



מוטי רוזנבוים

תכנית להמשכיות עסקית

(2011), השריפה, שכלתה את סניף "איקאה" בנתניה (שנת 2011), סיכנה את שליטתה של החברה בשוק; ועוד.

מכאן, שארגונים חייבים להיערך בצורה הולמת להבטחת המשכיותם העסקית. כיום, גופי פיקוח (כגון במגזר הפיננסי) החלו לחייב את הארגונים במגזר לקיים מסגרת עבודה כוללת לניהול המשכיות עסקית; במכרזים בין-לאומיים מתחזקת המגמה להתנות את ההשתתפות במכרז, בקיומה של מערכת המשכיות עסקית; וארגוני תקינה מפרסמים תקנים רלוונטיים, המפרטים את דרישותיהם בנושא.

להלן תקנים העוסקים בהמשכיות העסקית:

- התקן הבין-לאומי לביטחון חברתי: ISO 22301 (Societal security - Business continuity management systems).
- התקן הבריטי BS 25999 לניהול המשכיות עסקית [BCM] (Business Continuity Management).

ההסמכה לתקן היא הוכחה של הארגון על קיומה של מערכת ניהול המשכיות עסקית ולהיערכותו להתאוששות מאסון על-פי צרכיו העסקיים.

תכנית להמשכיות עסקית

התכנית להמשכיות עסקית (Business Continuity Plan) [BCP] היא תכנית מקיפה, שתפקידה הוא להבטיח את רציפות פעילותו הקריטית של הארגון בעתות משבר, אסון, או חירום. מטרת התכנית היא לספק מענה ההולם איומים חיצוניים ופנימיים, לספק שירותים חיוניים במשך זמן מוגדר וברמת שירות מוגדרת, ולהגן על נכסיו התחרותיים של הארגון.

התכנית כוללת את השלבים הבאים: הכרת הארגון (Understanding the organization); קביעת האסטרטגיות לניהול המשכיות העסקית (Determining business continuity management strategies); פיתוח פתרונות לניהול המשכיות העסקית (Developing and implementing business strategies).

(המשך בעמ' 14)

פיגועי ההתאבדות "Nine Eleven" אשר אירעו בארה"ב, בבוקר יום שלישי, 11 בספטמבר 2001, גרמו, בין-השאר, לקריסת מגדלי התאומים ולהרס מבנים נוספים במרכז הסחר העולמי (World Trade Center) [WTC]. הפיגועים גבו את חייהם של אלפי אנשים, אך נוסף על-כך, הם פגעו אנושות בעסקים רבים, שלא נערכו כיאות לאסון מסוג זה.

פיגועי טרור אינם הדוגמה היחידה לאיום, המסכן את קיומם של ארגונים ואת המשכיותם העסקית. ולראיה: בעיית התוכנה במכשירי הסלולר, מן הסוג "מוטורולה אלפא", איימה לחסל את חברת סלקום בתחילת דרכה (שנת 1995); המעילה של אתי אלון הביאה לקריסת הבנק למסחר (שנת 2002); אירועי מלחמת לבנון השנייה פגעו במפעלים ובבתי-עסק רבים, בעיקר, בצפון הארץ ובדרומה (שנת 2006); הרפורמה בשוק הסלולר פגעה פגיעה מהותית בחברות הריכוזיות, ששלטו בענף התקשורת (שנת

התכנית להמשכיות עסקית (Business Continuity Plan) [BCP] היא תכנית מקיפה, שתפקידה הוא להבטיח את רציפות פעילותו הקריטית של הארגון בעתות משבר, אסון, או חירום





בעל עסק / יבואן!

אנו מזמינים אותך לחוות לוגיסטיקה ברמה אחרת!
תתרגל לקבל יותר.



מטרת התכנית היא לספק מענה ההולם איומים חיצוניים ופנימיים, לספק שירותים חיוניים במשך זמן מוגדר וברמת שירות מוגדרת, ולהגן על נכסיו התחרותיים של הארגון

ממלא מקום לכל צוות, כדי להבטיח מענה הולם בעת הצורך.

(continuity management response); תרגול, תחזוקה וסקירה (Exercising, Maintenance and Review).

