

תוכן עניינים

2.....	מבוא
3.....	1. מבט כללי על תופעת אי-דיווח התקפות סייבר
4.....	2. תחליפי מוסר
6.....	3. עקרונות מוסר
8.....	4. אי-דיווח התקפות סייבר – קווים לפתרון
10.....	סיכום
11.....	מקורות

מבוא

חברות רבות שמנהלות את העסקים שלהם באמצעות האינטרנט ושומרות על מאגרי נתונים שונים, הינן חשופות בין הייתר לסיכוני התקפות סייבר. אחד מהחששות הבולטים של העסקים והצרכנים הם כי הפרטים האישיים של לקוחות יחשפו בפני עברייני סייבר והדבר ינוצל נגד הלקוח ונגד העסק (Raghavan, Desai, & Rajkumar, 2017, p. 10). תאגיד לעיתים עשוי להימנע מגילוי נאות כלפי לקוחותיו על כך שנתוניו האישיים נפרצו וכעת חשופים לגורם נוסף. במצב זה הצרכן כלל לא יודע שנתוניו האישיים נפרצו וכעת גם הוא חשוף למקרי הונאה כמו שימוש בנתוני אשראי וחשיפת סיסמאות (Morgan, & Gordijn, 2020, p. 123; Skinner, 2019, pp. 241-243). החל משנת 2011 חברות הנסחרות בבורסה בארה"ב מחויבות על פי חוק לחשוף את בקורות הסייבר, הסיכונים והפגיעות שלהם. אולם בנקים ותאגידים ציבוריים רבים אינם ממהרים לחשוף את סיכוני הסייבר שלהם ואת העבודה כי הם היו קורבנות לסייבר, הן משום ההשלכות הכלכליות הפוטנציאליות, והן משום שהתקיפה עצמה לעיתים נותרת סודית מעיני הציבור. לצד זה החוק האמור תקף רק לגבי חברות ציבוריות בלבד ולא לארגונים פרטיים אחרים שאינם נסחרים בבורסה (Skinner, 2019, pp. 241-243). **שאלת המחקר:** באיזה אופן ראוי שתאגידים שעברו התקפת סייבר ינהגו כלפי דיווח הלקוחות שלהם?

בפרק הראשון בעבודה אסקור את מאפייני התופעה של אי-דיווח התקפות הסייבר, את הסיבות לאי-הדיווח וההשלכות לכך. פרק זה יאפשר ליצור הבנה מקדימה על הנושא ומדוע חברות בוחרות להימנע מדיווח על התקפות סייבר למרות כי הן מבינות בהחלט את ההשפעה של ההתקפות על הלקוחות שלהם כמו הפוטנציאל למעשי מרמה והונאה. הפרק השני בעבודה יתמקד בתחליפי המוסר. בפרק זה אציג את תחליף השוק והחוק. השוק החופשי מעודד את התאגיד לפעול למען האינטרסים המשותפים שלו ושל הצרכן אחרת הצרכן עשוי לנטוש את התאגיד לטובת תאגיד אחר אמין יותר. אולם השוק שחופשי לא תמיד מעודד שקיפות וחשיפת מידע הן משום שחשיפה מוקדמת של התקפת הסייבר עשויה לפגוע במאבק נגד ההתקפה והן מתוך החשש של התאגיד לאבד לקוחות. תחליף נוסף הוא החוק. הפרק יציג כי כבר משנת 2011 ישנו חוק בארה"ב המחייב את התאגידים לדווח בפומבי על התקפות סייבר שהם חוו. אולם החוק לעיתים הינו כללי ומאפשר לתאגיד לפרסם הצהרה לקונית מבלי להזהיר לקוחות באופן פרטני וכן החוק מיעד רק לחברות ציבוריות הנסחרות בבורסה ולא לחברות פרטיות. נתונים אלה מלמדים כי תחליפי המוסר לא תמיד יעילים כלפי התנהלות התאגידים.

הפרק השלישי בעבודה יתמקד בעקרונות מוסר. עיקרון התועלתנות יראה כי מצד אחד אי-דיווח מונע פאניקה מסחרית מיותרת, אך מצד שני מאות מיליוני לקוחות חשופים למקרי הונאה ולא פועלים להגנתם. עיקרון החובות מראה כי תאגידים מצהירים כי הם מתייחסים ללקוחות שלהם בכבוד והדדיות, אך מצד שני כאשר ישנה התקפת סייבר התאגידים לעיתים מסתירים מידע מהלקוחות ובכך נותר פער בין ההצהרות לבין הייחס ללקוחות בפועל. עיקרון הזכויות מתמקד בזכות לפרטיות וזכות הקניין, והוא מראה כי מידע אישי של הלקוח המוחזק אצל התאגיד הינו מידע אישי של הצרכן והן רכוש משותף של התאגיד והצרכן, ולכן התאגיד מחויב לעדכן גם את הלקוח בנושא פריצה וגניבת הנתונים האישיים.

הפרק הרביעי יספק קווים לפתרון הבעיה. שימוש במודל בעלי העניין יראה כי התאגיד אינו מחויב רק למחזיקי המניות אלא גם חלה חובת דיווח לגורמים אחרים שמושפעים מהתאגיד כמו הלקוחות. כמו כן הפרק יראה כי ניתן לסווג את תוכן הדיווח, כאשר גניבת מידע אישי של הלקוח מחייב דיווח מידי ללקוח; מידע אישי ומסחרי של התאגיד שעלול לסכן את התאגיד יחייב דיווח רגולטורי; ומידע כללי – כמו גילוי התקפת סייבר, ניתן לבצע הצהרה כללית לציבור. תהליכים אלו יובילו לפעילות בת-קיימא המאפשרת לשמור על האינטרסים של הצרכן והתאגיד במשותף.

