קורא יקר,

וירוסים, פרצות וספאם הולכים ומתרבים מיום ליום **באופן מבהיל.** מערכות המחשוב הופכות למורכבות וסבוכות. במקביל, הפס הרחב, הוירטואליזציה, BI - מציעים **הזדמנויות חדשות ומלהיבות** וגם תפקיד מנהלי המחשוב עובר טרנספורמציה **דרמטית ומבטיחה**. כך, לנוכח שטף חידושים וגלי תמורות, שרק מתעצמים ומואצים, קשה להתמקד במה שבאמת חשוב. **למי להאמין? על מי לסמוך?**

תחקירי PCאון מספקים בכל שבוע ריכוז של החדשות החשובות ביותר בעולם המחשוב והתקשורת, יחד עם תחקיר מקצועי שמתמקד בנושא מפתח מרכזי ומשמעותי. הם משרתים חלק גדול ממנהלי המחשוב המובילים של מדינת ישראל. חלקם מנויים לשירות קרוב לשש עשרה שנים כיוון ש:

- PCאון הוא מקור מידע **אמין ותכליתי.** הוא מתמקד רק **בנושאי המפתח** החשובים ביותר בעולם המחשוב והתקשורת, והוא **מדבר בשפתך המקצועית.**
- PCאון כולל את ריכוז **החדשות החשובות** ביותר וגם **מגמות, טיפים, ידע יישומי ושימושי** נוסף. הוא מאפשר בהשקעה של **פחות מ-10 דקות** בשבוע, להיות כל הזמן **עם יד על הדופק.**
- PCאון מביא תועלת בכך שהוא **רלוונטי לבעיות הנוכחיות שלך,** בנוסף לכך, הוא מסייע לך בהערכות מוקדמת בפני **סכנות ואיומים** למערך המחשוב **ו/או ניצול הזדמנויות עסקיות** חדשות.
- ניתן **להתרשם ממנו באופן אישי** באמצעות תחקיר הדוגמא המצורף או להסתמך על למעלה ממאה חוות דעת של מנהלי מחשוב מובילים (ראה - www.pcon.co.il/v5/103.asp).

PCאון נתפס כיום כ**מפתח מוכח להצלחה מהירה,** וככזה גם אתה תוכל ליהנות ממנו בקרוב. כמו ארגונים רבים תוכל להצטרף כמנוי ארגוני ותאפשר לכל העוסקים במחשוב בארגונך, ליהנות מכל היתרונות שלמעלה.

מחירי מנוי השנתי בגין 52 תחקירים:

מספר מנויים	המחיר בדולרים + מע"מ
1	516
5	1270
10	1970
20	3270
50	5970
100	7700
200 ויותר	9700

נכון, אפשר לנסות להתמודד לבד עם כל התמורות. להתעלם או לדגום מאמר אקראי ולקוות לטוב. **תחשוב על התוצאות.** מצד שני ניתן ללכת **בדרך סלולה ובטוחה** שבה הולכים המובילים במחשוב הישראלי, שגם ימשיכו להוביל בבטחה. כדי להצטרף אליהם, ללכת יחד איתם, אפשר לקרוא על תחקירי PCאון ולהצטרף באתר ב- www.pCon.co.il/promo טלפון 03-9667939, פקס 03-9660310 או מייל - sub@pcon.co.il

קובי שפיבק
העורך הראשי של PCאון

נ.ב. על כל תחקירי PCאון חלות כל ההגנות החוקיות של זכויות יוצרים. ביחד עם זה, אנו מתירים לשכפל ולהפיץ את תחקיר זה, **מבלי לשנותו, עד 31.12.2007 ורק יחד עם דף היתר זה!** למנהלים, עמיתים ואנשי מחשוב נוספים, שעשויים לדעתך למצוא בו עניין.

מה אתה מקבל? - מפתחות להצלחה

קורא יקר,

תיזכר ב"נפילה" האחרונה של מערכת בארגון, ב"פספוס" בבחירת טכנולוגיה, בפרוייקט שלא "סיפק את הסחורה". מדמיין? עכשיו קח לך פחות מחצי דקה ותחשוב על מי שקרא תחקיר דומה, לפני כשנה. באינטואיציה פנימית חזקה הוא הבין שמצא פיתרון אמיתי לצורך אמיתי - להיות ממוקד באיומים האמיתיים וההזדמנויות המבטיחות שרלוונטיים לארגון ולתפקיד שלו, למציאות שבה הוא חי. שוב ושוב הוא נוכח מאז, שהוא מתבסס על מקור מידע שמדבר אליו בשפתו, מקור תכליתי ואמין.

כאשר חבר קרוב מתקשר ושואל לחוות דעתו על תחקירי PCאון. "מה הם נותנים לך באופן מעשי?" באופן טבעי הוא נזכר ומספר על כמה מהדוגמאות הבאות:

- **בתחקיר - ה-IT מאיץ חדשנות** - הוא גילה את הטרנספורמציה שעוברת היום כגל סוחף בעולם העסקי. ה-IT הופך מכלי שתומך בעסקים, למנוע שמאיץ חדשנות ופותח הזדמנויות חדשות. התועלת עבורו הייתה דרך הסתכלות חדשה על היבטי ה-IT, כזאת שפתחה בפניו דלת לקידום מהיר...

- **בתחקיר - חוסכים חשמל** - הוא מצא נתונים לפיהם, עלויות החשמל של דטה סנטר בשנה יכולות להיות יקרות יותר מכל עלויות החומרה שבו. הוא גם קרא כיצד השינוי בצריכת החשמל בניידים לוקחת אותנו לעידן חדש. התועלת שהפיק מהתייחסות ויישום הייתה - הרבה כסף לארגון. איך זה נשמע?

- **בתחקיר - כללי אצבע למנמ"ר** - הוא מצא נתונים, מספרים, כללי אצבע ומקורות שחיוני לכל מנהל שעוסק במחשוב להיות מצויד בהם. התועלת שהפיק הייתה קבלת החלטות מהירות יותר, מבוססות ומוצלחות יותר. התוצאות נראות בשטח. מכיר אנשים כאלה?

- **בתחקיר - וירטואליזציה בשרתים** - הוא הבין את המשמעויות המעשיות של מגמה מרכזית שסוחפות כיום את עולם המחשוב, כאשר הוא גילה **איך** וירטואליזציה יכולה להעניק יותר גמישות, חיסכון עצום, שרידות, עבודה קלה ועוד יתרונות נוספים. פתאום הכול התחבר. אתה רואה זאת?

