“ALEXANDRU IOAN CUZA” UNIVERSITY IAŞI
FACULTATEA DE ECONOMIE ȘI ADMINISTRARE A AFACERILOR (FEAA)
ȘCOALA DOCTORALĂ DE ECONOMIE ȘI ADMINISTRARE A AFACERILOR
DOMENIU FUNDAMENTAL: ȘTIINȚE SOCIALE
DOMENIU ȘTIINȚIFIC: ȘTIINȚE ECONOMICE
DOMENIU DOCTORAL: MARKETING

PROPUNERE DE VALOARE ÎN MOMENTUL SCHIMBĂRII TEHNOLOGIILOR DE SECURITATE CIBERNETICĂ DE LA SOLUȚII ON-PREMISES LA CLOUD: UN STUDIU DE CAZ AL SECURITĂȚII CIBERNETICE ACTIVE DE DEFENSIVĂ

REZUMATUL TEZEI DE DOCTORAT

DOCTORAND: GUY WAIZEL
COORDONATOR DOCTORAL: PROFESSOR ADRIANA ZAIT

2025

CUPRINS

CUVINTE CHEIE

Adoptarea Cloud-ului în Securitatea Cibernetică; Strategii de Migrare la Cloud; Propunerea de Valoare în Securitatea Cibernetică; Tehnologii de Apărare Activă Cibernetică; Tranziția de la On-Premises la Cloud; Strategii de Marketing în Securitatea Cibernetică; Comportamentul Cumpărătorului în Securitatea Cibernetică; Inteligența Artificială în Securitatea Cibernetică și Adoptarea Cloud-ului

INTRODUCERE

Această cercetare dezvoltă un model pentru a explica comportamentul consumatorilor în timpul tranziției tehnologiilor de securitate cibernetică de la soluții on-premises la medii cloud sau hibride, având ca scop informarea unui plan de propunere de valoare pentru departamentele de marketing din companiile de securitate cibernetică. Acest aspect este esențial, având în vedere că furnizorii lansează din ce în ce mai multe produse exclusiv pentru cloud, în timp ce elimină treptat suportul pentru soluțiile on-premises. O abordare strategică de marketing este crucială pentru a păstra clienții în contextul tendinței tot mai accentuate de migrare către cloud.

Temele cheie ale cercetării includ provocările adoptării cloud-ului atât pentru furnizori, cât și pentru clienți, percepțiile clienților asupra software-ului on-premises și cloud, strategii de marketing eficiente pentru a încuraja migrarea și contextul tehnologiei de apărare activă. Literatura existentă privind adoptarea cloud-ului oferă perspective asupra unor domenii tematice variate, dar lipsește de specificități în legătură cu provocările unice cu care se confruntă furnizorii de securitate cibernetică în timpul acestei tranziții.

Studiile actuale relevă lacune semnificative în înțelegerea dificultăților cu care se confruntă organizațiile atunci când adoptă soluții cloud, în special în ceea ce privește securitatea, conformitatea și resursele. De asemenea, există cercetări limitate cu privire la modul în care furnizorii pot facilita această tranziție sau factorii care influențează disponibilitatea clienților de a migra. Această cercetare își propune să abordeze aceste provocări și să ofere metodologii valoroase aplicabile în diverse sectoare, concentrându-se pe marketingul strategic și implicațiile pentru dinamica organizațională, cum ar fi instruirea profesională și securitatea locurilor de muncă. În ansamblu, un plan bine definit de propunere de valoare este necesar pentru a comunica eficient

beneficiile migrării de la soluțiile on-premises la soluțiile cloud, abordând în același timp preocupările atât ale furnizorilor, cât și ale clienților.

