי מפתח גיאוגרפית כדי למנוע נקודת כשל אנושית יחידה.

במקרה של אסון אזורי, היכן הצוות יישן? מה יאכל? כיצד יגיע לאתר החלופי כשדרכי התחבורה חסומות?

ניתוח השפעה עסקית (BIA):
עקרון הטריאז'

לא ניתן להציל הכל מיד. ה-BIA הוא תהליך התיעדוף העליון שקובע שקובע מה חוזר לאוויר ראשון.

פה כפנסטת
תהליכיים כיעוה ההטטראז'

הערכת משמעויות: כימות הנזק מכל דקת השבתה (אובדן הכנסה, קנסות רגולטוריים, פגיעה אנושה במוניטין).

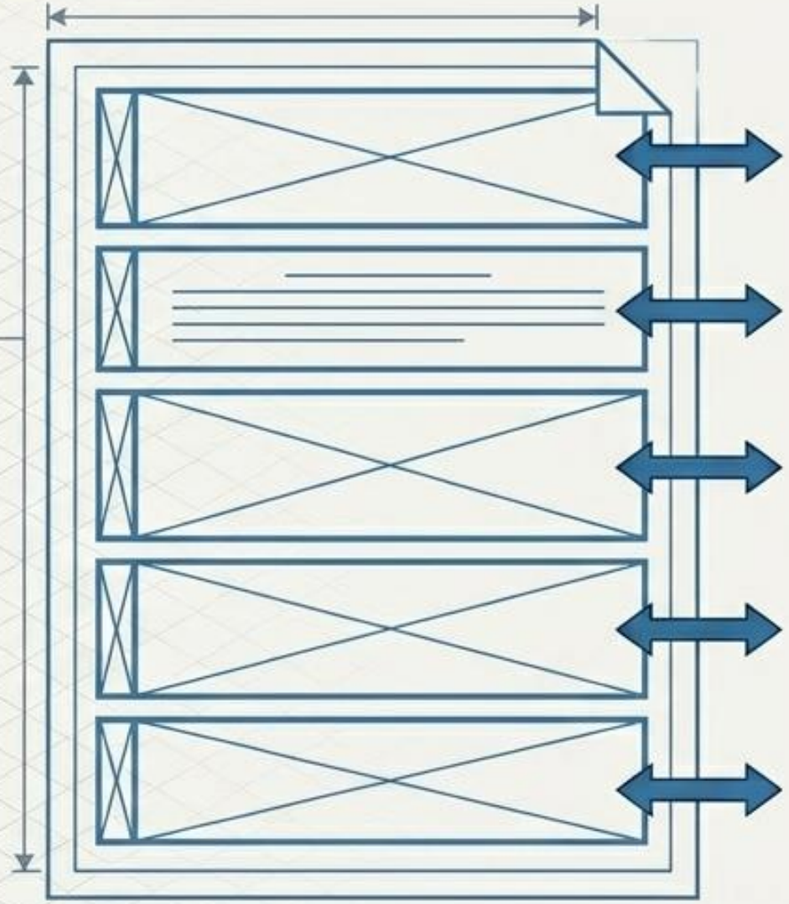
מיפוי תלויות (Top-Down):
זיהוי שרשרת האספקה קריטית – מערכות מידע, מבנים פיזיים, ספקי צד ג' וכוח אדם הכרחי לכל תהליך שסומן כקריטי.

מיפוי תהליכים:
זיהוי כלל הפעילויות בארגון ותעדוף מחמיר (מכירות, ייצור, כספים).

המכללה האקדמית רמת גן

ארכיטקטורת תיק ההפעלה (Runbook)

ה-Runbook הוא הלב הפועם של אסטרטגיית ה-DRP.
עליו להיות מדריך צעד-אחר-צעד חסין פאניקה.



אימות קריטריונים להפעלת
נוהל אסון.

עץ תקשורת ושרשרת
פיקוד מוגדרת מראש.

בידוד מערכות פגועות
(קריטי באירועי סייבר/כופרה).

סדר שחזור מדויק למערכות
קריטיות (לפי RTO).

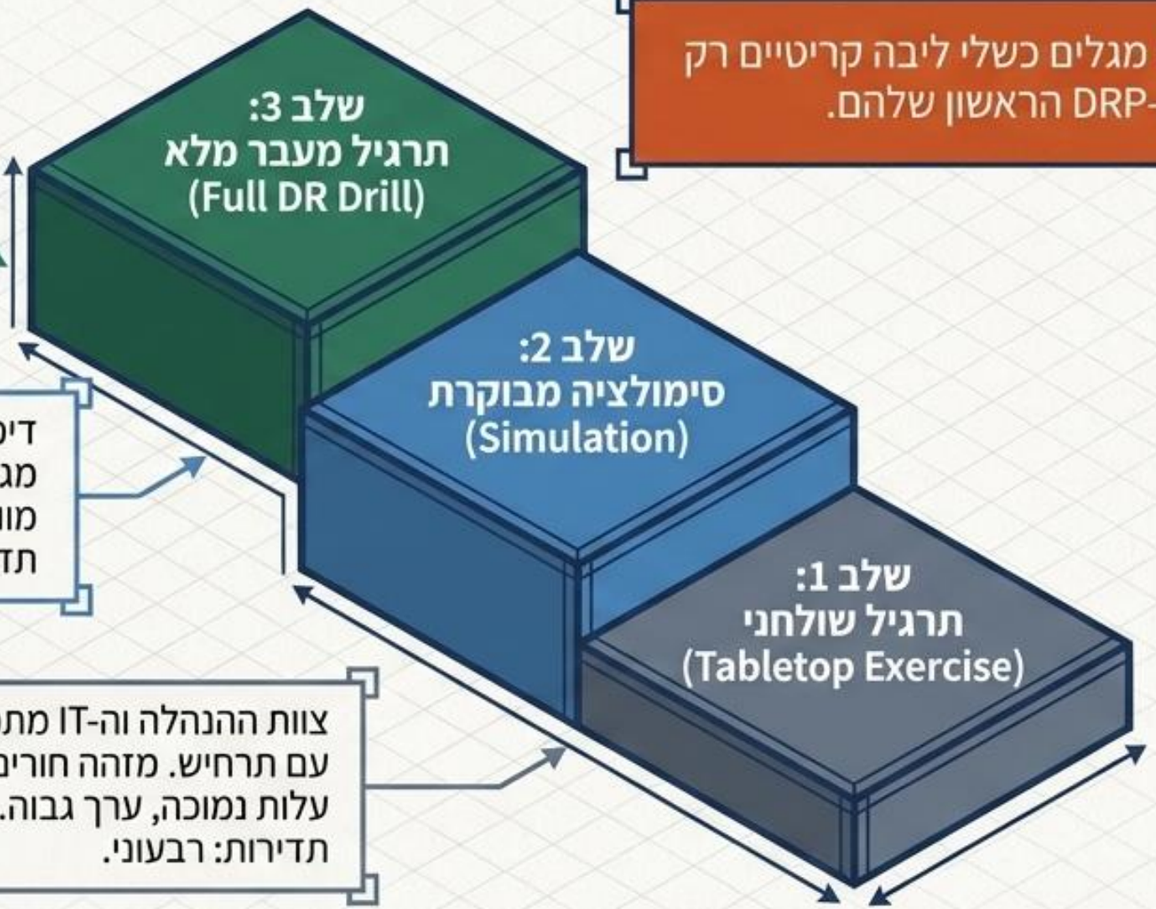
וידוא שלמות הנתונים טרם
פתיחת התעבורה מחדש.

כלל הזהב

ה-Runbook חייב להיות כתוב ברמה שטכנאי זוטר (Junior) מסוגל לבצע אותו ללא שגיאות.
המומחה הראשי לעולם
אינו זמין בזמן אסון.

ספקטרום הבדיקות:
תוכנית שלא נבדקה – אינה קיימת

75% מהארגונים מגלים כשלי ליבה קריטיים רק במהלך תרגיל ה-DRP הראשון שלהם.



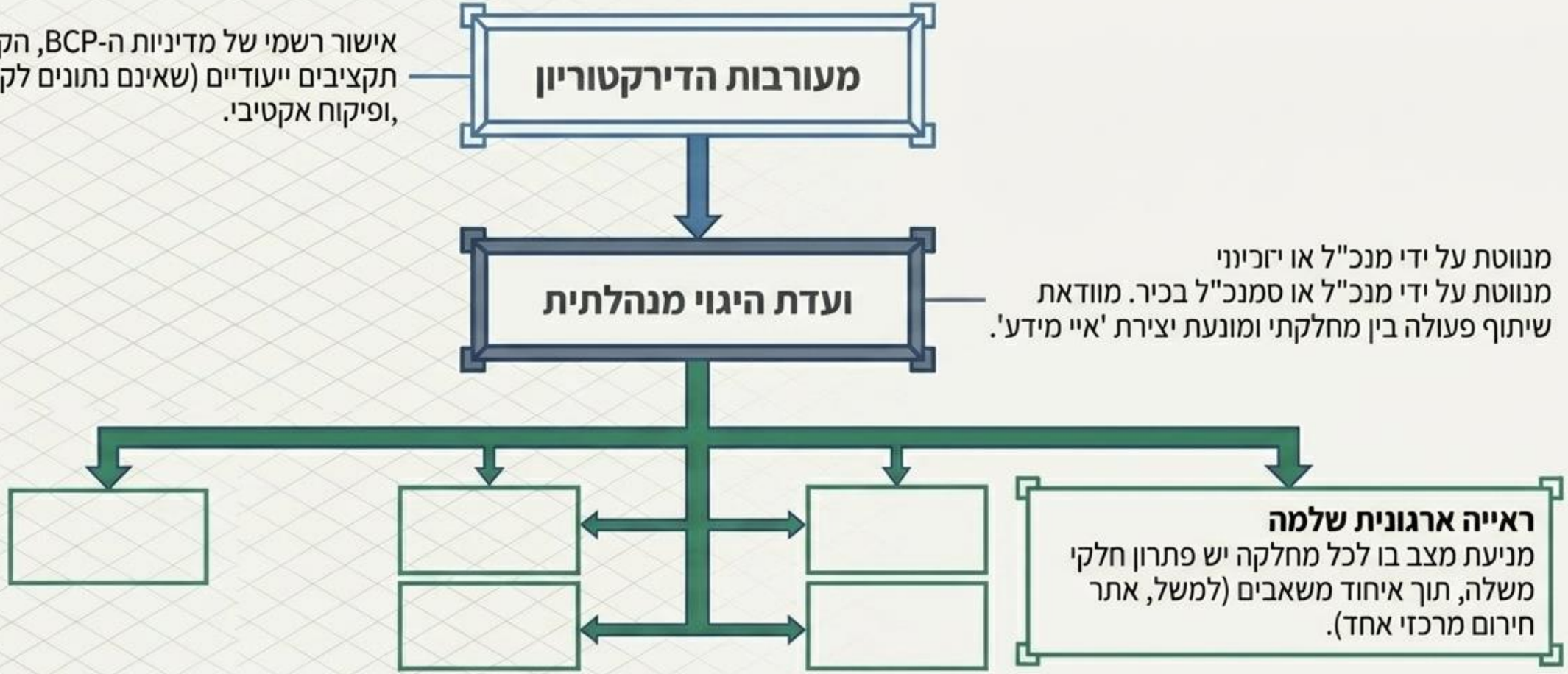
Failover מלא לאתר החירום.
העברת משתמשים אמיתיים לסביבת לסביבת ה-DR. יקר, מפחיד, אך הכרחי למניעת הפתעות.
תדירות: שנתי.

דימוי כשל למערכת ספציפית ושחזורה מגיבוי לסביבה מבודדת.
מוודא שהגיבוי אכן תקין.
תדירות: חודשי.

צוות ההנהלה וה-IT מתמודדים תיאורטית עם תרחיש. מזהה חורים בתהליך, עלות נמוכה, ערך גבוה.
תדירות: רבעוני.

ממשל תאגידי: אחריות הדירקטוריון

היערכות לאסון אינה פרויקט מחשוב. זוהי חובה ניהולית עליונה.
ועדות חקירה (דוגמת חבר המושבעים במחוז אורנג') מראות שתוכניות קורסות ללא מנהיגות פעילה.



כלל 3-2-1 לשרידות נתונים:

3 עותקים של המידע.

2 סוגי מדיה שונים (למניעת כשל טכנולוגי רוחבי).

1 עותק מחוץ לאתר (ענן, כספת מרוחקת).

צ'קליסט מנהלים: האם אתם באמת מוכנים?

- ☐ תרחישי אסון מוגדרים ומתועדים במדויק.
- ☐ ערכי RTO ו-RPO מאושרים על ידי ההנהלה לכל מערכת.
- ☐ קיים Runbook מעודכן שנוסה ברבעון האחרון.
- ☐ מנגנוני DLP פעילים גם בעבודה מאתרים חלופיים.
- ☐ העובדים יודעים בדיוק מה לעשות ואיפה לעבוד במקרה אסון.

BCP .....

- **מרכיבים חשובים בתכנון BCP טוב:**
- **Business Impact Analysis (BIA)** - ניתוח אילו תהליכים קריטיים לארגון ומה תהיה השפעה אם יושבתו.
- **Risk Assessment** – זיהוי תרחישים אפשריים (סייבר, תקלות חשמל, הצפות, שביתות וכו').
- **Disaster Recovery Plan (DRP)** - תכנית טכנולוגית להחזרת מערכות IT לפעולה.

המכללה
האקדמית
רמת גן

BCP המשך .....

- **מרכיבים חשובים בתכנון BCP טוב:**
- **Incident Response Plan** - תכנית תגובה לאירוע בזמן אמת (בעיקר אירועי סייבר).
- **Communication Plan** - מי מדבר עם מי, איך, ומתי – כולל תרחישי קיצון.
- **תרגול תקופתי (Tabletop & Live Exercises)** – ווידוא שמערכת BCP עובדת ולא רק קיימת במסמך.

המכללה האקדמית רמת גן

תוכנות וכלים לניהול BCP

תיאור	פתרון
פתרון פופולרי להמשכיות עסקית, ניתוח השפעה עסקית(BIA) - Business Impact Analysis, ניהול סיכונים ותגובה לאירועים	**Fusion Framework System** (Fusion Risk Management)
מערכת ניהול סיכונים וציות עם מודולים ל- Business Continuity ו- Disaster Recovery	**MetricStream**
פתרון GRC - Governance, Risk Management & Compliance הכולל כלים ל- BCP, ניתוח השפעות, תכנון תרחישים ותרגולים	**LogicManager**
פתרון לניהול התאוששות מאסון (DR) בזמן אמת, כולל גיבויים, רפליקציה ו- backup חכם	**Zerto (by Hewlett Packard Enterprise)**
מערכת תקשורת והתראה למצבי חירום – מאפשרת הפצת הודעות לעובדים, קבלת דיווחים ותיאום תגובות	**Everbridge**
מערכת מובנית לניהול תכניות BCP, ניתוח תרחישים, ומעקב אחר רמות מוכנות ארגונית	**ServiceNow Business Continuity Management**
שירותי התאוששות מאסון (DRaaS) וייעוץ BCP כולל אירוח חלופי והפעלת מערכות מגיבוי	**Sungard Availability Services**
שירות DR בענן עם רפליקציה חיה והפעלת מערכות תוך דקות במקרה של כשל	**CloudEndure Disaster Recovery** (AWS)

פתרונות טכנולוגיים וכלים מתקדמים

פתרונות נפוצים	תחום
Veeam, Acronis, Commvault, Zerto, Rubrik	גיבוי (Backup) והתאוששות מאסון Disaster (Recovery)
VMware vSphere HA, Microsoft Failover Clustering, Nutanix	High Availability (HA)
ServiceNow Business Continuity, Fusion Framework System	ניהול תהליכים עסקיים (BPM) והמשכיות עסקית
Microsoft Azure Site Recovery, AWS Disaster Recovery, Google DRaaS	ענן והתאוששות מבוססת SaaS
Castellan, Quantivate, Assurance Software, NAVEX	ניהול תיעוד ותהליכי BCP

BIA

המכללה
האקדמית
רמת גן

אלמנטים שאמורים להיכלל בתוכנית BCP טובה:

- ניתוח סיכונים (Risk Assessment)
- ניתוח השפעה עסקית (BIA – Business Impact Analysis)
- נהלים להתאוששות ושחזור
- סדרי עדיפויות עסקיים ותפעוליים
- תוכנית תקשורת (כולל חיצונית)
- תוכנית אימונים ובדיקות (Simulation Testing)

- **Business Impact Analysis (BIA) -** ניתוח אילו תהליכים קריטיים לארגון ומה תהיה השפעה אם יושבתו.

- תהליך ניתוח ומיפוי של תהליכים עסקיים בארגון, תוך קביעת חשיבותו ורגישותו של כל תהליך והבנת משמעויותיו העסקיות.
- תוצר תהליך BIA הינו מיפוי מלא של מערכות ותהליכים בארגון בסדר יורד.
- הערכות – DRP תיקח את תוצר ה –BIA ותממש/לא תממש אותה בהתאם לשיקולי עלות תועלת.

- **Business Impact Analysis (BIA) – המשך.**

- **תהליך ה - BIA כולל:**

- מיפוי התהליכים העסקיים.
- מהן התשומות שנכנסות לתהליך זה ומי/מה מספק אותן (מידע/חומר גלם וכו').
- מהם התוצרים בתהליך ומהו יעדם?

- משך הזמן בו הארגון יכול לפעול ללא תהליך זה בחלוקה למקבצי זמן (עד 4 שעות, 4-8 שעות, 8-21 שעות, 14-21 שעות, 14-48 שעות וכו') בחלוקה ל RPO/RTO
  - RTO - מהו משך הזמן המקסימאלי בו הארגון יכול לפעול ללא התהליך.
  - RPO - מהו משך זמן אובדן הנתונים המקסימאלי שהארגון מוכן לספוג בתהליך.

- **Business Impact Analysis (BIA) – המשך.**

- ביצוע ניתוח של כימות כלכלי של הפסד עסקי בחלוקה למקטעי זמן:
  - מיפוי נקודות זמן רגישות ביחס לתהליך (תחילת חודש/אמצע חודש/ מועד ספציפי במהלך החודש).
  - חלופות קיימות לכל תהליך ותהליך (בין אם ידניות באופן עצמאי/כשירות מספק חיצוני וכו').

- Recovery Time Objectives
- Recovery Point Objectives

המכללה
האקדמית
רמת גן

- **Business Impact Analysis (BIA) – המשך.**

תוצרי התהליך:

- מיפוי כלל התהליכים (תשומות ותוצרים).
- מיפוי מערכות בכל תהליך (חומרה, תוכנה).
- מיפוי ספקים חיוניים הקשורים לכל תהליך.
- מיפוי השלכות נזק כלכליות ישירות בציר הזמן של העדר תהליך.
- הערכת נזקים נוספים (תדמית, רגולציה וכו')
- ניתוח RPO/RTO לכל תהליך.
- מיפוי רגישויות ספציפיות פר לתהיך (רגישות לזמן, מיקום וכו').
- טבלאות חלוקה (גבוה, בינוני, נמוך) לקביעת רגישות/חשיבות התהליך.
- המלצה של השקעה מינימאלית/מקסימאלית ב - DRP ביחס לתהליך בהינתן נזק שיגרום העדרו על פני זמן.
- תוכנית עבודה מפורטת להערכות מומלצת.

המכללה האקדמית רמת גן

- **Risk Assessment** – זיהוי תרחישים אפשריים (סייבר, תקלות חשמל, הצפות, שביתות וכו').

Impact

Probability	Insignificant 1	Minor 2	Moderate 3	Major 4	Severe 5
5 - Very likely	5	10	15	20	25
4 - Likely	4	8	12	16	20
3 - Possible	3	6	9	12	15
2 - Unlikely	2	4	6	8	10
1 - Very unlikely	1	2	3	4	5

Risk level

- Low
- High
- Moderate
- Severe

המכללה
האקדמית
רמת גן

- **Disaster Recovery Plan (DRP)** - תכנית טכנולוגית להחזרת מערכות ITלפעולה.

- DRP זהו האספקט הטכני של המשכיות עסקית: .Disaster Recovery Plan
- אוסף המשאבים והפעילויות להפעלה מחדש של שירותי טכנולוגיית המידע (ובכללן רכיבים כגון תשתיות, תקשורת, מערכות, יישומים ונתונים) באתר חלופי לאחר הפרעה לשירותי מערכות המידע.
- תוכנית התאוששות מאסון כוללת פעילות עוקבת של שיקום ושחזור פעילויות גם באתר יותר קבוע.

המכללה
האקדמית
רמת גן

- **Disaster Recovery Plan (DRP)** -בעולמות הסייבר.

- ה-DRP הינו חלק מתוכנית לניהול המשכיות עסקית וכולל בתוכו את תחום תשתיות ה- IT ושיקום מערכות ה DATA במקרה של אסון.
- כמו גם כולל צוות בקרת נזקים אשר אמון על טיפול לאחר אירוע חירום בהתאם לצרכי הארגון.
- הצוות אחראי לתעדף את הטיפול בנזקים עד למצב של חזרה לשגרה.

ניתוח סיכונים טכנולוגיים לארגון

- ב- DRP מבצעים ניתוח סיכונים בעיקר בפן הטכנולוגי- סייבר למערכות מידע הכולל טיפול בחוות שרתים, שירותי ענן, גיבויים ועוד.
- בנוסף מטפלים בכל תשתיות תהליכי הייצור של הארגון.
- יכולת התאוששות מאסון של ארגון תלויה באופן ישיר בהיערכות מקדימה ראויה.

המכללה
האקדמית
רמת גן

- **Disaster Recovery Plan (DRP)** -בעולמות הסייבר.

- צמצום למינימום (או ל 0) זמן "מת" של מערכת
- צמצום למינימום (או ל 0) איבוד מידע
- עמידה בתקנים המחייבים אבטחת מידע ותקני התאוששות
- מערכות בהתאם ל (**IEC 27001** ו **IEC 62443**)
- ניהול תוכנית סיכונים ותוכנית גיבוי
- הכנה / מוכנות - לשינויים / תקלות / תרחישים לא צפויים

המכללה האקדמית רמת גן

Any Questions?

Please don't feel afraid to ask.

המכללה
האקדמית
רמת גן