- **בתחקיר - Rootkit - חפרפרת במחשב** - הוא קרא כי ברשת הארגונית של כל ארגון חמישי באוסטרליה (וכנראה כך גם בארץ), חבויה כיום תוכנה נסתרת, שיכולה לפתוח דלתות לתוכנות מזיקות. בדרך כלל, לא ניתן לגלות אותה! גניבת מידע, שיבוש נתונים, האזנות, ציטוטים, חדירות, נזקים. חלק מהאיומים יכולים להביא לקריסה. הוא עשה את כל שניתן לטפל בכך וישן טוב בלילה. ואתה?

הוא גם לא היחידי שחושב כך. מאה המלצות נוספות עם מסר חד וברור מדברות בעד עצמן. אחרי הכול, עם הישגים שמוכחים בשטח, קשה להתווכח...

לכן אנו ממליצים לשתף מספר רחב ככל האפשר של חברים, עובדים ומנהלים, בארגון ומחוצה לו, בשימוש בתחקירי PCאון. בדומה לטלפון ופקס, ככל שרבים יותר המשתמשים בהם, כך גם גדלה התועלת. אתה ודאי מכיר זאת.

עכשיו אתה מוזמן לקרוא את התחקיר המצורף, להתרשם באופן בלתי אמצעי ולהתקשר - דרך האתר www.pCon.co.il/promo לטלפן 03-9667939, לפקסס 03-9660310 או מייל - sub@pcon.co.il

אחרי שתצטרף ותסתכל קדימה שנה מהיום, יתכן וגם אתה תחשוב כמוהו? מה דעתך?

PCאון ©

למנהלים ומשתמשי מחשב בכירים

תדרוך מקצועי קצר ומרוכז ● בחדשות ומידע שימושי ייחודי ● למיצוי המחשוב באופן מרבי

והפעם... מנהלים סיכונים בהצלחה

מסר אישי

31% מפרוייקטי המחשוב בארגונים עומדים להיכשל! כך טוענת **Standish Group**. כמנמ"ר אתה עומד בחזית הטכנולוגיה בארגון, כשאתה נמצא בעמדה לשנות, לקדם ולהשפיע. מצד שני, החזית היא מקום מסוכן! בחירה טכנולוגית לא נכונה או השקעה בפרוייקט כושל עלולה למנוע השגת יעדים עסקיים ולעלות ביוקר לארגון ולך, ברמה המקצועית והאישית.

כיצד תמפה אזורי סכנה טכנולוגיים ופרוייקטאליים? כיצד תפעל נכון למזעור סיכונים? מי ומה יסייעו להיחלץ מכשלון? להתאושש במהירות? כיצד תבטיח שמהלכיך יצדיקו עצמם כלכלית ויתמכו על ידי ההנהלה? על כל אלה ועוד - בתחקיר זה.

תמצית החדשות בעולם המחשוב טור

תוכן התדרוך השבועי טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **ערן דרור**

תחקיר וכתיבה - **עמית לוי**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

E-Mail - **editor@pcon.co.il**

לתשומת לבך

לכבוד **קומרקטינג ישראל**
פקס 03-9660310
ת.ד. 2340 ראשון לציון 75121

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $119 / $214 / $394 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג ישראל** ומחכה לגיליון הקרוב.

שם מלא_____

ארגון_____

תפקיד בארגון_____

כתובת_____מיקוד_____

טלפון_____פקס_____

תאריך_____חתימה_____

הערות _____

PCאון© למנהלים ומשתמשי מחשב בכירים

606.11 – חדשות בקצרה

• **HP ומיקרוסופט הציגו מחשב קונספט חדש, האמור להיות בעל התאמה משופרת מהיסוד לצרכי המחשוב הארגוני. Athens** משלב טלפון **VoIP** ומצלמת וידיאו, הוא מפסיק לנגן כאשר אתה עונה לטלפון, מתריע באמצעות נורית מיוחדת על דואר נכנס, ומוותר על מצבי צריכה דוגמת **Sleep mode** לטובת מה שהמשתמשים מעדיפים: שני מצבי פעולה בלבד - כיבוי מיידי או הדלקה מיידית, החוזרת אל מצב המערכת האחרון.

• סקר **איגוד טכנולוגיות המידע** בארה"ב בקרב מנהלי גיוס בארגונים, מעריך כי שוק העבודה בתחום ה-**IT** יהיה יציב בשנה הקרובה. הביקוש לעובדים צפוי להישאר כמות שהוא או להצטמצם מעט. לפי הסקר, שכר עובדי ה-**IT** ב-3 מתוך 4 מהחברות שנשאלו נשאר עד עתה כמות שהוא או עלה מעט.

• מעבד **Intel Itanium 2** חודר לשוק: **InfoWorld** מדווח כי החברות **HP** ו-**IBM** הודיעו על שיבוצו במוצרי הדור הקרוב: **IBM** הודיעה כי שרת **x450** העתידי שלה יכלול 4 עד 8 מעבדים אלה, ו-**HP** הודיעה שתשיק בקרוב שני דגמי תחנות עבודה חדשות שישלבו את **Itanium 2** ואת מערכת ההפעלה **חלונות XP** בגרסת 64 ביט.

606.12 – דורשים מחשוב גמיש

קונספט המחשוב לפי דרישה - Computing On Demand - מציג אפשרויות חדשות לצריכת מחשוב בפני ארגונים. גישה זו מספקת גמישות שכל-כך חשובה בזמנים עתירי שינוי, סיכון וסיכוי עסקי. עיקרו - "צרוך רק כפי הנדרש לך" (בדומה לצריכת חשמל). הרעיון מיושם בשנים האחרונות כהצעות קונקרטיות, כולל ספקים מובילים, כאשר לאחרונה נעשו עוד כמה צעדים בדרך להתבססותו בארגונים. **Computer Associates** הציגה שישה מוצרים חדשים בגישה זו, שמטרתם שיפור יכולת הניצול של משאבים ארגוניים קיימים במסגרת פתרון **Unicenter** (www3.ca.com/Solutions).

IBM גם היא הציגה מוצרי **Computing On Demand** חדשים שיהיו זמינים החל מיולי. **TotalStorage** מורכב מ-**SAN Volume Controller**, שרת **SAN Integration**, ה-**SAN file system** הידוע בשם **Storage Tank** וטכנולוגיית ניהול מרכזית עבורם. פתרון **WebSphere** חדש של **IBM** כולל גם טכנולוגיית **Grid** העשויה אף היא לסייע ליישום מחשוב לפי דרישה בארגונים, וכן תוכנית חדשה לצריכה לפי שימוש בשם **Open Infrastructure Offering**. גם **Veritas** מצטרפת למגמת המחשוב לפי דרישה. בעזרת טכנולוגיות חדשות שרכשה. היא תציע בסוף השנה פתרון שיסייע להתאים **Data Center** למודל השימוש לפי דרישה. חשוב לציין שהפתרון לא יהיה מוגבל לטכנולוגיה מספק אחד בלבד (כמו **IBM**), אלא למגוון סביבות **Data Center** נפוצות.