Scopul și Obiectivele Cercetării

Scopul principal al acestei cercetări a fost de a dezvolta un model de comportament al consumatorilor care să explice modul în care clienții se comportă atunci când migrează de la software-ul de securitate cibernetică on-premises la soluții cloud sau cloud hibrid. Pe baza acestui model, a fost creat un plan de propunere de valoare pentru a ajuta la convingerea și păstrarea clienților care trebuiau să treacă la cloud, în special atunci când versiunea lor de suport on-premises era eliminată treptat. Cercetarea a fost realizată în trei etape, fiecare cu obiective specifice:
Etapa 1: Analiza calitativă: Scopul acestei etape a fost de a explora modul în care organizațiile care utilizează tehnologia de apărare activă cibernetică percep tranziția de la software-ul on-premises la aplicațiile cloud. Accentul a fost pus pe patru domenii cheie: percepțiile privind funcționalitățile extinse ale cloud-ului, noile integrări ale ecosistemului, economiile de costuri și încrederea în securitatea cloud-ului.
Etapa 2: Analiza cantitativă: Pe baza temelor identificate în Etapa 1, scopul acestei etape a fost de a realiza un sondaj cu un eșantion mai larg pentru a identifica principalele componente care influențează comportamentul clienților. Pe baza acestor constatări, a fost dezvoltat un model care explică comportamentul consumatorilor, urmat de crearea unui plan de propunere de valoare pentru a ajuta departamentele de marketing din domeniul securității cibernetice în migrarea clienților către soluții cloud sau hibride.
Etapa 3: Validarea calitativă: Folosind sesiuni Delphi cu experți, scopul a fost de a valida și de a ajunge la un consens între experți cu privire la modelul de comportament al consumatorilor și planul propus de propunere de valoare. Au fost făcute ajustări pe baza feedback-ului experților pentru a rafina atât modelul, cât și planul.

Problema de cercetare

Problema de cercetare se concentrează pe provocările cu care se confruntă organizațiile în adoptarea tehnologiei cloud, în special în ceea ce privește trecerea de la sistemele tradiționale on-premises. Preocupările legate de securitate și potențialul de pierdere a clienților atunci când

furnizorii elimină treptat suportul pentru produsele vechi complică această tranziție. Prin investigarea acestor provocări, cercetarea subliniază necesitatea unor strategii de marketing eficiente pentru a comunica beneficiile adoptării cloud-ului și a atenua riscurile asociate cu migrarea către medii cloud.

Întrebările de cercetare

Studiul este ghidat de o întrebare principală de cercetare (IPC) referitoare la componentele necesare pentru dezvoltarea unui plan de propunere de valoare pentru furnizorii de software de securitate care migrează clienții către cloud. Patru întrebări secundare de cercetare (ISC) investighează în continuare percepțiile legate de tranziția la aplicațiile cloud, inclusiv influența funcționalităților extinse, integrarea ecosistemelor, economiile de costuri și încrederea în securitatea cloud-ului. Împreună, aceste întrebări au scopul de a oferi o înțelegere cuprinzătoare a factorilor care influențează disponibilitatea clienților de a migra de la soluțiile on-premises la soluțiile cloud.

PARTEA I

BACKGROUND-UL TEORIC AL CERCETĂRII

Capitolul 1 — Termeni Cheie și Definiții

Cloud computing oferă o gamă de servicii precum stocare, rețele și software prin internet, sporind flexibilitatea organizațională și eficiența costurilor (NIST, 2011). Software as a Service (SaaS) permite utilizatorilor să acceseze aplicații precum Microsoft Office 365 pe bază de abonament, în timp ce tehnologia de apărare activă cibernetică folosește tehnici de înșelăciune pentru a îmbunătăți securitatea cibernetică (Zhang & Vrizlynn, 2021). Abordarea cloud-native permite dezvoltarea rapidă a aplicațiilor fără a impune blocajul furnizorului (Al Kiswani & Hasan Ahmed, 2019), iar cloud-urile hibride oferă un amestec de medii publice, private și on-premises pentru a facilita tranzițiile graduale către cloud, respectând în același timp cerințele reglementare (Google, 2023).

