היערכות לשינויים הגדולים בבנקאות: טכנולוגיה וחדשנות לצד ניהול סיכונים

המפקחת על הבנקים, ד"ר חדוה בר

כנס הפיקוח על הבנקים

"תמורות במערכת הבנקאית"

20.3.17

מערכת הבנקאות עוברת שינויים גדולים מאוד

- האם אנחנו ערוכים לסיכונים...?

השינויים בבנקאות נובעים ממספר גורמים

- שינויים בהעדפות וציפיות הצרכנים
- המהפכה הטכנולוגית ומהפכת המידע
- סביבת המקרו – בפרט ריביות נמוכות
- רגולציה וחקיקה פרו – תחרותית: הורדת חסמי כניסה וחסמי העברת מידע

הפיקוח מוביל :

- תחרות
- התייעלות
- שינויים טכנולוגיים וחדשנות

פעילות הפיקוח נועדה להשיג לציבור הלקוחות:

- בנקאות שמאפשרת צמיחה (למשקי הבית, עסקים)
- חדשנות בבנקאות (נוחות, הגדלת מגוון השירותים..)
- ירידת מחירים
- דיבידנדים לציבור (כבעלי רוב מניות הבנקים בפנסיה, בגמל..)

קידום המטרות מבוצע תוך הסרת חסמים והגדלת תאבון הסיכון הפיקוחי בנושאי טכנולוגיה ותחרות

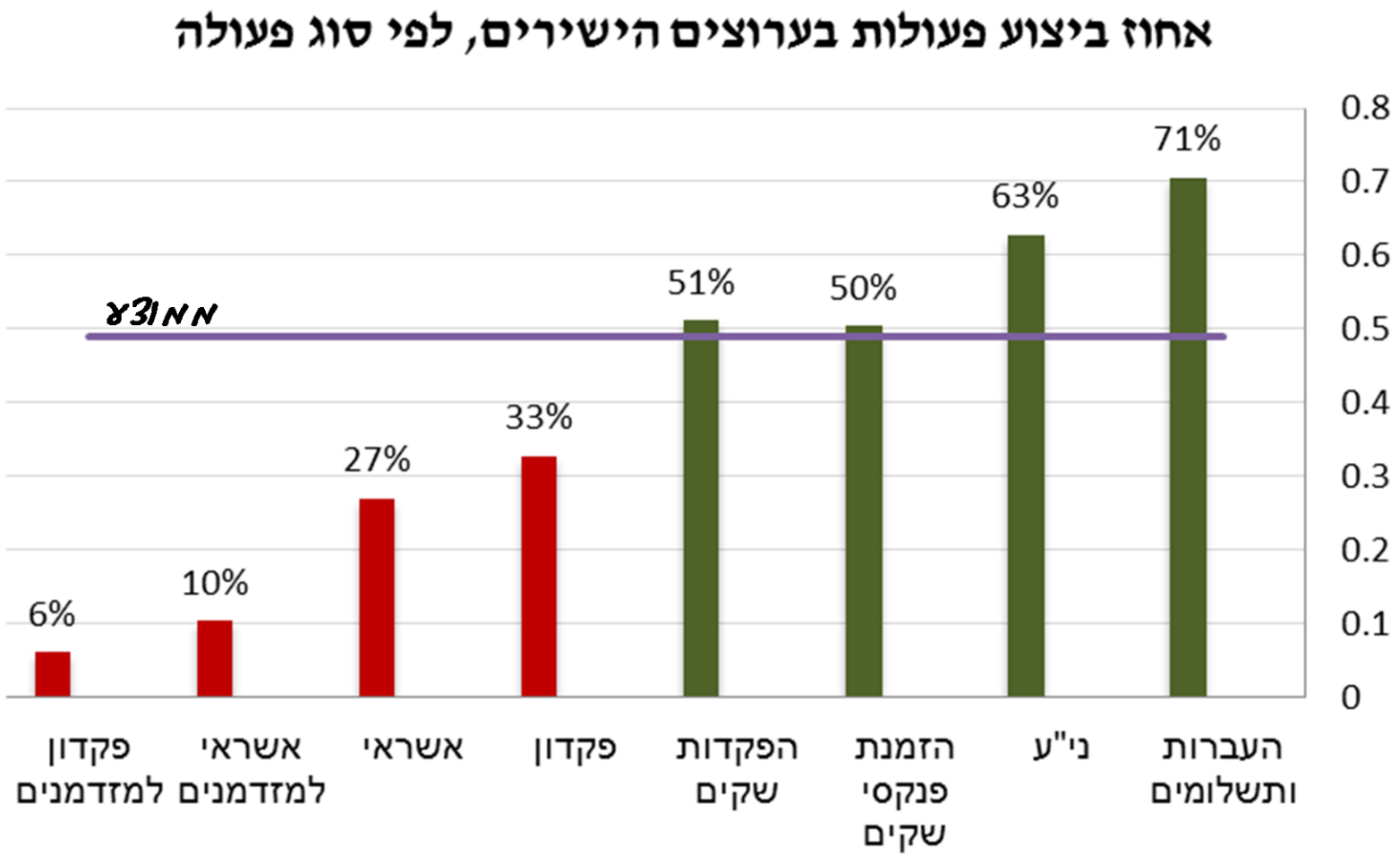
- זאת, כדי לאפשר קידמה ולהגביר תחרות לטובת הצרכנים

הבנקים מקדמים יוזמות טכנולוגיות חדשות רבות:

לטובת הצרכנים ולהתייעלות פנימית

- פיתוח מערכות לניהול קשרי לקוחות (CRM)
- החלפה\ שדרוג מערכות ליבה
- טכנולוגית ענן
- בנקאות בתקשורת ובמובייל
- חשבון דיגיטלי, סניף דיגיטלי, בנק דיגיטלי...
- פיתוח ערוצים ישירים נוספים: צ'ט, מיל
- שת"פ עם Fintech
- Big Data
- "בנקאות פתוחה": העברת מידע הלקוח לבקשתו
- הרחבת השירותים הבנקאיים:
  - ריכוז מידע פיננסי, אפליקציות תשלומים, אפליקציות לייעוץ בתיק השקעות, אפליקציות לליווי ברכישת דירה, סיוע ללקוח בניהול חייו הפיננסיים וחיסכון ועוד...

2016



הציבור הרבה פחות בסניף...:

חצי מהפעילות הבנקאית לא מבוצעת בסניף

הבנקאות הישירה היא במגוון תחומים

לצד ההזדמנויות בשינוי
יש גם סיכונים

לצד ההזדמנויות- הטכנולוגיה החדשה מגלמת סיכונים שונים וגדלים

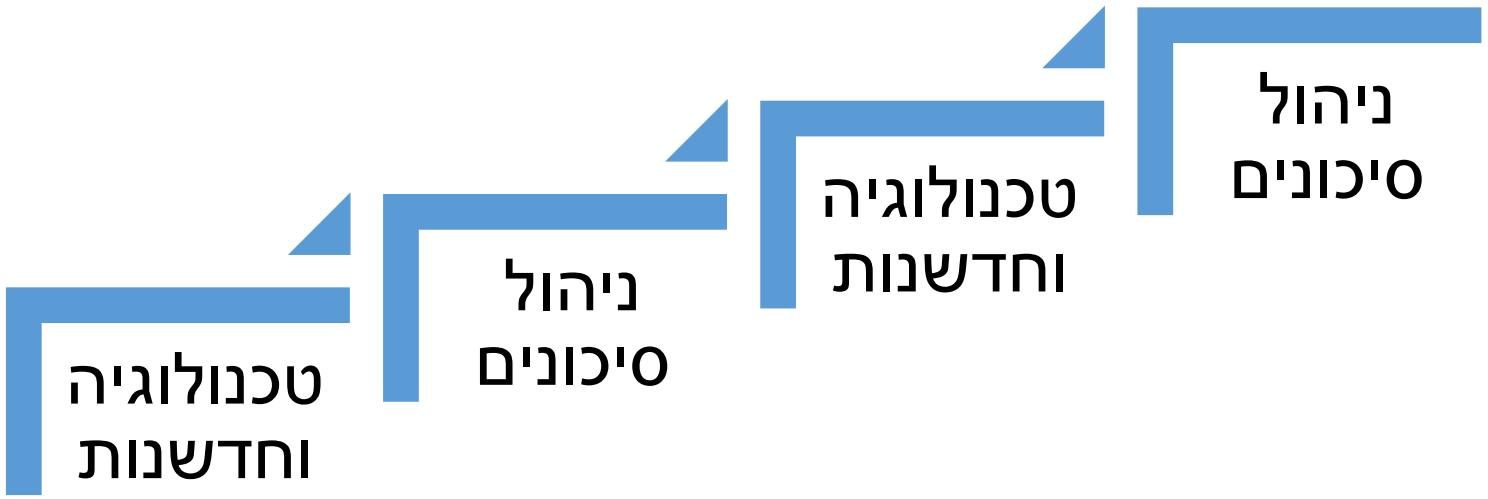
- **הטכנולוגיה מגדילה סיכון של "אירועי סייבר":**
  - **תקיפה טכנולוגית של הבנק מבפנים ומבחוץ**
  - **הונאות רשת וגניבת כספים**
  - **דרישות כופר**
  - **זליגת מידע**
  - **פגיעה בהמשכיות העסקית של הבנק**
  - **תקיפה דרך ספקי צד ג' לבנק**