606.13 – לאן יגיע הספאם ?

תופעת דואר הזבל שצמחה לממדי מגיפה מניבה כיום תגובות נגד רבות, עזות ויש לקוות - גם יעילות:

• **AOL ומיקרוסופט** תבעו לאחרונה כמה מפיצים כבדים של דואר זבל. שתי החברות החלו לתכנן בשיתוף **Yahoo!** גם צעדים שונים לצמצום התופעה, המתמקדים בצמצום יכולת הספאמר להסתיר זהותו. בהקשר זה עולה בארה"ב לדיון מחודש הצעת חוק חשובה שתאסור הסתרת כתובת השולח האמיתית. הצעות חוק נוספות מדברות על ענישה לפשיעת ספאם חוזרת והצעה נוספת ומעניינת מבקשת לחייב שולחי דואר לסמנו באותיות **ADV** אם הוא נשלח אליך לראשונה.

• בוועידה ממשלתית שהתקיימה לאחרונה בארה"ב על הנושא המחישה **AOL** במספרים את כמויות הספאם בהם היא נאלצת לטפל: מעל שני מיליארד הודעות באחד הימים האחרונים! להערכתה, מספר זה מייצג רק 80% לכל היותר מהספאם שנשלח למנוייה. **AOL** הוסיפה כי כמויות הספאם העוברות דרכה הוכפלו בחודשיים האחרונים לבדם.

• בארה"ב התלוננו לאחרונה כמה בעלי טלפונים סלולריים מסוג **סימנס S46** כי הודעה שקיבלו מחקה את ספר הטלפונים ואת הדואר שלהם. לטענתם הנזק התרחש גם מבלי לפתוח את ההודעה כלל. עדיין לא ברור אם מדובר בבאג בטלפונים או בוירוס מתוחכם מסוג חדש.

• ולבסוף ניתן להזכיר גורם משמעותי ביותר, בלעדיו הייתה תופעת הספאם דועכת מעצמה. לפי סקר שערך ארגון **Direct Marketing Association** האמריקאי - כ-37% מהנשאלים הודו שקנו לפחות פעם אחת בעקבות פרסום בדוא"ל! אלה הם אותם אנשים המתפתים לרכוש מספאמרים, הנותנים להם את הסיבה להציף את כולנו בפרסומותיהם המטרידות. לכן: **אימרו לא לספאם!**

606.14 – חוקרים וחוזים

כמה מחקרים חשפו לאחרונה תובנות מעניינות:

• בסקר **מטה גרופ** שנערך לאחרונה ציינו 80% מאנשי העסקים את ה-**E-Mail** ככלי התקשורת העסקית המועדף. מדיום זה מועדף גם על פני הטלפון, כאשר 74% מתארים הישארות בלעדיו כגרועה מהישארות ללא הטלפון.

• **מטה גרופ** רואה בעתיד **חלונות** מגמות אלה: עד 2007 תהיה הסביבה העסקית הדומיננטית **PC** מבוססי **חלונות**. במקביל ייכנסו לשימוש התקני מחשוב אחרים, כפי שיכתיבו סגנונות עבודה חדשים (כניידות ותקשורת אלחוטית).

• אנליסט **iSuppli**, **מתיו וילקינס**, חוזה כי ביטול התמיכה ב**חלונות 9x** יביא בקרוב לעליית מכירות ה-**PC**. זאת עקב הצורך לשדרג מחשבים לחומרה התואמת ל**חלונות XP**.

• מחקר **Trend Consulting** חושף כי ההתעניינות ב**לינוקס** ומוצרי קוד פתוח גוברת אך בפועל המכירות חלשות. 46% ממנהלי מחשוב שסקרה הביעו בטחון גובר בפתרונות קוד פתוח. כמו כן נראית תחילת התעניינות ב**לינוקס** גם ליישומי מחשוב קריטיים. למרות זאת, ישנה ירידה בת אחוז אחד בשימוש בפועל בפתרונות קוד פתוח רק 36% השנה.

• סקר **IDC** על שרותי **Web** חושף כי ארגונים עדיין ניגשים אליהם בזהירות רבה, מבחינת מספר הפרוייקטים והיקף ההשקעה הכספית. עם זאת, 88% מאמינים כי תועלות התחום לארגונים יגדלו בעתיד.

606.21– מנהלים בסיכון ?

מנהלי מחשוב - כמו הארגונים עצמם - חייבים לקחת סיכונים במסגרת המאבק ליתרון עסקי. לעתים מדובר בסיכון שאמור להניע יתרון עסקי (כמעבר לתוכנת CRM משוכללת) ולעתים מדובר בכניסה מוקדמת לתחום טכנולוגי חדש, כהצעת שרותים מבוססי מיקום. מובן שלצד הפוטנציאל מסתתרים גם סיכונים.

כבר ב-2001, בעקבות "פאניקת" סיכוני באג 2000, גילה סקר Economist Intelligence Unit עלייה ביישום ניהול סיכונים, כאשר מבין המנהלים הכלכליים הבכירים בעולם, שהסכימו להשתתף בסקר - 41% יישמו ניהול סיכונים ארגוני במידה מסויימת ו-32% תכננו לישם זאת בחמש השנים הבאות. לפי סקר עדכני (CarbonBased Consulting), מעל מחצית מהמנהלים מגדירים ניהול סיכונים כחשוב במידה בינונית או גדולה. כיום מובילה ארה"ב התעוררות גדולה בנושא, אך לפי סקר CFO Research Services, רק 5% ממנהלי הכספים מרוצים מההתאמה בין ניהול הסיכונים למטרות העסקיות.