Capitolul 2 — Recenzia Literaturii

Acest capitol examinează barierele și factorii care susțin adoptarea cloud-ului, în special în contextul securității cibernetice. Preocupările legate de securitate, inclusiv confidențialitatea datelor și riscurile de breșe, au fost principalele bariere în adoptarea soluțiilor cloud, în special Software as a Service (SaaS) (Shultz, 2016). Alte provocări includ resurse insuficiente, probleme de conformitate cu reglementările și lacune în formare, în special pentru organizațiile mai mici (Ivan & Ille, 2021; Griffith & Stewart, 2020). În ciuda acestor obstacole, atât sectoarele publice, cât și cele private recunosc beneficiile scalabilității și eficienței costurilor ale adoptării cloud-ului (FutureScape, IDC, 2022).

Cadrele reglementare, cum ar fi FedRAMP, NIS2 și DORA, sprijină adoptarea cloud-ului în sectoare precum finanțele și serviciile IT, abordând preocupările legate de securitate și conformitate (Waizel, 2023; DORA, 2023). Inteligența artificială joacă un rol dublu în acest peisaj, îmbunătățind securitatea cloud-ului, dar introducând și noi riscuri, inclusiv atacuri cibernetice bazate pe AI (Wang et al., 2023; Gonaygunta, 2023). Inovații precum învățarea federată arată promisiuni în atenuarea acestor riscuri prin permiterea instruirii colaborative a modelelor AI într-un mod securizat (Hacks, 2024).

În ansamblu, adoptarea cloud-ului în securitatea cibernetică este modelată atât de progresele tehnologice, cât și de cele reglementare, iar AI și noile cerințe de conformitate joacă roluri fundamentale în depășirea barierelor tradiționale.

Capitolul 3 — Cadru Teoretic

Teoriile relevante pentru adoptarea cloud-ului includ teoria costurilor de tranzacție, teoria difuzării inovațiilor și Teoria Unificată a Acceptării și Utilizării Tehnologiei (UTAUT), care abordează factori precum securitatea și încrederea clienților (Sobragi et al., 2014; Liu et al., 2008). Teoriile de marketing, cum ar fi teoria părților interesate, subliniază integrarea intereselor clienților în propunerile de valoare (Freeman, 1984; Fishbein et al., 1975). Integrarea continuă a inteligenței artificiale în securitatea cibernetică prezintă atât oportunități, cât și provocări, necesitând inovație continuă pentru a combate amenințările emergente (Waizel, 2024).

Capitolul 4 — Cadru Conceptual

Acest capitol introduce un cadru de cercetare pentru un plan strategic de marketing destinat dezvoltării unui plan de propunere de valoare pentru furnizorii care încearcă să convingă clienții din domeniul securității cibernetice să treacă de la versiunile de produse on-premises la versiunile cloud. Acesta explorează concepte tehnologice, literatura relevantă și teorii privind deciziile organizaționale, identificând lacune în cunoștințele actuale și strategiile de marketing. Capitolul ilustrează, de asemenea, poziția cercetătorului, scopul cercetării, designul, întrebările de cercetare și ipotezele. Prin utilizarea atât a metodologiilor calitative, cât și cantitative, studiul a dezvoltat un model de comportament al consumatorilor care informează strategii de marketing eficiente pentru a facilita adoptarea cloud-ului. Cadrul conceptual este ilustrat în Figura 4.1.