להלן פירוט השלבים בבניית התכנית להמשכות עסקית ולניהולה:

שלב א': הכרת הארגון

שלב זה כולל את הרכיבים הבאים:

- ניתוח ההשלכות העסקיות (Business Impact Analysis) [BIA]. מטרת הניתוח היא לזהות מוצרים/שירותים חיוניים, תהליכים עסקיים קריטיים, משאבים קריטיים, גורמי מפתח פנימיים וחיצוניים, וכו'; לנתח את השפעתם על המשכיות העסקית; ולהגדיר רמות עמידות נאותות, כגון: משך הזמן המרבי המותר לאיבוד נתונים (Recovery Point Objective) [RPO], משך הזמן המרבי המותר עד להתאוששות (Recovery Time Objective) [RTO], משך הזמן המרבי להשבתת שירות ללא נזק מהותי (זמן השבתה נסבל) (Maximum Tolerable) [MTPOD] (Period Of Disruption), וכו'.
- ניתוח האיומים והסיכונים (Threat and Risk Analysis) [TRA]. הניתוח כולל את הרכיבים הבאים: זיהוי האיומים האפשריים, המסכנים את הארגון, כגון: תקלה גורפת, שביתה, פשיטת רגל של לקוח/ספק אסטרטגיים, שינויי חקיקה/רגולציה, שריפה, שיטפון, רעידת אדמה, התקפת סייבר (Cyber attack), מגיפה, פשע, טרור, מלחמה, וכו'; הערכת הסתברותם של האיומים; כימות עוצמות הנוקים האפשריים; והערכת העלויות לטיפול באיומים אלה. בדרך-כלל מומלץ להתמקד באיומים שהסתברותם אינה זניחה, שחומרת פגיעתם היא משמעותית, ושעלות הטיפול בהם היא סבירה. בצורה זו, הארגון יכול להתמקד באיומים רלוונטיים ולתת להם את המענה המיטבי.
- הגדרת תרחישי הפגיעה, אשר משבשים את הפעילות (Impact scenarios), כגון: פגיעה בתשתיות, הרס מבנה, השבתת קו ייצור, אתר לא נגיש, קריסת מערכת מידע, וכו'.
- פירוט דרישות ההתאוששות (Recovery requirement), כגון: יעדי התאוששות, המפרטים רמות התאוששות וזמני התאוששות לפעילויות חיוניות (כגון: אספקה של מוצרים חיוניים ברמה קריטית, בתוך שעות ספורות; אספקה של מוצרים חיוניים אחרים בתוך 24 שעות; ואספקה של 80% ממיגוון המוצרים בתוך 72 שעות).

את הכנת התכנית מבצעת קבוצת צוותים רב-מערכתית (Multi-disciplinary). גישה זו מאפשרת לבעלי התפקיד השונים בקבוצה להציף מיגוון היבטים, לגבש את הפתרונות המיטביים לארגון ולייצר תכנית פעולה, אשר נותנת מענה התואם תרחישים שונים.

להלן דוגמה להתארגנות הצוותים, המעורבים בהכנת התכנית:

- צוות ההיגוי וניהול המשברים. הצוות אחראי על הנושאים הבאים: קביעת מדיניות הארגון בתחום המשכיות העסקית; קבלת החלטות אסטרטגיות; אישור תקציבים; אישור תכניות; וניהול המשברים המסכנים את המשכיות העסקית של הארגון. הצוות כולל את הגורמים הבאים: ההנהלה הבכירה של הארגון, המנהל האחראי על המשכיות העסקית, ויועצים מומחים בתחום. הצוות ממנה את "דובר הארגון", אשר תפקידו הוא לתקשר עם אמצעי התקשורת בעת הצורך ולספק מידע על האירוע.
- צוות הניהול. הצוות אחראי על הנושאים הבאים: פיתוח תכניות להבטחת המשכיות העסקית, יישומן, בדיקת אפקטיביותן, ותחזוקתן. הצוות כולל את הגורמים הבאים: נציג הנהלה בכיר, המנהל האחראי על המשכיות העסקית, מנהל השיווק והמכירות, מנהל שרשרת האספקה, מנהל התפעול, מנהל מערכות המידע, וכו'; ויועצים מומחים בתחום.
- צוות הביצוע. הצוות אחראי על ביצוע הפעולות התפעוליות, הרלוונטיות להבטחת המשכיות העסקית של הארגון. הצוות כולל את בעלי התפקידים הרלוונטיים בארגון, הן בתוכו והן מחוץ לו (כגון: ספקים, נותני שירות, קבלני-מסנה, וכו'). בין היתר, הצוות אחראי לשמר את הידע הביצועי ולהעבירו לחברי צוות חדשים.