לאור המצב הכלכלי שבו מנהלי המחשוב נדרשים לתת הסברים רבים יותר על כל השקעה ובאופן מיוחד על השקעה כושלת, בחירת טכנולוגיה לא נכונה, כניסה לפרוייקט הרפתקני או ניהול לא זהיר של פרוייקט, יכולים לעלות למנהלי המחשוב במשרתם. לפיכך לפני כל פעילות השקעה משמעותית כמו גם נושאים שבהם הם עשויים להיות מואשמים במחדל, גורמי סיכון חייבים להיחשף מוקדם ככל האפשר ולאפשר פעילות מניעה או התמודדות יעילה. לאחר הבום של שנת 2000, מנהלי חברות רבים מרגישים מאוכזבים ובאים (בגלוי או במרומז) בטענות למנמ"רים על ה"בזבוז" העצום שנדרשו לו. לכן גם היום דורשים מהם להוכיח באותות ובמופתים כדאיות כל השקעה ולהוכיח שלא נלקחים סיכונים מיותרים. המצב הכלכלי הלא סימפטי מחמיר כמובן את הסיטואציה עוד יותר. לכך נוסף גם המצב הבטחוני (מקומי ועולמי), המגביר סיכוני אבטחת מידע קלאסיים ומחייב כניסה להשקעות יקרות בפתרונות התאוששות מאסון.

בראש המענה לאתגרים נמצא ניתוח סיכונים שיטתי ומתודי (בעזרת נוהל כ**מפת"ח** - ראה 606.53), הסתייעות בתוכנות עזר וביועצים ושיטות מזעור סיכון - מפיילוטים לצד מיקוד בטכנולוגיות מבוססות ועד שיטות צריכת מחשוב מתקדמות. ניהול סיכונים הוא תחום רחב של ייעוץ כלכלי ואנו נתמקד בתחקיר בניהול סיכונים טכנולוגי, מנקודת מבטו של המנמ"ר.

ניהול סיכוני המחשוב צריך להיות חלק מניתוח וטיפול במכלול השירותים בארגון, אבל גם אם אין פעילות כוללת, חשוב ליזום, ליידע ולבצע פעילות כזאת לאגף המחשוב.

<u>לסיכום - ביטוח המנהלים מגן עלייך מפני חלק מהסיכונים האישיים בהם אתה עלול להתקל - ניהול סיכונים ארגוני משחק תפקיד דומה בצמצום וביטוח מפני סיכונים עסקיים בארגון. ככל שהסביבה והפרוייקטים בטוחים פחות - כך עליך להקפיד ליישם מתודולוגית ניהול סיכונים סדורה.</u>

606.22– רמזורים אדומים

אלו הסיכונים השונים בפעילות המחשוב הארגונית:

1. **השקעות כושלות -** מנהל מחשוב עשוי להוביל למה שיתגלה בדיעבד כבזבוז זמן וכספים על השקעות שלא מחזירות עצמן כמצופה. קיום מערכת שאינה עונה על הצרכים, פותחת את הארגון לסיכונים עסקיים בתחום שבו הוא נמצא ואינה מאפשרת להשיג יעדים תחרותיים.
2. **אפיון שאינו מתאים לצרכים -** אפיון שאינו מתאים לצרכי הארגון מבחינה עסקית וארגונית - אפילו אם הוא "המילה האחרונה" מבחינה טכנולוגית, יביא להוצאות עצומות ולכישלון בסבירות גבוהה.
3. **תקלות מערכת -** טעויות חישוב או תקלות מערכת עלולות לגרום נזקים כספיים לארגון וללקוחותיו וכן נזקי תדמית לארגון. לדוגמא: הסיכון באיבוד מידע רגיש על הלקוחות.
4. **שימוש פנימי מזיק -** הצורה הנפוצה ביותר של שימוש לרעה הן פשוט טעויות אנוש המסתיימות בנזקים שונים. מעילות והונאות הן גורם נוסף המשבש תהליכים עסקיים.
5. **שינויי שוק -** שינויים שלא נצפו בשוק העסקי בו פועל הארגון עשויים להביא למצב שמערכות המחשוב לא הוכנו אליו או גף המחשוב לא ערוך היטב להסתגלות מהירה אליהם.
6. **שינויי מחשוב -** שינויים בלתי צפויים בטכנולוגיות שבשימוש הארגון ואף התיישנות טכנולוגית מחייבים הסתגלות מבעוד מועד ומייצגים סיכון קבוע אליו יש להיות מודע (צידו השני של הסיכוי הגלום בחידושים).
7. **אירועי סביבה חיצוניים -** הסביבה בה פועל הארגון - גאוגרפית וכלכלית, עשויה להציב סיכונים רבים: פגיעה ממלחמות, מעשי טרור ושפל כלכלי, שיובילו אף לאסון ארגוני.
8. **סיכונים משפטיים -** אלו כוללים סיכונים להפסדים כתוצאה מהעדר יכולת לאכוף משפטית הסכמים או מתביעות כנגד החברה. מחלקת המחשוב עשויה להיות כפופה גם לחוקים או תקנים המחייבים ניהול סיכונים כמו הוראה 357 של **בנק ישראל** המחייבת בנקים.
9. **אי-עמידה בלוחות זמנים -** ככל שפרוייקט מורכב יותר, והצוות העובד עליו גדול יותר, כך קל יותר לחרוג מלוחות זמנים, תקציבים ותכונים. כל חריגה כזאת מפחיתה את הרווח מהפרוייקט ויכולה, לבסוף, להפכו לבלתי משתלם.
10. **כניסה לטכנולוגיות לא בשלות -** טכנולוגיות שאינן בשלות אמינות פחות, זמינים פחות מומחים ובעלי ניסיון מהם ניתן ללמוד, ועתידן לרוב אינן מובטח. שקול היטב לפני השקעה.

606.23– הפתרונות בשרוול

אלו האמצעים בעזרתם תתמודד מול הסיכונים האורבים בפעילויות ובפרוייקטי המחשוב בארגונך:

- **ניתוח סיכונים שיטתי -** מעל הכל, יישום ניתוח סיכונים שיטתי ויסודי יכין אותך למזעור הסיכונים ולהתמודדות אופטימלית איתם במידה ואכן יתממשו.
- **ביצוע פיילוט -** יישום מצומצם, למשל בצורת ביצוע פרוייקט פיילוט מחלקתי לפני יישום כלל ארגוני, יספק התנסות ראשונית חיונית ויחשוף סיכונים שקשה לצפות.
- **שימוש בטכנולוגיות סטנדרטיות -** שיטה טבעית לצמצום סיכונים היא גישה זהירה באימוץ טכנולוגיות חדשות. במקומן תוכל להתעמק בחידושים במסגרת טכנולוגיות מוכחות.
- **מודל עסקי בסיכון מופחת -** ישנם מודלים עסקיים שיקטינו מראש סיכונים מובנים ביישום. לדוגמא, מודלים של תשלום לפי שימוש. ראה עוד בתחקיר **600**.
- **ייעוץ מקצועי -** חברות ייעוץ טכנולוגיות רבות מציעות הערכות כלכליות של הסיכונים והתועלות ומסייעות בכך לארגון להחליט אם וכמה להשקיע בכל טכנולוגיה ובכל פרוייקט, וכיצד להתגונן מפני פריצה, השבתה וחשיפת מידע.
- **דיוק בנתונים -** מנקודת מבט של קבלת ההחלטות ושל ההנהלה, הקפדה על דיוק ועומק הנתונים עליהם תתבסס תסייע להבהרת התמונה הכללית של פרוייקט ובכך להתמודדות יעילה עם סיכונים שהוא מציב.
- **שימוש בתוכנת ניהול פרוייקטים -** כלי ניהול פרוייקטים מתריעים על כל חריגה מלוחות הזמנים, מהתקציבים ומהמשאבים - ומאפשרים ניהול יעיל ושמירה על לו"ז תקין.

606.31– כמה עולה לטעות ?

סיכוני מחשוב עלולים לעלות ביוקר רב לארגון. גם ללא הערכה מספרית, ברור למשל הנזק בדוגמא העדכנית הבאה: לפי **InfoWorld**, תקלה במערך אחסון במערכת בסיסי נתונים ב-**Danske Bank** (הגדול בדנמרק) שיתקה 90 בסיסי נתונים והשביתה פעילות באחד משני מרכזי המחשוב למעל יממה. לפי הודעת הבנק, תהליך ההתאוששות ארך כשבוע, לטענתם בגלל שלושה באגים שנחשפו רק במהלכו בבסיס הנתונים **DB2**. לפי **גרטנר**, הערכות בלתי מספקת בארגונים מול הווירוסים **Nimda** ו-**Code Red** הביאה עוד בשנה שעברה לנזקים בגובה מיליארדי דולרים. גם בתחום הצעיר של מסחר מקוון מזהירה **גרטנר** כי אפילו מקרי הונאה קטני היקף יניבו נזקים בשיעור מיליוני דולרים.

על פי **גיגה**, הנסיון לקבוע מדדים לתקציבי מערכות מידע מטעה ואף פוטנציאלית מסוכן, אך מנמ"רים עדיין זקוקים לצידוקים להגנת תקציבים שהם מציעים. לשם כך תוגדר חלוקת התקציב כך, עם שיקולים אלה: **עלויות פעילות מחשוב נוכחיות** ייתפסו חצי מהתקציב עם מרווח טעות של 10% לכל כיוון, ויהיו לרוב זהות או נמוכות ביחס לתקציב הקודם. הצידוקים יגיעו מהמנמ"ר עצמו ומדדים ישמשו לתאור עלויות גבוהות מדי ולא לקביעת מטרות שרירותית. **עלות יוזמות מחשוב חדשות שנדרשות ביוזמת יחידות שונות בארגון** תתפוס שליש מהתקציב עם מרווח טעות של 10% לכל כיוון. נטל ההצדקה יהיה על יחידות אלו וללא יכולתן לשכנע את ההנהלה בנחיצות ההשקעה - מומלץ למנמ"ר שלא לכלול זאת בהצעת התקציב. **עלות יוזמות חדשות למערכות מידע מאגף המחשוב עצמו** תתפוס עוד 17% מהתקציב, עם מרווח טעות של 5% לכל כיוון. היא דורשת הכנה יסודית לשם שכנוע ההנהלה. מאחר ומדובר בתועלות כלל ארגוניות ואסטרטגיות, כמו שיפור רמת האבטחה או השפעה על תהליכים עסקיים, ה"פטרון" - לאחר שכנועו - צריך להגיע מההנהלה. מסיבות פרקטיות לא יהיה זה לרוב המנכ"ל, אלא מנהל בכיר מהיחידה העסקית, ובדרך כלל זו שתרוויח יותר מהיוזמה.

606.32– יתרון לנהג הזהיר

היתרונות לניהול סיכונים יעיל:

1. **צמצום נזקים -** ניהול סיכונים ימנע ויצמצם נזקים לארגון. זאת קודם כל על ידי מניעת התרחשותם. שנית, על ידי כך שבמקרי התממשות סיכון ימצא עצמו הארגון מוכן מבעוד מועד להתמודד עמו.
2. **התראה מוקדמת -** החשיבה והתיעוד המסודרים ומנגנוני הבקרה שיוכנסו לתהליכים הארגוניים, יספקו למפעיליהם התראה מוקדמת יקרת ערך. כך יוכלו להתמודד עימם בעוד מועד, וההנהלה תקבל ביסוס משופר להחלטות עתידיות.
3. **צמצום סיכוני הבלתי ידוע -** מחשבה מוקדמת ויסודית על מצב חדש - נאמר הטמעת מערכת חדשה - יחשוף סיכונים עליהם אולי לא חשבת, בגלל היותם חדשים לך, ממש כמו המערכת עצמה. לדוגמא: המעבר ממערכת ידנית לממוחשבת, עשוי לגרום לכמה ימי תפקוד לקוי.
4. **כח שיכנוע למנמ"ר -** ניהול סיכונים יביא לנכונות גדולה יותר מצד ההנהלה לסמוך על המנמ"ר ועל הטכנולוגיה ש"באמתחתו", כציר קריטי לסיכונים הנחוצים להתקדמות.
5. **גידול בתקציב -** יכולת משופרת זו להצדיק הצעות להשקעה ותקציבים מבוקשים תגדיל הסיכוי שאכן יאושרו לך תקציבים לפרוייקטים בעלי ערך ממשי.
6. **מניעת פגיעה אישית -** בארגון וניהול מושכל ושקוף להנהלה של נושא הסיכונים, תצמצם פגיעה מקצועית אישית. זאת על ידי צמצום הנזקים בהם תהיה מעורב ושיתוף מוקדם של ההנהלה באפשרות להתרחשויות כאלה.

606.33– נבחרת השוערים

ישנם כמה מקורות נוספים בהם תוכל להיעזר ברמה האסטרטגית של ניהול סיכוני מחשוב. בין שרותי הייעוץ:

- **ועדת בזל** היא מקור עולמי מרכזי לנושא הסיכונים, כולל סיכונים תפעוליים שנושא סיכוני ניהול פרוייקטים הוא אחד מהם. קישורים ומעקב חדשות בנושא הוועדה ופרסומיה ראה במקור המצוין הבא - www.baselalert.com
- **מטאור -** מתמחה בייעוץ ומציעה מתודולוגית ניהול סיכונים ייחודית שאומצה לפני שנתיים כ"גילוי דעת" של לשכת מנתחי המערכות. החברה מעבירה סדנאות הכוללות "איתור ומיפוי סיכונים" (יום-יומיים), תיעדוף סיכונים (ביטוי קריטיות סיכון לפי עוצמת הנזק, סבירות ומיידיות התרחשותו. (אורך כיום) ופיתוח תוכניות פעולה (יום עד שלושה ימים). שלבים אלה מיושמים לאורך כל חיי הפרוייקט. לפרטים נוספים ☎ 03-5783520.
- **מתודה -** נוהל **מפת"ח** הנפוץ מתייחס בעיקר לפיתוח תוכנה. גרסה 6 כוללת גם ניהול סיכונים, תוך יכולת לרכז מגוון סיכונים רחב מאוד. המחיר לעמדה **712**$. **מתודה** מספקת גם ייעוץ בנושא ניהול סיכונים ומאפשרת לרכוש **CheckLists** של סיכונים בתחומים שונים. ☎ 03-6133336.
- **קסלמן פתרונות בניהול סיכונים -** **PwC** מספקת לצד ייעוץ גם הדרכה לפי מתודולוגיה בפיתוחה בשם **Executive Approach**. בשיטה זו "מפורק" הארגון ליחידות ותהליכים עסקיים שעל כל אחד מבצעים ומכמתים ניתוח סיכונים. כך מניבים מה שמכונה בחברה ניתוח רב ממדי. ☎ 03-7954850.
- **מכון התקנים הישראלי -** מציע מספר תקנים חשובים בתחום אבטחת מידע וניהול סיכונים במחשוב. תקן ***7799*** ותקן **1495** הם הבולטים. לפרטים ורכישה ☎ 03-6465154.

ארגונים נוספים המסייעים בייעוץ בנושא ניהול סיכונים:

- **ארנסט את יאנג** (☎ 03-6232525)
- **גיגה** (☎ 03-9245524).
- **גרטנר** (☎ 03-6484114)
- **מטה גרופ** (☎ 09-7444474)
- **פילת יעוץ ניהולי** (☎ 03-7679233)
- **קומסק** (☎ 03-9234646)
- **Deloitte Touche** (☎ 03-6085555)
- **EDS** (☎ 09-9708129)
- **HMS (הלפרין שירותי ניהול)** (☎ 03-5223738)
- **IBM Global Services** (☎ 03-5313558)
- **KPMG** (☎ 03-6848000).

גם במסגרת כנסים ותערוכות גדלה כיום ההתייחסות לניהול סיכוני מחשוב בארגון. תוכל כבר לרשום ביומנך כי ב-11 בספטמבר צפויים כנס ותערוכת **OpRisk 2003** בארגון **אדר יזמות** (☎ 03-9730691).

PCאון© למנהלים ומשתמשי מחשב בכירים

606.41 – לעתיד בטוח

כמה תובנות נוספות הבאנו מהשטח:

ד"ר משה אור-גד, מנכ"ל חברת **מטאור** (☎ 03-5783520), מספר שהחברה פיתחה נוהל מתודולוגי לניהול סיכונים בארגון, אותו ניתן להשיג מ**לשכת מנתחי מערכות**. לדבריו, ניהול סיכונים בארגון מתחלק ל-3 סוגים: **1)** ניהול סיכונים בתחילת פרוייקט כדי להבטיח את הצלחתו ולצמצם חריגות (ללא ניהול סיכונים, הוא טוען, כ-60% מהפרוייקטים חורגים בלוח זמנים ובתקציב, וכ-20% ננטשים ונכשלים לחלוטין). **2)** ניהול סיכוני מחשוב כללי בארגון - תהליך של זיהוי סיכונים פוטנציאלים ופעולה לצמצומם. **3)** בחירת פורטפוליו מבין השקעות אפשריות על-פי ניתוח הסיכונים. גישה שיטתית לניהול סיכוני מחשוב כלליים בארגון תתחיל באיתור כל הסיכונים (**מטאור** מזהה מעל 100 סיכוני מחשוב אפשריים), מדידת הסיכון (תוך התחשבות בהסתברות שהסיכון יתממש והנזק שעלול להגרם כתוצאה ממימושו), איתור פעולות לגידור הסיכונים (פעולות שיצמצמו את הנזק, או את הסתברות מימוש הסיכון) ולבסוף ניתוח עלות/תועלת של פעולות הגידור (כדי להחליט אם מחירן משתלם או שעדיף מבחינה כלכלית להשאר עם הסיכון). **משה** מדגיש כי ניהול סיכונים מציע תשואה גבוהה מאוד עבור מאמץ והשקעה קטנים יחסית.

מני צרפתי, סמנכ"ל פיתוח עסקי בחברת **WE!** (☎ 09-9718231) טוען כי היום מנמ"ר צריך לתת טיעונים עסקיים הרבה יותר משכנעים להצדקת כל פרוייקט. לדבריו, פרוייקט שמגיע מאגף ה-IT לא תמיד מושלם מבחינה עסקית, במיוחד בארץ. פרוייקטי **DRP** למשל נוהלו בהרבה מקרים באפס סיכון - ארגונים פשוט הכפילו מערכות מידע לאתר אחר, אבל המחיר הגבוה גרם נזק כלכלי לארגון. לטענת **מני**, מי שצריך להגדיר את הצד העסקי אינו המנמ"ר.

ערד קופ, ראש תחום עסקי וממשלתי בחברת **מתודה** (☎ 03-6133336) אומר כי ההשקעה בניהול סיכוני מחשוב בארץ אינה גבוהה, אך ניתן לראות סימני התעוררות לכך. המלצותיו: להבין שניהול סיכונים נכון מחזיר את ההשקעה וכדאי להציג מחוייבות ניהולית בכירה לנושא לשם העברת המסר על חשיבות ביצוע התהליך. כדוגמה ניתן לציין את האפשרות לחייב מנהלי פרוייקטים בארגון לבצע ניהול סיכונים ולהציגו כלפי ההנהלה. ולבסוף - מומלץ שכל פרוייקט - קטן (כרכישת שרת מסוג חדש) כגדול - ינוהל על פי מתודולוגיות מוכחות כדוגמת מתודולוגיית **מפת"ח** הכוללות את תחום ניהול הסיכונים.

606.42 – רכישות נגד סיכונים

תוכנות ניהול סיכונים אינן בשימוש נרחב לסיכוני מחשוב, אך במידת הצורך תמצא כמה הצעות מעניינות:

• **BindView - bv Control** הוא מחולל דו"חות סיכון אקטיבי דינמי, המסוגל לקבל מידע מכל סביבת **מיקרוסופט נובל** ו-**UNIX**, ללא צורך בהתקנת תוכנת שליטה ובקרה בשרתים. ל-**bv Control** יכולת ביצוע שינוי הרשאות והגדרות במרוכז והוא מגיע עם מאות דו"חות מוכנים מראש לשימושך. **ניו אפליקום** ☎ 09-9598889.

• **Palisade** - מציעה מבחר פתרונות ובהם: תוסף ניתוח סיכונים ל-**Excel** בשם **@Risk** (החל מ-**570$**) המיישם את מודל מונטה קרלו לסימולציית סיכונים, **@RISKAccelerator** (**495$** למעבד) המאיץ סימולציות בעזרת ניצול ריבוי מעבדים, ערכת הפיתוח **@RISK Developer's Kit** (מ-**970$**) ו-**@RISK for Project** (מ-**770$**). - www.palisade.com

• **PwC - TeamRisk** הוא מודול ניהול סיכונים, במסגרת כלי כולל למבקרים ומנהלי סיכונים **Team Mate**. כלי זה מיישם את מתודולוגיית ניהול הסיכונים של חברת הייעוץ **PwC**. המחיר לעד חמישה משתמשים **10,500$**. **קסלמן פתרונות בניהול סיכונים** ☎ 03-7954850.

• **SAS - Risk Dimensions Risk-Management Solution** מטפל בשלושת סוגי הסיכון העיקריים: סיכוני שוק, אשראי וסיכונים תפעוליים. הפתרון כולל מחסן נתונים ומשנע מידע אל **Risk Data Store** עליו מפעילים ניתוחים שונים. כלולים גם ממשקים מובנים למערכות **ERP** שונים וכן כלי ניתוח, תחקור ודיווח. **SAS** מציעה גם פתרונות ורטיקאליים לשווקים שונים דוגמת חברות אנרגיה. **מיה מחשבים** ☎ 09-9712626.

• **ספרים על ניתוח סיכונים** - תוכל למצוא אצל **Risk Publications**. בכתובת - www.riskpublications.com

דגש – הכשרת מנהלים

רק בשנים האחרונות התחילה להתארגן הכשרה מסודרת לצד הכלכלי של עבודת מנהל המחשוב. היום יש מגוון קורסים לבניית תכניות עסקיות והמנמ"רים יותר מעורבים בצוותי ניהול החברה או שיש להם השפעה משמעותית שם.

הכשרות בנושאים אלה תמצא ממקורות רבים: זה יכול להיות **לה"ב** - לימודי הכשרה בניהול במסגרת **אוניברסיטת ת"א** (☎ 03-6437787), קורסים לחשיבה פיננסית ויזמות עסקית כגון אלו שמציעה **ISEMI יזמות** (☎ 03-6424422), קורסים במסגרת חברת ייעוץ כ**מתודה** (☎ 03-6133336) או חברת הדרכה כ**ג'ון ברייס** (☎ 03-7100777).

606.43 – כך תנהל ותת"על

העזר בצעדים אלה ליישום ניהול סיכונים בארגון:

1. **זהה סיכונים** - זהה את הסיכונים השונים, כולל סיכונים הנובעים ממקורות חיצוניים (כלכלה מקומית, מתחרים) או פנימיים (מבנה ותהליכים ארגוניים, מערכות מחשוב ועוד).
2. **הערך סיכונים** - נתח והערך כל סיכון וסיכוי להתממשותו. הערך את השלכות התממשות הסיכון על הארגון. בדוק מהי שרשרת השירות - מהם **כל** מרכיבי הטכנולוגיה. ייתכן ותגלה כי שרת **X** הוא חלק משרשרת השירות ודווקא אלמנט קטן יחסית במסגרתו הוא הקריטי ביותר.
3. **הגדר רמת סיכון סופית** - הערך באופן סופי את רמת כל סיכון מהסיכונים שהגדרת. בסס זאת על מכפלת הסתברות מימושו במידת חומרתו ושקלל לציון בין 1 ל-5 וכדומה.
4. **שקול כדאיות** - אם מדובר בהערכת ניהול לסיכון שאינו הכרחי (בניגוד לסיכון קבוע כאיבוד נתונים קיימים, המחייב גיבויים), הערך כדאיות ההשקעה בו: שקול מה הערך המוסף מול הסיכון ותג המחיר.
5. **טפל בסיכונים בהדרגה** - התחל בטיפול בסיכונים על פי חומרתם. אין צורך להשקיע בהכרח בטיפול בכולם אלא לבצע מדרג סיכונים. על פיו שקול את הצורך בטיפול ואת מידתו על פי ההשקעה הכספית אל מול הסיכון.
6. **הערך להתמודדות** - הכן בקרות (לניטור הסיכונים) ולצידן הכן פתרונות פעילות מונעת (למנוע התממשות סיכונים) ופעילות מתקנת (לגבי סיכונים שלא תוכל למנוע). לאורך זמן דאג להטמיע את הבקרות ולהעריך את האפקטיביות שלהן.
7. **חזור בקביעות על הערכת הסיכונים** - בצע ניתוח סיכונים באופן שוטף לאורך חיי פרוייקט/מערכת ולא רק ניתוח חד פעמי. למשל אחת לתקופה או במסגרת אבני הדרך המרכזיות בחיי פרוייקט.

606.51 – בצל הטרור

יש תחום אחד שבאחריות מנהל המחשוב, שעוסק בעצמו, ישירות, בניהול סיכונים. הכוונה למכלול הידוע כאבטחת מידע: התגוננות מפני נוזקה לסוגיה, האקרים, גניבת מידע וריגול תעשייתי. התמודדות עם הסיכונים תדרוש החלטות כבדות כלכלית וטכנולוגית - ברכש ציוד הגנה או ביתירות ציוד לשם שרידות בשעת חרום. לסיבוך העניין מוסיפה העובדה שאלו מערכות מניעה בלבד ולא מערכות יצרניות ה"מצדיקות" בבירור את ההשקעה בהן.

אופיר זילביגר, מנכ"ל SecOZ (☎ 02-6428543) אומר שמכל איומי האבטחה נראה שוירוסים הם עדיין הדבר המפחיד ביותר בעיני מנמ"רים, מהיותם דבר מוחשי יותר לרובם. נושא ה-**DRP** קיבל לאחרונה תקציבים גדולים משמעותית מאלה שהופנו לנושאי אבטחת מידע רגילים. לדבריו, המלחמה הקלה על מנהלי מחשוב להצדיק השקעות כאלה. שנה שנתיים לפני כן, כשדובר על המשכיות עסקית והתאוששות מאסון, אפשר היה לראות גישה שונה לחלוטין. **אופיר** אומר כי ההתעסקות הטכנית מהווה רק תשתית עבור איש אבטחת מידע אמיתי וזה ממש לא העניין. העניין הוא להבין שההתעסקות באבטחת מידע להקטנת סיכונים מורכבת מהבנת המטרות העסקיות של הארגון, איזה מידע יש בארגון, איך הוא משרת את מטרות הארגון ומהם התהליכים העסקיים שמבססים את הארגון. בגישת אבטחה לא מסודרת - בה מתחילים מהתשתיות - אתה עלול להשקיע בתשתיות לא רלוונטיות. את רמת הסיכון יש למדוד קודם מנקודת המבט העסקית ולא הטכנולוגית, כשתפקיד מנהל המחשוב לתרגם את רמת הסיכון העסקי לו חשוף הארגון, לסיכון טכני. לאחר הערכת סיכונים וחישוב הסיכון, הוא יפנה להנהלה לגבי אופן ניהול הסיכון ושם תתקבל ההחלטה.

606.52 – קח עוד טיפ

העזר בטיפים מעשיים אלה לניהול סיכונים מחושב:

- **קח כל פרמטר כסיכון נפרד -** לדוגמא: **Downtime** של מערכות הוא מרכיב משמעותי ללא ספק, אבל עד כמה? הסיכון תלוי בכל מקרה לגופו. אם מדובר במערכת שמשרתת לקוח פנימי לעניין לא קריטי הסיכון קטן ביחס לשרתי **אינטרנט** בחנות ספרים מקוונת.
- **חלק אחריות -** הגדר במדויק אחראי לכל פריט או סוג מידע הדרוש להערכת הסיכונים. האחראי יהיה הכתובת הרשמית לקבלת המידע המדוייק והעדכני. לדוגמא: מי ידווח על מצב פרוייקט או מי ממונה על מערכת קיימת מסויימת שתפקודה רלוונטי להקמת מערכת חדשה.
- **ראה זאת כניהול השקעות פיננסי -** כהמלצת **גיגה**, זכור שתקציב ההשקעות ב-**IT** דומה להשקעת כסף באפיקים פיננסיים ונהל אותו בצורה זו בדיוק ולפי אותם פרמטרים, בדגש על אופן ניהול התקציב (הבטחת התאמה בין פרויקטים והשקעות לצורכי לקוחות פנימיים, ניהול תקשורות ודיווחים ללקוחות הפנימיים על ביצועי השקעות שונות וכדומה).
- **מיישם בגדול! שכור מומחה -** אם ברשותך מחלקת מחשוב גדולה עם אתגר ניהול סיכונים משמעותי, שקול יצירת תפקיד מבקר פיננסי או קבלת עובד בחצי משרה מאגף הכספים בארגון. כך תספק כתובת מקצועית פנימית וקבועה לצד הכלכלי של ניהול הסיכונים.
- **מזג סיכונים -** השקעה במניעת סיכונים לא מניבה תמורה מיידית כהשקעה במוצר או שירות יצרני. לכן בכדי למזער את העבודה שקול למזג מספר סיכונים לסיכוני על, כך יהיה קל יותר למצוא להם פתרון בפחות עבודה.
- **למד מהעבר -** בצע תחקור על פרוייקטים שכבר הסתיימו, בכדי לאתר ולתעד סיכונים ודרכי טיפול בהם. כך תהפוך את הארגון למה שמכונה ארגון לומד ותמצה השקעה קודמת בפעילויות ניתוח סיכונים.
- **התאם SLA -** תשומת לב לניסוח **Service Level Agreement** עשויה למנוע סיכונים בעבודה מול ספקים. התייחס לסיכונים בתחום בו מדובר, למה שצריך לקבל במסגרת החבילה ודאג שאתה מכוסה מבחינת כל מרכיבי הפתרון. נושא החוזים המשפטיים נעשה לרוב עם **Templates** שיש בארגונים גדולים, אבל אם מדובר בפרוייקט בתחום לא מוכר עדיף להתייעץ עם מומחים לשם ניסוח מדוייק יותר.

606.53 – מדבגים ניתוחים

פיתוח תוכנה הוא נושא מחשובי נוסף בו רבים הסיכונים. מחקר **Standish Group** קבע כי 31% מפרוייקטי המחשוב בפיתוח ומערכות מידע ייכשלו. 52.7% יסתיימו רק לאחר שיבושים רבים ושינויים בלוחות זמנים ותקציבים. בתהליכי וכלי פיתוח מסודרים כבר כלולים אלמנטים מסייעים לניהול סיכונים, שכדאי להכיר ולנצל: עבודה לפי מתודולוגיות פיתוח מספקת שיטה ומסגרת לכך. כלי ניהול תצורה ו-**CASE** (תכנון בעזרת מחשב) מסייעים להימנע מהסתבכות הפרוייקט. עוד בשלב ראשוני של בחירת כיוון פיתוח ניתן לישם מתודולוגיה כנוהל **מפת"ח**: זהו נוהל תקני ומאגר מידע לניהול מכלול פעילויות המחשוב בארגון, מרגע האפיון, דרך בדיקות, הבטחת איכות, והערכה שותפת. **מפת"ח** מאפשר ניתוח סיכונים לכמה חלופות אפשריות לפרוייקט. לפרטים - www.methoda.co.il/maftech.htm **מתודה** ממליצה לנתח סיכונים בכל אבן דרך בפרוייקט.

גיגה מציינת נוהג נפוץ של התאמות תוכנה קיימת לצרכי ארגונים. היא מזהירה כי ביצוע הסבה עצמאי עשוי להיות מסוכן ולהביא להפסדים כספיים, זמן יצירה והטמעה ארוך, תחזוקה בעייתית ולבסוף - פגיעה בתוצאות העסקיות. לכן חיוני לבחון היטב שלושה צידוקים עיקריים ששומעים לכך: **זה חיוני בגלל חזון ארגוני מיוחד** - טיעון שמתאים במקרים בודדים בלבד, דוגמת חברת הענק **וול-מארט**. **גיגה** מציינת כדוגמא הפוכה את **קיי-מארט** שבזמני קושי כלכלי נכשלה במדיניות התאמת יישומים. **זה חיוני בגלל העלות** - אם נראה שאינך זקוק לכל חלקי פתרון מדף בו משתמשים המתחרים - בדוק אם אין חסרון בחזון שלך והאם פתרון חלקי - לא יצא שכרו בהפסדך. **זה חיוני בגלל הגמישות** - תוכנות מוכנות ובשלות כבר מציידות בגמישות רבה שעשויה בהחלט לאפשר התאמה מהירה לצרכיך, גם בלי פיתוח מיוחד. לסיכום, ממליצה **גיגה** גם להתייעץ עם גורם חיצוני, הרואה את הדברים בצורה אובייקטיבית.