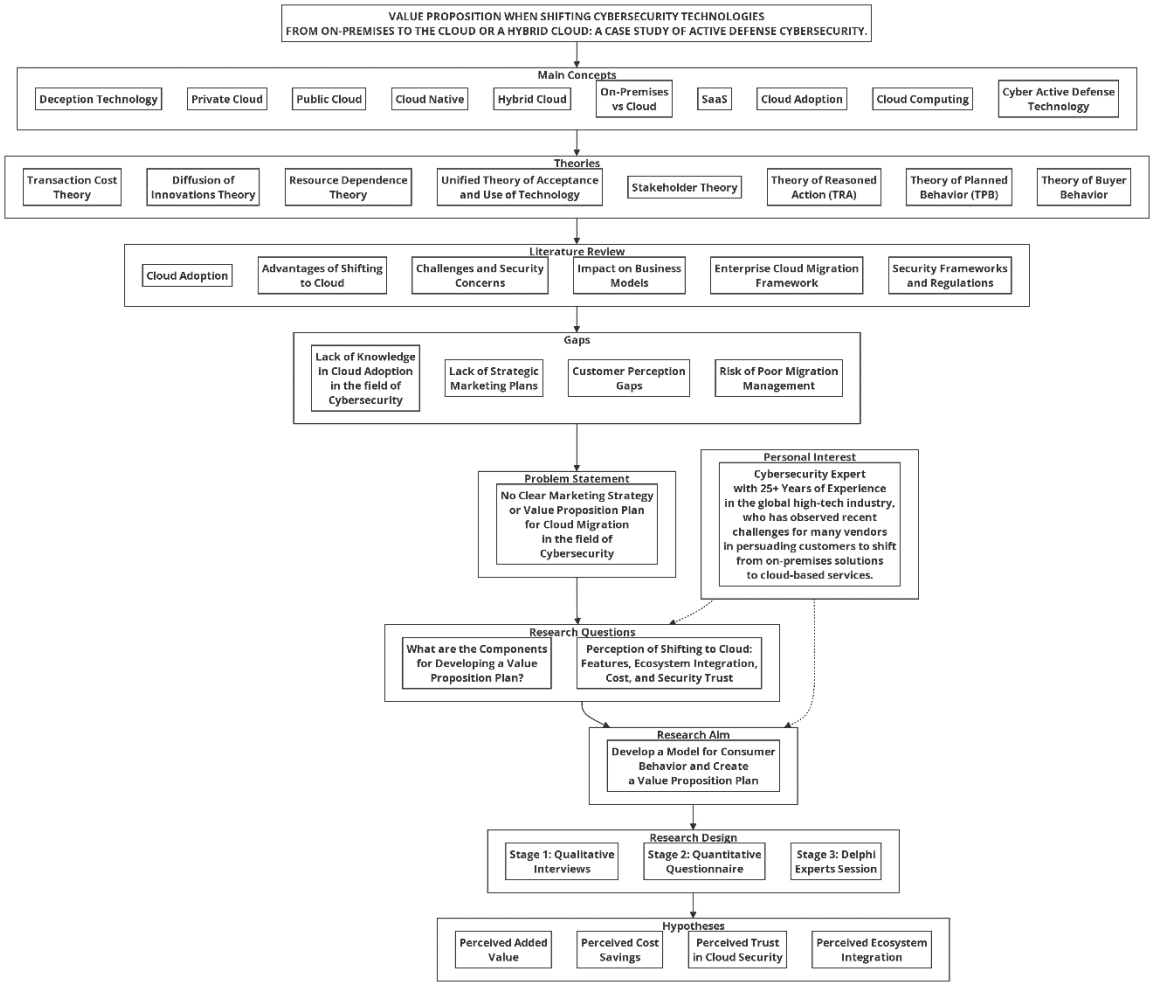

Figura 4.1: Cadru Conceptual pentru Cercetare

PARTEA A II-A

CONTRIBUȚII PERSONALE

Capitolul 5 — Metodologie

Metodologia acestei cercetări este împărțită în trei etape: calitativă, cantitativă și validare calitativă. Cercetarea calitativă a avut ca scop explorarea percepțiilor organizațiilor privind tranziția de la software-ul on-premises la aplicațiile cloud, concentrându-se pe caracteristicile extinse, integrările ecosistemului, economiile de costuri și încrederea în securitatea cloud-ului. Datele au fost colectate prin interviuri semi-structurate cu 13 profesioniști în securitate cibernetică și analizate folosind analiza de conținut. Analiza cantitativă a avut ca scop examinarea percepțiilor unui eșantion mai larg privind factorii identificați în prima etapă, care au fost folosiți pentru a dezvolta un model de comportament al consumatorilor și un plan de propunere de valoare. Un chestionar cu întrebări închise a fost distribuit electronic prin platforma GuidedTrack, iar SPSS a fost folosit pentru analiza datelor. Sondajul a ajuns la 165 de participanți recrutați prin platforma Positly și LinkedIn. În final, au fost desfășurate sesiuni Delphi cu experți pentru a valida și rafina modelul și planul de propunere de valoare. Aceste sesiuni au implicat 8 experți manageri în securitate cibernetică și au folosit analiza de conținut pentru interpretarea datelor.

