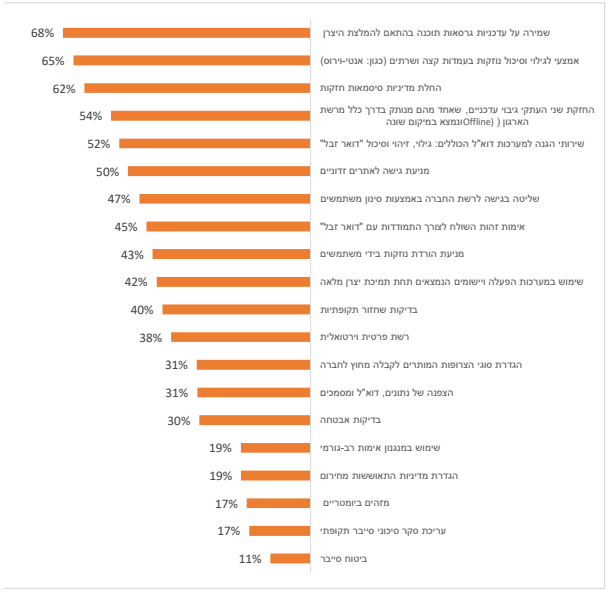

Chart 16 - Percentage of enterprises, by type of security measure implemented

תרשים 16 - אחוז העסקים, לפי סוג אמצעי אבטחה

security measure	Percentage שיעור	סוג אמצעי אבטחה
Cyber insurance	11%	ביטוח סייבר
Conducting a periodic survey on cyber security risks	17%	עריכת סקר סיכוני סייבר תקופתי
Biometric identifiers (e.g. fingerprint, facial or voice recognition)	17%	מזהים ביומטריים
Specifications regarding disaster recovery protocols (e.g. RTO, RPO)	19%	הגדרת מדיניות התאוששות מחירום
Use of Multi Factor Authentication	19%	שימוש במנגנון אימות רב-גורמי
Security checks (e.g. system invasion attempts, warning system checks, security procedure assessments, etc.)	30%	בדיקות אבטחה
Data, files and email encryption	31%	הצפנה של נתונים, דוא"ל ומסמכים
File typing of attachments (e.g. DOC, DOCX, PDF) to be accepted from outside the enterprise ("Whitelist")	31%	הגדרת סוגי הצרופות המותרים לקבלה מחוץ לחברה
The enterprise has a virtual private network (VPN) to transfer data safely through public domains	38%	רשת פרטית וירטואלית
Periodic recovery tests to ensure proper recovery if needed	40%	בדיקות שחזור תקופתיות
Use of operating systems and applications which are under full manufacturer's support (not in "end of life" state)	42%	שימוש במערכות הפעלה ויישומים הנמצאים תחת תמיכת יצרן מלאה
User malware download prevention (e.g. Firewall, SWG – Secure Web Gateway) or cloud-based security software	43%	מניעת הורדת נזקות בידי משתמשים
Authentication of Sender ID (DMARC) for handling spam	45%	אימות זהות השולח לצורך התמודדות עם "דואר זבל"
Control over access to enterprises' network, by user filtering	47%	שליטה בגישה לרשת החברה באמצעות סינון משתמשים
URL filtering by means of firewall, Secure Web Gateway (SWG) or cloud-based security software	50%	מניעת גישה לאתרים זדוניים
Security protection services for the enterprises' email systems, including: detecting and responding to spam and malware (e.g. SEG, Mail Relay)	52%	שירותי הגנה למערכות דוא"ל הכוללים: גילוי, זיהוי וסיכול "דואר זבל"
Having multiple updated backup copies, with one offsite and usually offline	54%	החזקת שני העתקי גיבוי עדכניים, שאחד מהם מנותק בדרך כלל מרשת הארגון (Offline) ונמצא במיקום שונה
Strong password policy (e.g. periodical password reset, minimum password length policy, requiring combination of letters, numbers and characters)	62%	החלת מדיניות סיסמאות חזקות
Means of detecting and responding to malware at endpoints and servers (e.g. antivirus system)	65%	אמצעי לגילוי וסיכול נזקות בעמדות קצה ושרתים (כגון: אנטי-וירוס)
Keeping systems up-to-date per manufacturer's recommendation, or at a more frequent rate	68%	שמירה על עדכניות גרסאות תוכנה בהתאם להמלצת היצרן