ב- 2016 התרחשו אירועי סייבר\ טכנולוגיה גדולים בבנקים בעולם

- אנגליה: פריצה לבנק TESCO וגניבה מ-20,000 חשבונות
- יפן: תקיפת 1,400 מכשירים אוטומטיים ומשיכה
- הולנד: העמדת הלוואות פיקטיביות באון-ליין
- ארה"ב, בנק גדול: גניבת מידע ודרישות כופר
- הודו: הדבקת 3.2 מיליון כרטיסי אשראי בנוזקה

דרישת הפיקוח:

על הבנקים "לעלות בסולם" החדשנות בשתי הרגלים



דרישת הפיקוח על הבנקים:

לאמץ חדשנות גם בניהול הסיכונים

- לאמץ טכנולוגיות חדשות גם לניטור הסיכונים בתוך הארגון ומבחוץ (לדוגמא Machine learning)
- להגדיר תוכנית הגנה ייעודית למובייל, לענן, ולכל פעילות / טכנולוגיה חדשה
- לנטר את "הגורם האנושי" בארגון
- לפעול להגברת מודעות וסיוע ללקוחות: במעבר לבנקאות הישירה וגם בניהול הסיכונים הכרוכים בכך

גם לקוחות הבנקים נדרשים לפעול לצמצום הסיכונים הטכנולוגיים

- להגביר ערנות ולהיות חשדניים: לא למסור את הסיסמה של חשבון הבנק; להיזהר במענה למיילים ופתיחת קישורים
- לבצע הגנות על המובייל: סיסמת נעילה; תוכנה למחיקת המכשיר מרחוק; תוכנת אנטי-וירוס
- להימנע משימוש באינטרנט אלחוטי במקומות ציבוריים לצורך גלישה לבנק
- לעקוב באופן תדיר אחר החשבון

השנה עשינו "קפיצת מדרגה" בניהול הסיכונים:

החודש חנכנו את מרכז הסייבר הבנקאי

- לפיקוח יש מחויבות גבוהה להצלחת המרכז

שותפים להקמת מרכז הסייבר

- רשות הסייבר
- משרד האוצר
- כל הבנקים וחברות כרטיסי האשראי
- הפיקוח על הבנקים

מרכז הסייבר הבנקאי יהוה רובד משמעותי בהגנה על הלקוחות והבנקים

- צמצום אירועי הסייבר
- ניהול יעיל של אירועים לאומיים- לכשיתממשו

הערך המוסף של מרכז הסייבר צפוי להיות גבוה.

מפי מנהלי הגנת הסייבר של הבנקים:

- "שיתוף מידע יוצר הפחתת סיכון"
- "מאפשר איתור וטיפול מהיר באירועים"
- "נותן יכולת טכנו – מודיעינית" (סממני התקיפה)
- " יוצר חיבור יכולות עם גופי המדינה המומחים"
- " הסינרגיה בין הבנקים מייצרת ערך מוסף: כולם מותקפים"
- "ערך משמעותי"

לסיכום:
נדרשת חדשנות גם בניהול הסיכונים

והיערכות לניהול אירועים גדולים

- על כולנו להיערך לאירוע סייבר גדול
- הבנקים נדרשים להשקיע בכלים חדשים לניהול הסיכונים החדשים שהטכנולוגיה יוצרת
- הקמנו יחד מרכז סייבר בנקאי חדש, שמהווה "שכבת הגנה נוספת" חשובה ביותר
- על הדירקטוריונים וההנהלות לתת את הטון מלמעלה ולהוביל לשיתוף מידע ואירועים עם המרכז, לצורך הגנה על הלקוחות והבנקים

חדשנות ושינויים
לצד ניהול הסיכונים

תודה