Capitolul 6 — Prima etapă a cercetării: Analiza calitativă – Interviuri

6.1 Scop și Obiective

Faza inițială a acestei cercetări a implicat interviuri semi-structurate cu profesioniști în securitate cibernetică pentru a explora percepțiile lor privind tranziția la aplicațiile cloud. Această abordare calitativă a abordat întrebări specifice de cercetare legate de percepțiile asupra funcționalității cloud-ului, integrărilor ecosistemului, economiilor de costuri și încrederii în securitatea cloud-ului. Studiul s-a concentrat pe patru obiective cheie: examinarea modului în care organizațiile care utilizează tehnologia de apărare activă cibernetică percep tranziția de la software-ul on-premises la aplicațiile cloud în timp ce valorifică caracteristicile și funcționalitățile extinse; explorarea percepțiilor asupra noilor integrări ale ecosistemului cloud; analiza percepțiilor economiilor de costuri în migrarea de la instalațiile on-premises la aplicațiile cloud; și explorarea percepțiilor asupra încrederii în securitatea cloud-ului în timpul acestei tranziții.

6.2 Întrebările de cercetare

Întrebările secundare de cercetare, aliniate cu obiectivele, sunt următoarele: ISC1 investighează modul în care organizațiile care utilizează apărare activă cibernetică percep tranziția la aplicațiile cloud în timp ce valorifică caracteristicile extinse; ISC2 se concentrează pe percepțiile privind noile integrări ale ecosistemului cloud; ISC3 examinează percepțiile economiilor de costuri asociate cu această tranziție; iar ISC4 se concentrează pe percepțiile privind încrederea în securitatea cloud-ului.

6.3 Pilot și Instrument de Cercetare

Chestionarul a fost dezvoltat pe baza literaturii și a experienței cercetătorului în domeniu. Acesta a fost validat și pilotat cu patru participanți: trei care corespund profilului definit pentru această etapă, axat pe securitate cibernetică, cloud și tehnologie, și unul care a oferit feedback din perspectiva științelor sociale cu privire la structura chestionarului, ordinea întrebărilor, claritatea, aspectele lingvistice și comunicarea. Pe baza acestei validări și teste pilot, chestionarul final a fost rafinat și îmbunătățit, fiind pregătit pentru utilizare în prima etapă a cercetării.

6.4 Metodologie și Recrutarea Participanților

Studiul a utilizat eșantionarea stratificată și intenționată pentru a recruta treisprezece profesioniști israelieni în securitate, toți cu cel puțin doi ani de experiență în securitate cibernetică și autoritate de decizie în ceea ce privește tranzițiile către cloud. Recrutarea a început prin LinkedIn cu scopul de a selecta cincisprezece participanți, dar a fost mutată pe WhatsApp pentru o programare mai eficientă și pentru a obține consimțământul.

6.5 Proceduri de Colectare a Datelor

Participanții au primit o invitație la întâlnire și un formular de consimțământ care detaliază drepturile lor, cu asigurări privind anonimatul datelor. Interviurile au durat între 43 și 47 de minute și au fost înregistrate, însoțite de note detaliate privind limbajul corporal al participanților și nivelul lor de confort.

6.6 Abordarea Analizei Datelor

Analiza de conținut a fost aplicată sistematic, implicând organizarea datelor, definirea unităților de analiză, crearea și rafinarea codurilor, precum și validarea rezultatelor. Acest proces a generat 234 de coduri, 24 de categorii și 23 de teme generale aliniate la întrebările de cercetare.