חיוני לנהל את נתוני הקשר העדכניים של כל בעלי תפקידי המפתח ושל חברי הצוות. מומלץ לקבוע

שלב ב': קביעת האסטרטגיות לניהול המשכיות העסקית

שלב זה כולל את קביעת האסטרטגיות לניהול המשכיות העסקית. האסטרטגיות עוסקות בכל אחד מן המשאבים החיוניים לקיום הפעילות, כגון: אתרי פעילות, תשתיות, אמצעים, משאבי-אנוש, מערכות מידע, ספקים, מלאי, וכו'.

להלן דוגמאות לאסטרטגיות לניהול המשכיות העסקית:

- יתירות (Redundancy). קיבולת עודפת של תשתיות ושל אמצעים, המאפשרת לארגון להמשיך את



כיום, גופי פיקוח (כגון במגזר הפיננסי) החלו לחייב את הארגונים במגזר לקיים מסגרת עבודה כוללת לניהול המשכיות עסקית; במרכזים בין-לאומיים מתחזקת המגמה להתנות את ההשתתפות במרכז, בקיומה של מערכת המשכיות עסקית; וארגוני תקינה מפרסמים תקנים רלוונטיים, המכרטים את דרישותיהם בנושא



- המוצרים/השירותים החיוניים ביותר.
- הלקוחות האסטרטגיים של הארגון.
- המשאבים הקריטיים, המשפיעים על זרימת החומר/מתן השירות. כולל: מתקנים קריטיים, תשתיות, אמצעים, טכנולוגיות, וכו'.
- אנשי המפתח, החיוניים להמשכיות פעילות התפעול.
- התקשורת הארגונית בעתות משבר, אסון, או חירום, ובכלל זה: הנהלה, עובדים, צוותי חירום, ספקים, לקוחות, יועצים, רשויות פיקוח, ערוצי תקשורת, וכו'.
- התהליכים העסקיים ונוהלי העבודה הרלוונטיים.
- הרכיבים המיובאים, שזמינותם מותנית בעבודה רציפה של נמלי ים ואוויר.
- המלאי, ובעיקר, המלאי החיוני להבטחת רציפות האספקה.

שלב ד': תרגול, תחזוקה וסקירה

- שלב זה כולל את הרכיבים הבאים: תרגול התכניות ובקרתן המובנית על-פי תרחישים שהוגדרו מראש, תחזוקתן וסקירתן.
- התרגול כולל את בדיקתן של התכניות, את אישורן (Testing and organizational acceptance) ואת ביצוע ההתאמות הדרושות. התרגול יכול להתבצע במיגוון רמות, ולדוגמה: תרגילים "על הנייר" (Tabletop exercises), הכוללים תרחישים פשוטים; תרגילים ברמת ביניים (Medium exercises), הכוללים תרחישים עם מורכבות מסוימת; ותרגילים ברמה גבוהה (Complex exercises), הכוללים תרחישים מערכתיים עם מורכבות רבה. בסיום התרגול בודקים את אפקטיביות התכניות, מבצעים את ההתאמות הדרושות, ומאשרים את התכניות.
 - תחזוקת התכניות צריכה להתבצע תדיר (לפחות פעם בשנה), כדי להבטיח את המטרות הבאות:
 - חיזוק המודעות בארגון להבטחת המשכיות העסקית;
 - תרגול הפתרונות הטכניים לפעולות התאוששות מאסון (Technical solutions established for recovery operations) ואימות אפקטיביותם;
 - תרגול נוהלי הארגון הרלוונטיים להתאוששות (Organization recovery procedures) ואימות אפקטיביותם.
 - ממצאי התחזוקה מהווים בסיס לסיקור חוזר של איומים ושל סיכונים, כדי לתת מענה הולם לאיומים חדשים, לסיכונים ששיעורם השתנה, לשינויים במסגרות התקציב, למוצרים/לשירותים חדשים, ללקוחות חדשים, וכו'. הממצאים מועברים לצוות ההיגוי, אשר מקדם את שיפור התהליכים ואת עדכון התכניות, כך שכל הנושאים יקבלו את המענה המיטבי על-פי הצורך.
 - לסיכום, זיהוי נכון של משאבים קריטיים; ונוסף על-כך, הפיתוח של תכנית להמשכיות עסקית, יישומה ותרגולה מבטיחים, כי הארגון נערך במוכנות גבוהה להתמודד עם איומים ועם אירועים בלתי-צפויים, וכי יש לו יכולת להתאושש על-פי יעדים מוגדרים בצורה, התואמת את צורכיהם של הארגון ושל לקוחותיו. ■

