ביטוח סיכוני סייבר- האתגר שבהעברת כשלים בעולם דיגיטלי-גלובלי

Jeimy J. Cano, Ph.D., COBIT Foundation, CFE,
הוא עמית מחקר של קבוצת לימודי טכנולוגיית המידע, תקשורת ומסחר אלקטרוני (GECTI) בפקולטה למשפטים ופרופסור כבוד באוניברסיטה לוס אנדס שבקולומביה.

הביא לתרגום:
שחם גונצ'רובסקי, CPA, MBA, CISA, CRISC

ככל שארגונים נעשים גלובליים ומְמַנפים את פעילות טכנולוגיות המידע שלהם, כך עולה רמת הניראות שלהם, ובמקביל עולה חשיפתם לאיומים בהיקף גלובלי. בעידן הנוכחי, המאופיין ברמת קישוריות ודינמיות גבוהות, המידע נמנה על הנכסים יקרי הערך ביותר. על כן, חיוני להבין את הדרישות ואת האחריות שבפניהן עומדות חברות כאשר הן פועלות בסביבה עסקית שבה מודל יצירת-הערך, המוניטין ויחסי הגומלין עם בעלי העניין, נמצאים בסיכון.

במצב זה, כחלק מהתנהלותם הנאותה, ארגונים מקדמים מימוש ניהול הסיכונים שלהם, ומבצעים זאת ברצינות הנדרשת. ניהול סיכונים קובע מסגרת כללית לפעילויות שארגונים מבצעים, והחלטות שהם מקבלים, לקידומם בסביבה לא יציבה ובתקופות משבר בסקטור העסקי. על אסטרטגיה לניהול סיכונים לקחת בחשבון השלכות הנובעות מהזירה הבינלאומית, שכן אלו משפיעות על הזדמנויות ועל תפיסת העתיד של מועצות המנהלים שלהם.

התרבו הדיווחים אודות פְּרָצות באבטחת מידע, ופעולות בלתי מורשות בתשתיות טכנולוגיות המידע של ארגונים. הדבר מעיד על מגמה של גידול במספר האנשים או הקבוצות, הפועלים במטרה להסב תשומת לב להיבטים מסויימים במציאות של מדינה או של איזור כלשהו; אפשר שמוטיבציה זו מונעת גם להפקת תועלת פיננסית. נעשה שימוש בפרצות לא-קונבנציונליות, היוצרות אוירת לחץ בארגונים ומחלישות את המערך הטכנולוגי שלהם, וחושפות בכך את הצורך בהגברת תשומת הלב לאבטחה ולבקרה של פעולות.

בהתאם לכך, הצעדים והאסטרטגיות הארגוניים, אשר מטרתם להפוך את פעילותם במרחב הדיגיטלי לעמידה יותר, הופכת גלויה למתקיפי-סייבר (Cyber attackers). צדדים שלישיים בלתי מורשים, מעוניינים לא רק לנטוע פחד, אי-ודאות וספקנות בקרבם של אנשי עסקים בכירים, אלא גם להשיג שליטה על מידע קריטי שניתן לנצלו לרעה לצרכים עסקיים, לסחיטה, למודיעין או לפעולה צבאית. כתוצאה, ארגונים הופכים למטרות אסטרטגיות בעלות עניין לאומי ואיזורי.

מכאן, החל שלב חדש של ניהול סיכונים אסטרטגים – שלב שבו נקודת מבט מתמהיל של גלובליות, דיגיטליות ופוליטיקה, מתווה את המציאות של סיכוני הסייבר.

המונח "סייבר" מחייב הבנה לכך, שארגונים לא רק מייצגים את האינטרסים של החברה בתוך קהילה עסקית, אלא הם גם שלובים בדינמיקת הגלובליזציה, אשר בתוכה אינטרסים עסקיים באים לידי ביטוי. בעולם גלובלי, ארגונים עלולים להיות מושפעים ממדינות, התורמות להגדרת התסריט הגיאופוליטי של כלל אומות העולם ולהשפעתו. תאגידים גם משיגים קלות תנועה, הודות לקישוריות המפותחת, ולשימוש האינטנסיבי בטכנולוגיות מידע ותקשורת (ICT), אשר מאפשרות עסקאות וקשרי גומלין המבוססים על מרחב הכלכלה הדיגיטלית, המשרתת קהילות חדשות מסביב לעולם.