6.7 Constatări și Temele Cheie

Constatările au evidențiat teme semnificative în percepțiile organizațiilor asupra tranzițiilor către cloud, în special importanța vitezei și flexibilității în îmbunătățirea eficienței operaționale. Factorii de încredere legați de fiabilitatea furnizorului și conformitatea au apărut ca influențe critice asupra procesului decizional.

6.8 Sumar și Implicații

Această primă etapă a cercetării a abordat cu succes întrebările de cercetare și a elucidat relațiile complexe care influențează percepțiile asupra adoptării cloud-ului. Rezultatele sugerează că adoptarea tehnologiilor cloud poate îmbunătăți capacitățile de răspuns, poate genera economii de costuri și necesită un accent strategic pe încredere pentru a facilita o adoptare eficientă a cloud-ului în peisajul tehnologiei de apărare activă cibernetică.

Capitolul 7 — A doua etapă a cercetării: Analiza cantitativă – Sondaj

7.1 Scop și Obiective

A doua fază a cercetării a implicat o analiză cantitativă utilizând un sondaj online destinat părților interesate specifice. Acest chestionar cu întrebări închise, dezvoltat pe baza informațiilor obținute din interviurile calitative, a avut scopul de a cuantifica percepțiile unui eșantion mai larg de 165 de participanți cu privire la factorii și temele deja identificate. Obiectivul a fost dezvoltarea unui model care să explice comportamentul consumatorilor, conducând la un plan de propunere de valoare care să sprijine departamentele de marketing în migrarea clienților către soluții cloud sau cloud hibrid.

7.2 Întrebarea principală de cercetare și ipotezele de cercetare

Întrebarea principală de cercetare pentru această etapă a fost: Ce componente și considerații sunt necesare pentru a dezvolta un plan de propunere de valoare pentru furnizorii de software de securitate care migrează clienții de la soluțiile tradiționale on-premises către cloud sau cloud hibrid? Ipotezele corespunzătoare de cercetare includ: caracteristicile extinse percepute ale valorii cresc dorința de a migra; o integrare mai mare a ecosistemului îmbunătățește dorința de migrare; economiile percepute de costuri facilitează tranziția; și încrederea în securitatea cloud-ului influențează pozitiv adoptarea.

7.3 Dezvoltarea sondajului și testarea pilot

Sondajul a constat din 23 de întrebări de percepție, împărțite pe patru dimensiuni aliniate cu întrebările de cercetare. A fost testat pilot cu cinci participanți pentru validare, urmat de o sesiune pilot cu 30 de participanți (20 din Positly și 10 prin LinkedIn). Scările pentru Economii de Costuri, Funcționalități, Integrare în Ecosistem și Încredere au fost formative, astfel că Alpha lui Cronbach nu a fost esențial (Diamantopoulos & Siguaw, 2006; Stadler et al., 2021). Cu toate acestea, toate valorile au depășit 0.7.

7.4 Recrutarea Participanților și Eșantionarea

Eșantionarea stratificată a fost utilizată pentru a recruta participanți prin platforma Positly și LinkedIn, vizând profesioniști în securitate și IT cu vârsta de 18 ani sau mai mult, cu cel puțin doi ani de experiență, obținând un eșantion necesar de 165 de participanți din Statele Unite și Israel.

7.5 Proceduri de Colectare a Datelor

Sondajul online a fost realizat pe platforma GuidedTrack, asigurând exportul sigur al datelor după completare. Verificările de validare au menținut calitatea datelor prin eliminarea participanților care nu îndeplineau criteriile stabilite.