- פעילותו גם כאשר חלק מהם נפגע.
- ניתוב חלופי (Alternate Routing). הניתוב מאפשר את העברת המידע באמצעות ערוצים חלופיים (כגון שימוש בתקשורת סולרית, במקום בתקשורת קווית).
- אתר חלופי (Alternate Site). האתר מאפשר לארגון להמשיך את פעילותו, כאשר אתר הקבע נפגע (בעיקר, כאשר מדובר במתקן קריטי). האתר החלופי חייב להיות זמין למשך תקופה מספקת - עד להחזרת הפעילות לאתר הקבע. רצוי שהאתר החלופי יהיה במיקום גיאוגרפי מרוחק מאתר הקבע.
- להלן מיגוון האפשרויות לאתר החלופי:
 - אתר חם (Hot Site): אתר הכולל חומרה ותוכנה, התואמים לאלה הקיימים באתר הקבע. האתר החם זמין לשימוש בתוך שעות אחדות, ולכן הוא החלופה היקרה ביותר;
 - אתר חמים (Warm Site): אתר הכולל את התשתית העיקרית (מסופים, קווי רשת), ללא המחשב המרכזי;
 - אתר קר (Cold Site): אתר הכולל תשתיות בסיסיות (כגון חשמל ומיזוג) בלבד, והכשרתו לשימוש עלולה להימשך שבועות אחדים. לכן, חלופה זו היא הזולה ביותר.
- הסכם הדדי עם חברה אחרת (Reciprocal Agreements). ההסכם מאפשר לארגון להיעזר באתרים, בתשתיות ו/או באמצעים של ארגון (אחד או יותר), שעימו יש לו הסכם הדדי.
- גיבויים (Backup). אמצעים חלופיים לביצוע התהליכים העסקיים, כגון: רישום בטפסים ידניים, מחוללים (גנרטורים) לגיבוי, מרכזי אנרגיה כפולים, מערכת נתזים (ספרינקלרים) כפולה, וכו'; ואמצעי גיבוי לשמירת קובצי הנתונים, כגון: אחסון בשרתי גיבוי, הממוקמים באתרים שונים בארגון, או בחוות שרתים חיצונית (כולל שימוש בטכנולוגיית ענן).
- הסכמים עם ספקי מיקור-חוץ (Outsourcing service providers). ההסכמים יאפשרו את רציפות הפעילות בשרשרת האספקה (הובלה, אחסנה, ייצור, לוגיסטיקה, הפצה, גבייה, אחזקה, וכו').

שלב ג': פיתוח פתרונות לניהול המשכיות העסקית ויישומם

- בשלב זה מכינים תכניות, הכוללות הנחיות פעולה מפורטות ליישום האסטרטגיות שנקבעו בשלב הקודם. ההכנה כוללת את הגדרת בעלי התפקיד בניהול משבר, את תחומי אחריותם ואת סמכויותיהם.
- התכניות מספקות את המענה המיטבי בכל השלבים הבאים: מניעה, מענה מידי לאירוע, שיקום בטווח-הקצר ושיקום בטווח-הארוך, והן כוללות תכנית התאוששות מאסון (Disaster Recovery Plan) [DRP], העוסקת, בעיקר, בתכנית לחידוש פעילות מערכות המידע, כגון: יישומים, נתונים, ומערכות תקשוב (תקשורת ומחשבים), כגון: חומרה, תוכנה, ועוד.
- התכניות מפרטות את הרכיבים הבאים: