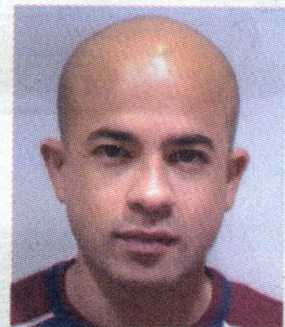
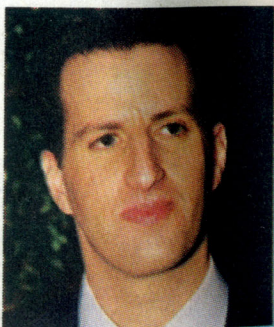


הרוצה בהמשכיות, יערך לשעת חירום

רק עדיפות עליונה בהקצאת המשאבים לטיפול בתוכנית להמשכיות עסקית ובהיערכות לשעת חירום, תבטיח שעסקים יוכלו לחזור במהירות למצב של פרודוקטיביות. כך כותבים רואי החשבון דורון רונן ואלון כהן באתר האיגוד הישראלי לביקורת ואבטחת מערכות מידע www.isaca.org.il



דורון רונן (מימין) אלון כהן: ניתוח דירוג הסיכון, מאפשר לדגל את המערכות לצורך קביעת אסטרטגיית ההתאוששות



5. רישומים, אגב תחזוקת התוכנית (לרבות עריכת ניסויים, הדרכה וסקירות), נשמרים על-ידי הארגון.
- מבקר מערכות מידע, שמתבקש לערוך ביקורת בנושא התאוששות מאסון והמשכיות עסקית, יסתייע בנהלי ביקורת כמפורט להלן:
1. הערכת תוכנית ההתאוששות ותכנית הארגון להמשכיות עסקית, על-מנת לקבוע את נאותותן ועדכניותן.
2. הערכת היעילות והאפקטיביות של התוכניות באמצעות סקירת תוצאות הניסויים שבוצעו על-ידי הארגון.
3. הערכת יכולותיהם של עובדי החברה להגיב באופן יעיל ואפקטיבי במקרה חירום.
4. סקירת פעילויות התמיכה הצפויות בציוד הקצה של המשתמשים.
5. בחינת שלמות: האם כל היישומים הרלוונטיים קיבלו ביטוי בתוכנית ההתאוששות.
6. בחינה האם החברה זיהתה את כל מערכות המידע הקריטיות האמונות על התהליכים העסקיים הקריטיים.
7. סקירת רשימת אנשי הקשר המעורבים ביישום התוכנית (בשעת חירום).
8. הערכת תוצאות ניסויים המבוצעים על-ידי הארגון. על המבקר לסקור ולבצע הערכה של תוצאות הניסויים. כמו-כן על המבקר לבחון האם הניסויים שבוצעו הם יעילים ואפקטיביים.
9. הערכת נאותות מתקן הגיבוי החלופי, לרבות סקירת הבקורות וסקירת תוכן המתקנים הללו. האם המתקן מכיל את הגרסאות העדכניות של היישומים המיועדים. על המבקר לבצע ספירת מלאי במתקן, שתכלול גם בחינה של תקינות רישום הפרטים על אמצעי הגיבוי ועל המסמכים הרלוונטיים. כמו-כן יש להעריך את זמינות המתקן עבור צרכי הארגון.
10. תשאול אנשי מפתח באשר לאופן ביצוע משימותיהם בשעת חירום.
11. הערכת הבקורות במתקן הגיבוי החלופי: יש לוודא, כי מתקיימות בקורות גישה פיסיות ולוגיות למתקן האמור.
12. סקירת הסכמים ליחידות עיבוד חלופיות.
13. סקירת הכיסוי הביטוחי, תוך וידוא שהוא מכסה את העלות האמיתית המגולמת בביצוע מהלכי התאוששות. הדבר כולל, בין היתר, תחלופה של ציוד, דמי שימוש באתר חלופי (קר/חם), הפסדים כספיים, הפסד מוניטין ואובדן מסמכים.

**חשוב מאד לבצע ניסוי התאוששות
או המשכיות שמטרתו לבחון את
היעילות והאפקטיביות של תוכנית
הארגון להמשכיות עסקית**

תהליך דירוג הסיכון אמור להתבצע על-ידי אנשי מערכות מידע, בשיתוף עם משתמשי הקצה ומקובל לדרג את הסיכון למספר רמות:

- קריטי (CRITICAL) – פעילויות אינן יכולות להתבצע, אלא על-ידי החלפה במערכת זהה. כמו-כן כשלא ניתן להחליף את פעולות מחשב באמצעות שימוש בנהלים ידניים. מידת הסובלנות (TOLERANCE) כלפי שיבושים היא נמוכה מאוד, ועלות שיבושים גבוהה מאוד.
- חיוני (VITAL) – ניתן להחליף את פעולות המחשב באמצעות נהלים ידניים, אך לפרק זמן קצר בלבד. מידת הסובלנות לשיבושים גבוהה ביחס לדירוג קריטי, ועלות השיבושים – נמוכה יותר.
- רגיש (SENSITIVE) – פעילויות אלו יכולות להתבצע באופן ידני, בעלות סבירה, למשך זמן ארוך יחסית למערכות חיוניות. על-פי רוב, נדרש כוח-אדם נוסף לביצוע הנהלים הידניים.
- לא קריטי (NONCRITICAL) – פעילויות שניתן לבצע (באופן משובש) למשך זמן ארוך יחסית. עלותן נמוכה מאוד, והן דורשות עדכונים ספורים בשלבי ההתאוששות.

בחירת אסטרטגיית התאוששות

אסטרטגיית ההתאוששות היעילה ביותר נחשבת לזו אשר מתחשבת בעלות של אורך זמן קריטי סביר, תוך התייחסות להשפעה של השיבוש וההסתברות של השיבוש.

חשוב מאד לבצע ניסוי התאוששות או המשכיות שמטרתו לבחון את היעילות והאפקטיביות של תוכנית הארגון להמשכיות עסקית. הניסוי אמור לכלול את כל המרכיבים הקריטיים ולדמות מצב של עומס בעיבוד שוטף. מפרט הבדיקות יכלול, בין היתר:

1. וידוא שלמותה של התוכנית להמשכיות עסקית.
 2. הערכת ביצועיהם של הגורמים המעורבים בביצוע התוכנית.
 3. הערכה של רמת ההדרכה והמודעות של אנשי הצוותים שאינם מהיחידות העסקיות.
 4. הערכת התיאום בין הצוותים לבין הספקים וגורמים שלישיים נוספים.
 5. הערכת תהליך אחזור הנתונים החיוניים.
- על הארגון לתעד את תוצאות הניסוי שערך, ואף לתעד את התצפיות שנערכו במהלך הבדיקות, הבעיות שהופיעו והחלופות שמוצעות לפתרון.
- האחריות לתחזוקת התוכנית, היא של מתאם ה-BCP. באחריותו לוודא, בין היתר, כי:
1. ה-BCP/DRP משקפים את צורכי הארגון.
 2. שינויים באסטרטגיית עסקית של הארגון מקבלים ביטוי בתוכניות ההתאוששות, והאיל והם עלולים להשפיע על רמת הקריטיות של התהליכים ו/או יישומים מסויימים.
 3. קיים לוח זמנים לסקירה תקופתית של התוכנית, לרבות יידוע בעלי התפקידים הרלוונטיים.
 4. קיימת תוכנית הדרכה לכוח האדם הרלוונטי, בנוגע לפעולות הגיבוי והתאוששות.

היערכות להתאוששות מאסון – DRP – היא התוכנית המבוצעת על-ידי מערכת המידע, על-מנת לאושש חלק ממערכת המידע, או על-ידי היחידות העסקיות, על-מנת לאושש חלק מהמערכת העסקית. התוכנית חייבת להיות עקבית ותומכת בתוכנית הכוללת של הארגון.

מטרתה של תוכנית להמשכיות עסקית – BCP – הן: א. לבחון את נאותות היערכות הארגון למקרה של אסון, על-מנת לוודא חידוש תפקודן של מערכות המידע במקרה של שיבוש קצר טווח, או במקרה של התחלה מחדש (RESTART), או הרצה מחדש (RERUN) של תהליך. ב. להעריך את יכולתו של הארגון להמשיך לספק פעילות באמצעות מערכות המידע העומדות לרשותו, אם מתקני העיבוד העיקריים אינם זמינים.

ג. להעריך את יכולתו של הארגון להבטיח המשכיות עסקית במקרה של שיבוש עסקי. שיבוש שכזה, המוגדר אסון – גורם לאי תפקוד של חלק כלשהו במערכת המידע, למשך זמן מסוים, דבר שגורם נזק לפעילות הארגון. האסון מוערך על-פי משך הזמן בו המערכת אינה מתפקדת, ובקריטיות המידע שאינו זמין באותו פרק זמן. אסון מחייב פעולת התאוששות כלשהי שבמהלכה יתבצע שחזור של נתונים ותוכנות. במקרה האחרון יש לוודא שהאתר החלופי יהא זמין לתקופה מספקת, שתאפשר להחזיר את אתר הקבע של הארגון לקדמותו.

ניתוח השלכות עסקיות (BIA-BUSINESS IMPACT ANALYSIS) הוא תהליך קביעת הקריטיות של משאבי מערכת המידע, כגון יישומים, נתונים, רשתות, תוכניות מערכת, מתקני חומרה וכיוצא באלה, שתומכים בפעילותו של הארגון. בתהליך זה משתתפים נציגי ההנהלה, אנשי מערכות מידע ומשתמשי הקצה – תמהיל אנושי שמאפשר לכלול את כל סוגי משאבי המידע הקיימים בארגון.

שיבוש במערכת המידע אינו נחשב לאסון, אלא אם כן הוא מוביל לשיבוש של תהליך עסקי קריטי, לדוגמה: חוסר יכולת למכור, דבר שמביא באופן מיידי לאיבוד הכנסה. השפעתו של אסון גוברת ככל שהזמן מקורות האסון מתמשך. עלותם של מתקני השחזור פוחתת, אם הם נצרכים בתדירות נמוכה יותר ואז קיימת נקודת איזון, שבה השפעתו של האסון שווה לעלותו של מתקן השחזור.