ביטוח סיכון-סייבר הוא אמצעי לקיחה בחשבון של סיכוני הסייבר, ושל בחינת תחומי האחריות העסקית החדשים הנובעים מפעילות בזירה בינלאומית. הצגת ביטוח סיכון-סייבר כאופציה לכיסוי, אינה מיועדת לפצות על התרשלות ארגונים במילוי חובת ההגנה על המידע והתשתית הטכנולוגית שלהם.

התפיסות הבסיסיות של ביטוח

ביטוח משמש לרוב, כאסטרטגיית פיצוי במצבים ספציפיים, בהם מעורבים אינטרסים של צד שלישי. במובן זה, נכרת חוזה או הסכם בין הצדדים - המבטח והמבוטח. היבטים, כגון הסיכון בר-הביטוח, ההתחייבות המותנית של המבטח והפרמיה, נבדקים על מנת להגדיר את מסגרת הפעולה ואת הגנה הנחוצה, המבוססת על עקרון תום הלב השורר במערכת יחסים זו. סיכון בר-ביטוח הינו "אירוע מקרי, אשר בשל היותו פתאומי ובלתי צפוי אינו קשור, במקורו ובהתפתחותו, לפעולה אנושית מודעת, בין אם התוצאה רצונית ובין אם לאו"[1]. כפי שניתן לראות, האירוע המבוטח הוא מצב חריג שאינו תוצאה של פעולות מכוונות על ידי בני אדם, וכך הצד המבוטח מוגן מפניו.

חשוב לציין, שקיים סיכון הקשור בהונאות (כגון, מעשה רצוני, התנהגות מזיקה מתוך כוונה) אשר לא ניתן לבטח אותו. אירועים מסויימים (כגון, ארועים שיתרחשו בוודאות), אירועים בלתי אפשריים אירועי עבר

(כגון, אירועים שהתרחשו והיו מחוץ לכיסוי המקורי), אירועים לגביהם קיימות הוראות יחודיות החלות על המבוטח ואירועים הקשורים לסנקציות פליליות שאופיין כלכלי, אינם בני-ביטוח. אין לאירועים אלו, השפעה על הכיסויים או על התשלומים, מאחר שמלכתחילה הם אינם מבוטחים.

יש להבין את האינטרס בר-הביטוח, מנקודת מבט של ביטוח נזקים, כמערכת יחסים כלכלית הקושרת את הצד המבוטח עם אוביקט. בעוד שאינטרס בר-ביטוח הוא הנושא של חוזי ביטוח, חיוני לזכור ש"מספר אינטרסים בני-ביטוח עשויים להתכנס לאותו אוביקט, בשם אותו אדם, או בשמם של בני אדם שונים... ובלבד שהפיצוי, אם האירוע אכן מתרחש, לא עולה על ערכו של האוביקט במועד קרות האירע."[2]

ההתחייבות המותנית של המבטח, ישימה בקרות האירוע (דהיינו, כאשר התנאי הדרוש מתקיים), מועד שבו המבוטח זכאי לפעול למימוש זכויותיו לתשלום מצד המבטח של תגמולי הביטוח המוסכמים. ההתניה מספקת שני מרכיבים עיקריים: ברות-אכיפה ועיכוב. ברות-אכיפה מציינת מתי התחייבות הופכת מתלויה ועומדת למחויבות מעשית (רגע קרות האירוע), עניין התלוי בתנאי הפיצוי המוסכמים. בנוסף, עיכוב (קיום מראש של תביעה רשמית העונה על הנטל הראייתי הבסיסי, הוכחת קרות האירוע והסכום), מתייחס לכך, שאם התביעה לא נענתה על ידי המבטח בתוך חודש, היא נכנסת למצב של ברירת מחדל יחד עם המטרות, הריביות או הפיצוי על נזקים.[3]

לבסוף הפרמיה, כמרכיב חיוני בחוזה ביטוח, היא הרכיב המעביר את הסיכון למבטח. טכנית, מדובר בתוצאה של שיעור, המבוטא באחוזים, מתוך הערך המבוטח. הפרמיה כוללת ארבעה גורמים מרכזיים[4]:

- עלות בפועל של העברת הסיכון (פרמיית סיכון - ניתוח סטטיסטי של ההסתברות להתרחשות)
- עלות אדמיניסטרטיבית (כולל עלויות חידוש הביטוח)
- עלות תיווך (תשלום עמלות לסוכנים)
- רווח צפוי

מושגי יסוד אלה בתחום הביטוח, הם הבסיס לבחינת המציאות החדשה באשר לאחריותן של חברות בהקשר לסיכוני-סייבר.

תחומי אחריות חדשים של חברות במאה ה- 21

ככל שארגונים מתחרים בתרחישים דיגיטליים ביותר יחד עם מעורבות גבוהה מצד גורמים חיצוניים בפעילותם, כן תלוי המידע בעל הערך הרב ביותר לארגון, בעיבוד מדוייק על ידי משתמשים להם גישה אליו. מכך מתחייבת נקיטת סדרה של נוהגים לאבטחה ולבקרה, שעל כל אחד מהצדדים המעורבים ביישום מחזור החיים של המידע לתקף.

אם האמור נכון, אזי הסיכון לאבדן ו/או לדלף של מידע מתפתח לדאגה קריטית של ארגונים, שכן התממשות סיכון מסוג זה, עלולה לחשוף ארגונים לפגיעה במוניטין, לאבדן של לקוחות, של יתרון תחרותי ושל שווקים; זאת, בנוסף לקנסות, פעולות תיקון וסנקציות הרגולציה. אלו כרוכים בעלויות ובפיצויים אשר, בהיעדר היערכות נכונה ונקיטת צעדי מנע, עלולים לפגוע ביכולתם של ארגונים להמשיך לפעול בטווח הקצר והארוך[5].

מידע הפך למשאב הטבעי החדש של המאה ה- 21 כי הוא מאפשר פעילות בעולם המצוי בתנועה מתמדת ונחלק, בדרך כלל, בין שחקנים שונים. הוא נושא עימו סיכון שיש לזהותו ולהתייחס אליו, על מנת לנקוט בצעדי מנע המקדימים השפעות שליליות פוטנציאליות בשל עיבוד לא תקין. הדבר מחייב מתן ביטוי להתנהלות נאותה והבטחת סטנדרט מינימלי, אשר כוללים חובת זהירות מצד אנשים, יכולת חיזוי במצבים שליליים בעיבוד מידע, הפעלת תקן לטיפול נאות באבטחת מידע, ומקבץ של אמצעי זהירות סבירים, המצביעים על גישה פרואקטיבית כלפי נזקים העלולים להיגרם.[6]

רבים מגורמי הפרצות באבטחת מידע בלתי צפויים; עם זאת, ניתן למנות אחדים מהגורמים השכיחים ביותר המתרחשים במהלך העסקים הרגיל:[7]

- מחשבים או מכשירים ניידים שאבדו או נגנבו
- העברה לא מורשית של נתונים להתקני USB
- סיווג ומיון לא הולם של מידע רגיש
- גניבת נתונים על ידי עובדים או צדדים שלישיים
- הדפסה או העתקה של נתונים רגישים על ידי עובדים
- תגובה לא מספקת לחדירות או פריצות אבטחה
- הפצה בשוגג של נתונים רגישים
- שימוש בסמאות חלשות ו/או ידועות
- שיח במרחב ציבורי אודות נתונים רגישים
- ניטור בלתי מורשה של תקשורת

מסיבות אלה, דרושה סדרה של תחומי אחריות תאגידית חדשים, בייחס לעיבוד מידע הקשור לתהליכים ואינטראקציות ממוחשבים (בין אם הם מופעלים על ידי הארגון או על ידי צדדים שלישיים) לתמיכה במודל יצירת-הערך של החברה. דהיינו הבנה, שבמרוץ ליעילות, טכנולוגיות מידע ותקשורת (ICT) ימלא תפקיד מרכזי, שכן באמצעות הגברת רמת האוטומציה, ארגונים יהפכו ליעילים וזריזים יותר. עם זאת, תלות זו תחשוף ארגונים לפגיעויות ולכשלי אבטחה ובקרה שזוהו לעיל.

בניהול סיכונים, ישנן גישות שונות לסיכון: קבלה, צמצום והעברה. ארגונים מבינים את הרגישות של נושא זה בכל הקשור להגנה על האינטרסים שלהם, ולוקחים זאת בחשבון בפעילות הרלבנטית. על כן , הארגונים מגדירים תוכניות עיבוד הכוללות היבטים אנושיים, נהליים וטכנולוגיים אשר מכוונות לסגור פרצות מזוהות ולצמצם את רמות החשיפה שנותחו. כמו כן, ארגונים מגדירים ביטוח כדרך להעברת הסיכון הדורשת, מהצד המבוטח, יישום אפקטיבי ועקבי של נהלים להגנה על נתונים.

על אף זאת, ההשפעות של אירועי אבטחת מידע - אלו שזוהו, ואחרים המופיעים לראשונה - אפשר שלא יהיו כלולות בניתוח הסיכונים. לתוצאות של אותם אירועים, עלולות להיות השלכות מכבידות וכרוכות בפיצויים, המערערות את התחזיות הטובות ביותר שמפעילים ארגונים באסטרטגיה שלהם לצמצום והעברה של סיכונים כגון אלו. לכן, הפעילות הדיגיטלית של ארגונים מחייבת בחינה של הצעות להעברת סיכונים, על מנת לגבש נקודת מבט מדוייקת יותר של מציאות

זו, ועל מנת להתגבר על תנאי ביטוח מסורתיים בתחום זה, כגון טעויות או השמטות באספקת שירותים טכנולוגיים, הפרה של זכויות קניין רוחני, נזקי גניבות באמצעות מערכות עסקאות אלקטרוניות, ופשיעת מחשב[8].

הבנת תחום ביטוח סיכוני סייבר

כיום, פוליסות ביטוח, המוגדרות כמסמכים המכלים את חוזה הביטוח[9], כוללים סיווגים וכינויים מרובים על מנת לקבוע את היקפן, ואת ההגבלות החלות בהן. לעניין ביטוח סיכוני סייבר, כללי מדיניות לזיהוי סיכון מסווגים אותו במסגרת "כל הסיכונים" (All-Risks) ו"סיכון נקוב" (Named-Risk). בעוד שהראשון, מכוון לכיסוי האינטרס בר-הביטוח בהתייחס לכל סיכון שאינו מוחרג בחוזה, או אלו המבוטחים משפטית מכוח הסכמה מפורשת (מוסכם עם המבטח), השני - מיועד לכסות את האינטרס בר-הביטוח של הסיכון המוגדר.[10]

מנקודת ראות הצד המבוטח, שיטה מסורתית זו, מאמצת את הקשיים המקובלים בהבנה, לפי החוזה, את זיהוי הסיכון על פי הגדרתו הבסיסית וסעיף החרגה אחד או יותר.[11] סעיפי החרגה מוגדרים כנסיבות שבהן הסיכון, כהגדרתו, אינו מכוסה על פי בחירת המבטח. בהקשר זה, ביטוח סיכוני-סייבר מצוי בצומת הדרכים בין המבטח, הכיסוי המוצע וההחרגות המוגדרות, במענה לצרכים, לבקשות ולדרישות של הצד המבוטח. זאת, משום שמורכבות סיכוני-סייבר מחייבת הבנה של משתנים אנושיים פרוצדורליים, טכנולוגיים ומשפטיים, שהאינטראקציה ביניהם מספקת תרחיש תוצאות התלויות בכל מקרה ומקרה.

עם זאת, הכיסוי של ביטוח סיכוני-סייבר כולל היבטים הדומים לפוליסות ביטוח כל הסיכונים, למשל:[12]

- אחריות כוללת לפשע באמצעות האינטרנט
- רכוש (נתונים אינם נחשבים רכוש)
- טעויות והשמטות
- חבות מקצועית
- חבויות דירקטורים ונושאי משרה
- חבות בגין נוהלי העסקה (פעולות של העובדים)
- הפרעה לפעילות העסקית
- סחיטה וחטיפה
- חבות קבוצת עובדים (עובדי מפתח)
- כיסוי ביטוח חיים של עובדי מפתח
- כיסוי חבויות מדיה
- הפרות חובת הנאמנות ופשיעה
- כיסוי אבטחת רשת
- קניין רוחני
- ביטוח פטנטים
- כיסוי אלימות במקום העבודה

הכיסויים הניתנים על ידי הסוכנים הגדולים לביטוח סיכוני-סייבר, קשורים לרכוש וגניבות, וכן לחבויות[13]. **איור 1** מסכם את הכיסוי הטיפוסי.