1. מבט כללי על תופעת אי-דיווח התקפות סייבר

התקפות סייבר מחולקות לשני ממדים: פריצה למערכות ממוחשבות בכדי לגרום נזק, לשנות ולשבש את פעילות המערכת. התקפות סייבר כיום הינן מהוות איום כמעט על כל סוגי הארגונים וזאת משום ההשלכות הפוטנציאליות של ההתקפות, החל מפגיעת פעילות הארגון ושיתוק המערכות, פגיעה במוניטין, הוצאות כספיות על תיקון הנזקים, שיפור אבטחת המידע, פגיעה בלקוחות, הפסדים כספיים כתוצאה ממעשי מרמה או גניבת מוצרים וזכויות יוצרים (Héroux, & Fortin, 2020, p. 75).

לפי הערכת חברת נורטון – המתמחה באבטחת מידע, וחברת Acquisdata המתמחה במידע פיננסי דיגיטלי, כ-978 מיליון בני אדם היו קורבנות לסייבר בשנת 2017 בין אם באופן ישיר כאשר בוצע פריצה למחשבים האישיים ובין אם באופן עקיף כאשר בוצעה פריצה למחשבי תאגיד מסוים וממנו נגנבו פרטי מידע אישיים על לקוחות. כתוצאה מהיקף התקפות הסייבר העולמיות, הדבר הוביל לעליה בשוק הגנת הסייבר שנאמד ב-96 מיליארד דולר בשנת 2018 ועתיד לעלות לכדי 113 מיליארד דולר עד סוף שנת 2020. אולם בעוד שחברות אבטחת מידע נהנות מהכנסות עצומות בתחום הגנת הסייבר, הרי שחברות שחוו התקפות סייבר סובלות מהפסדים מהסיבות המגוונות שהוצגו מעלה. בשנת 2015 היקף ההפסדים על התקפות סייבר נאמד ב-400 מיליארד דולר בעבור חברות עסקיות בלבד; ובשנת 2017 היקף זה נאמד כבר ב-600 מיליארד. אולם חישוב של הפסד כספי כולל עבור חברות פרטיות, מוסדות מחקר, מוסדות מדינה ואנשים פרטיים הגיע לכדי 1.75 טריליון דולר באזור אסיה פסיפיק בלבד בשנת 2017 (Acquisdata Ltd. 2018, pp. 5-6).

אחד האתגרים השכיחים בהתקפות סייבר הוא גניבת המידע של הלקוחות. החשש הגדול עבור הלקוח הוא כי מידע אישי שלו נחשף לכל עבר והדבר עשוי להוביל למעשה הונאה, מרמה, סחיטה ומטרות פליליות אחרות. בעבור החברה המסחרית הדבר עלול להוביל לנטישת לקוחות והוצאות כלכליות גדולות בכדי להתמודד עם הנזקים השונים. מתוך כך לעיתים חברות נמנעות מגילוי התקפת הסייבר עליהן. דוגמה מעניינת לכך היא חברת Equifax האמריקנית המתמחה בפעילות אשראי והיא מחזיקה במידע פיננסי של יותר מ-800 מיליון צרכנים בעולם. בשנת 2017 החברה ספגה התקפת סייבר שהובילה לגניבת מידע אודות 143 מיליון לקוחות – מרביתם אמריקנים. החשש של החברה היה כי הדבר יוביל לנטישת לקוחות, תביעות משפטיות והוצאות גדולות ולכן החברה נמנעה מזה חודשים רבים מדיווח ללקוחות שלה כי הנתונים האישיים והפיננסיים שלהם נפרצו ונגנבו ורבים מהם היו עשויים להיחשף למעשי הונאה מבלי לדעת על כך. תהליך זה נודע רק לאחר שמנהלי הארגון החלו למכור מניות של התאגיד באופן מחשיד מהחשש כי הערך של המניות ירד כאשר יתגלה היקף הפריצה. באופן דומה תאגיד יאהו Yahoo המתין כמעט שנתיים עד שדיווח כי התאגיד עבר התקפת סייבר בשנת 2014 שחשפה את פרטיהם של מיליוני לקוחות, וזאת מהחשש לפגיעה בתדמית הארגון (Skinner, 2019, p. 241).

מבחינה אתית וגם מקצועית, על חברות שחוו התקפות סייבר ונגנב מהם מידע, עליהן לדווח ללקוחות כי המידע האישי שלהם נגנב וזאת בכדי שהלקוחות יוכלו לגלות ערנות למקרי הונאה ואולי אף להחליף נתונים כמו סיסמאות או אפילו כרטיסי אשראי בכדי להתמודד עם ההשלכות של התקיפה. הדיווח לכשעצמו יכול להוות כלי להפחתת השלכות נזקי הסייבר ולצמצם את הנזקים כלפי לקוחות התאגיד. לעומת זאת אי-הדיווח עלול לתרום להחלשת המלחמה בהתקפת הסייבר שכן לקוחות עשויים להיחשף להונאות, והתאגיד עצמו עשוי להסתיר את המידע ולא להתמודד כראוי עם הבעיה ובכך להנציח אותה. הדיווח של התקפת הסייבר אולי עשוי להוביל לכעס של לקוחות והוצאות כספיות של התאגיד, אך הוא מאפשר ליצור סביבת התגוננות טובה יותר בפעמים הבאות (Morgan, & Gordijn, 2020, p. 123).