מחקרים עדכניים אודות ביטוח סיכוני-סייבר, מצביע על התפתחות משמעותית בתחום ניתוח הכיסויים, עובדה המשקפת הבנה גוברת של המורכבות המאפיינת סיכוני-סייבר. מחקר שהושלם לאחרונה, הציג מסקנה שלפיה יש לראות בהתקפות סייבר את האתגר הכלכלי והלאומי החמור ביותר, אשר בפניו ניצבות ממשלות וארגונים בעולם[14]. על בסיס הבנה זו, המחקר מפרט את גורמי הסיכון הכרוכים באתגר זה:

- חבות משפטית
- פְּרָצות אבטחת מידע
- פגיעה בפרטיות
- גניבת-סייבר (Cybertheft)
- ריגול-סייבר (Cyberespionage)
- סחיטה (Cyberextortion)
- טרור-סייבר (Cyberterrorism)
- אבדן רווחים
- החזר עלויות
- נזק תדמיתי
- פגיעה בהמשכיות עסקית / שרשרת אספקה
- איומי סייבר על תשתיות לאומיות קריטיות

בהתבסס על סיכון זה, הסקר מתאר כיסויים מסויימים, הכוללים אספקטים כגון:

- פרטיות המידע
- פְּרָצות ברגולציות, עיצומים כספיים וענישה
- הפרעה לרשתות עסקיות
- נזק לנתונים וסחיטת-סייבר
- ניהול משברים ותגובות לגניבת זהויות (כולל עלויות בגין תחקור ראיות)

בנוסף, מחקרים המתמחים בעניינים אלה, מצביעים על כך, ששוק הביטוח לוקה באסימטריה בין הצד המבוטח לצד המבטח באשר למידע, במיוחד ככל שהדבר ממוקד בהפסדים ראשוניים בפוטנציה (לדוגמה, אבדן ישיר של מידע או נתונים, השעיה של פעילות), ופחות כאשר מדובר בנזקים משניים

איור 1- הכיסויים המוצעים על ידי חברות ביטוחי-סייבר הגדולות ביותר

	כיסוי
רכוש וגניבה	הרס של מידע או של תוכנה
	התאוששות מוירוסים או מקוד זדוני אחר
	הפרעה לפעילות העסקית
	מניעת שירות (DoS)
	גניבת מידע
	סחיטה קיברנטית
	הפסדים כתוצאה ממעשי טרור
חבות	הגנת רשת
	נזק למדיה אלקטרונית או לתכנים
	הפרה של חסיון הנוגע לפרטיות

מקור:
Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala, "undergraduate thesis, Universidad de San Carlos de Guatemala,2009, p.70, *http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf*

(לדוגמה, עלויות עקיפות, ירידה במוניטין, השם הטוב, אמון הלקוחות, עוצמה אסטרטגית, אבדן לקוחות). בהתרחשות אירועים, אומדן התביעות יקבע על פי הערכות כלכליות המייצגות את המצב התפעולי של הארגון (הפסד ראשוני), והשארת הנזקים משניים כפופים להערכות סובייקטיביות המבוססות על התנסויות והשוואות עם תהליכים דומים. דבר זה, יוצר חוסר איזון בהגנה, אשר פועל לעיתים לטובת המבטח, ולעיתים לטובת המבוטח[15],[16].

ניתן להסיק, שביטוח סיכוני־סייבר נועד למנוע את ההיקף ואת ההתפשטות של אירוע, ולשאת בסכום הנדרש לצורכי תיקון, החלפה או הקמה מחדש של הנכסים אשר נפגעו כתוצאה מהתממשות סיכון הסייבר.

המו"מ המשתמע מסוג זה של מדיניות, קשור בהחרגות. החרגות, הן נסיבות או אירועים המוצאים אל מחוץ לכיסוי המבוטח ומצויינים בצורה מפורשת בפוליסת הביטוח. החרגות אלו, קשורות בדרך כלל לסיכונים שלא ניתנים לביטוח שהוצגו לעיל, וכוללים לדוגמא: התיישנות הנכס המבוטח, רשלנות בלתי נסלחת או ביצוע לקוי של התחזוקה דרושה להפעלתו התקינה של הנכס המבוטח; וכן נזקים למבוטח או לצד שלישי כתוצאה מפעילות מסחרית, תעשייתית או מקצועית שונה מזו הנקובה בפוליסה[17].

החרגות מעניקות מענה לדרישה מהנהלות להבטיח את האינטרס המבוטח, אשר, בכל הנוגע לסיכון־סייבר, משמעו בחינה מערכתית של הסיכון בהקשרו הספציפי לארגון. היינו, נקודת מבט שכוללת הבנה של קשרי הגומלין של הארגון מעמדתו העסקית, קשרי הגומלין שלו עם קהלים ובעלי עניין, וכן עם הממשל והניהול של טכנולוגיות המידע, במטרה לעמוד על הקשריות רבת-המימדים הקיימת בפרקטיקה זו.

באופן דומה, אבטחת מידע ממלאת תפקיד מרכזי בביטוח סיכון־סייבר, מפני שהמבטח דורש הבנה של המידע כנכס אסטרטגי, המהווה את הבסיס ליחסים הפנימיים והחיצוניים של החברה, כמו גם של האחריות המשותפת לניהול המידע ולבקרה עליו עם הצדדים השלישיים המעורבים. בתרחיש זה, צדדים שלישיים גם נכללים בקטגוריה של גופים שותפי־אחריות, ועליהם להיות מחויבים לנוהגים טובים, כלומר-עליהם לשתף פעולה במניעת סיכון־סייבר בחברה המתקשרת בחוזה.

מסקנות

על מועצות המנהלים של ארגונים לכלול שיקולי סיכון-סייבר, בעת סקירתם את הסיכון האסטרטגי של חברות. התעלמות מפרשנות זו של הדינמיקה העסקית העכשווית (השלכותיה ניכרות במקרים בינלאומיים מרובים כגון אירועי Target, JPMorgan Chase, Sony ו- Office Depot), משולה לציפיה לתרחישי משבר שבדרך כלל אינם ידועים מראש, וששההתמודדות עימם מחייבת פעולות מיוחדות ומתואמות על מנת לצמצם את השפעתם המזיקה.

בפרקטיקה זו, על חברי ההנהלה לא רק ללמוד ולהכיר את המציאות החדשה[18], אשר בדרך כלל באה לידי ביטוי בכשלים גדולים ובפרצות אבטחה, אלא עליהם גם להבין את רמות המוכנות שיש לארגון בהתמודדות עם מצבים דומים. הכרחי להקים את אמצעי המנע והרחבת הגנה הדרושים, לכיסוי אספקטים רלוונטיים, אשר הפעולות השוטפות מכסות חלקית בלבד.

ביטוח סיכון-סייבר מצטייר כאופציה שיש לשקול כל אימת שפרקטיקות אבטחה ובקרה נדרשות לחברות על מנת להגביל את האפקט של התקפות סייבר מאסיביות ומתואמות – חלקן למטרות סחיטה או ריגול-סייבר – העלולות לפגוע בנכסי המידע האסטרטגיים של החברה, בזהותם של אנשיה או באסטרטגיות עסקיות שלהן, ואף עלולות לסכן את תפעולן של תשתיות קריטיות של מדינות. בדומה לאמור, ביטוח סיכון-סייבר כולל פרשנות קריטית של הרכוש הבלתי מוחשי של החברה בתרחיש של אופרציה דיגיטלית, ומשולבת עמוק בדינמיקה של החברה עם ניראות גלובלית.

ביטוח סיכון-סייבר, מציג הבנה של קשרי הגומלין במערכת האקולוגית הדיגיטלית, במטרה להבין את המשמעות של רמות הסף המותרות לאבדן ערך. הדבר מקדם הפעלת שיקול דעת בדבר האוביקט המגדיר את אומדן להפסד מירבי על ידי ארגון, עם פרופיל יכולת שרידות הכולל שורת פעילויות של החברה.

ככל שגדלה ההבנה של התרבות הארגונית הנוגעת לאבטחת מידע, של זמינות יכולות התאוששות והמשכיות, של הידע על פגיעויות עסקיות מתעוררות, ושל אפיון תוקפים אפשריים - כך גדלה המוכנות והתגובה של החברה מפני סיכון-סייבר.

עולם ביטוח סיכון-סייבר ימשיך להתפתח בהתאם לאתגרים ולדרישות השוק וכתוצאה מהופעתן של טכנולוגיות משבשות ובלתי מסורתיות. הכרחי להיות מודעים, להשפעות של כשלון בלתי נמנע, על מנת להבין את הכיסויים וההחרגות המוצעים בחוזי ביטוח, בעוד שחברות ביטוח מתחילות ללוות ארגונים, תוך שהן פועלות כישויות משגיחות על מערכות המידע, ניהול התקשורת ועיבוד מידע.

מראי מקום

[1] Ordonez, A.; *Elementos esenciales, partes y carácter indemnizatorio del contrato*, Insurance law lesson no. 2, Universidad Externado de Colombia, Bogota, Colombia, 2002, p. 10

[2] *Ibid*., p. 32-33

[3] *Ibid*., p. 48-51

[4] *Ibid*., p. 42

[5] Ernst & Young, *Data Loss Prevention. Keep Your Sensitive Data Out of the Public Domain. Insights on Governance, Risk and Compliance*, October 2011, www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

[6] Triump, I.; "Confronting the Legal Liabilities of IT Systems," *EDPACS: The EDP Audit, Control, and Security Newsletter*, 46(2), 2012, p. 11-16

[7] *Op cit* Ernst & Young, p. 6

[8] Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala," undergraduate thesis, Universidad de San Carlos de Guatemala, 2009, http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf

[9] Ramirez, E.; Specialization in Insurance course, Universidad Externado de Colombia

[10] *Ibid*.

Insurance law lesson No. 3, Universidad Externado de Colombia, Bogota, Colombia, 2004

[16] Bandyopadhyay, T.; V. Mookerjee; R. Rao; "Why IT Managers Don't Go for Cyber-insurance Products,"*Communications of ACM*, 52(11), November 2009, p. 68-73

[17] Generali Seguros; "Generali negocio seguro. Condiciones generales y condiciones generales específicas,"http://62.97.131.36/rep_documentos/phogar/GENERALI-CCGG-COMERCIOS.pdf

[18] Rai, S.; *Cybersecurity: What the Board of Directors Needs to Ask*, ISACA-IIA, 2014,www.theiia.org/bookstore/downloads/freetoall/5036.dl_GRC%20Cyber%20Security%20Research%20Report.pdf

[11] Ordonez, A.; *Cuestiones generales y caracteres del contrato*, Insurance law lesson No. 1, Universidad Externado de Colombia, Bogota, Colombia, 2001

[12] Drouin, D.; "Cyber Risk Insurance: A Discourse and Preparatory Guide," GIAC Security Essentials Certification, 2004, www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412

[13] *Op cit* Garcia

[14] Carpenter, Guy; Ahead of the Curve: *Understanding Emerging Risk*, 2014, www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/AheadoftheCurve-UnderstandingEmergingRisks.pdf

[15] Ordonez, A.; *Las obligaciones y cargas de las partes en el contrato de seguro y la inoperancia del contrato de seguro*,

Quality Statement:

This Work is translated into Hebrew from the English language version of *Cyberinsurance – the Challenge of Transferring Failure in a Digital, Globalized World* published in the *ISACA Journal* by Shacham Gonczarowski with the permission of the ISACA. Shacham Gonczarowski assumes sole responsibility for the accuracy and faithfulness of the translation

הצהרת איכות:

העבודה מתורגמת לעברית מהגרסה בשפה האנגלית של *Cyberinsurance – the Challenge of Transferring Failure in a Digital, Globalized World* על ידי שחם גונצ'רובסקי בהסכמת ISACA®. שחם גונצ'רובסקי נוטל על עצמו אחריות מלאה על הדיוק והנאמנות של התרגום.