7.6 Metodologia de Analiză a Datelor

Analiza datelor a fost realizată folosind SPSS versiunea 28. Mai întâi, au fost efectuate statistici descriptive, urmate de testarea celor patru ipoteze. Variabila dependentă, dorința de a migra către cloud (măsurată pe o scală de la 1 la 10), a fost examinată în raport cu patru variabile independente ordinale: caracteristicile extinse percepute, integrarea ecosistemului percepută, economiile de costuri percepute și încrederea percepută în securitatea cloud-ului. Au fost efectuate teste de corelație Spearman separate pentru fiecare ipoteză pentru a evalua corelațiile dintre variabilele independente și variabila dependentă.
Pentru a evalua dacă variabilele de fundal—cum ar fi anii de experiență, dimensiunea organizației, sectorul, vârsta, genul, nivelul de educație și familiaritatea cu tehnologiile IT/securitatea cibernetică—moderează corelațiile, au fost efectuate teste de corelație Spearman între fiecare variabilă de fundal și variabila dependentă.
Au fost realizate analize de regresie multiplă pentru a examina dacă nivelul de educație, familiaritatea cu tehnologiile IT/securitatea cibernetică, vârsta și sectorul clientului moderează

corelațiile dintre variabilele independente (caracteristicile percepute, integrarea ecosistemului percepută, economiile de costuri percepute și încrederea percepută) și variabila dependentă (dorința de a migra către cloud). Fiabilitatea a fost verificată utilizând Alpha lui Cronbach, toate valorile fiind peste 0.7.

7.7 Constatări

Studiul a testat ipotezele că percepțiile mai mari ale caracteristicilor extinse, integrării ecosistemului, economiilor de costuri și încrederii în securitatea cloud-ului vor conduce la o dorință mai mare de a migra către aplicațiile cloud. Toate cele patru ipoteze au fost confirmate, arătând corelații pozitive între aceste percepții și adoptarea cloud-ului.
Studiul a examinat, de asemenea, influența factorilor demografici și organizaționali asupra dorinței de a adopta aplicațiile cloud:
Familiaritatea cu tehnologiile IT și securitatea cibernetică și nivelul de educație au arătat corelații pozitive semnificative; Vârsta și sectorul au prezentat corelații negative, cu vârsta fiind aproape semnificativă din punct de vedere statistic.
Analiza de regresie liniară a arătat că: Nivelul de educație a moderat efectul caracteristicilor și funcționalităților, slăbind impactul acestora; Familiaritatea cu tehnologiile IT și securitatea cibernetică a moderat toate variabilele independente, slăbind influența acestora; Vârsta a moderat efectul majorității variabilelor independente, cu excepția încrederii; Sectorul a moderat efectul caracteristicilor și funcționalităților extinse.
Aceste constatări subliniază rolul semnificativ al factorilor percepuți demografici și organizaționali, cu efecte de moderare din partea educației, familiarității, vârstei și sectorului în modelarea dorinței de adoptare a cloud-ului.

7.8 Dezvoltarea Modelului CLIFFDO

Modelul CLIFFDO dezvoltat încorporează factorii cheie care influențează adoptarea cloud-ului în securitatea cibernetică, concentrându-se pe economiile de costuri, încredere, integrare, caracteristici, familiaritate și factori demografici și organizaționali. Acesta ilustrează interacțiunea dintre aceste componente și impactul lor asupra dorinței clienților de a migra către cloud, așa cum este ilustrat în triunghiul de adoptare a cloud-ului în securitate cibernetică CLIFFDO dezvoltat (Figura 7.8.1) și modelul extins. (Figura 7.8.2)

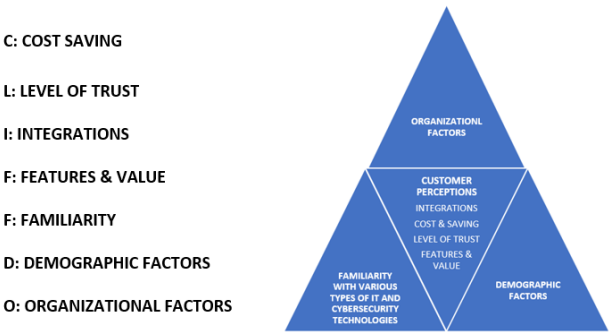

Figura 7.8.1: Modelul Triunghiular de Adoptare a Cloud-ului în Securitatea Cibernetică CLIFFDO

CLIFFDO

Simbolizează un bărbat (cumpărător de securitate cibernetică) stând pe o STÂNCĂ și făcând Adopție Cloud în timp ce vede norii din jur

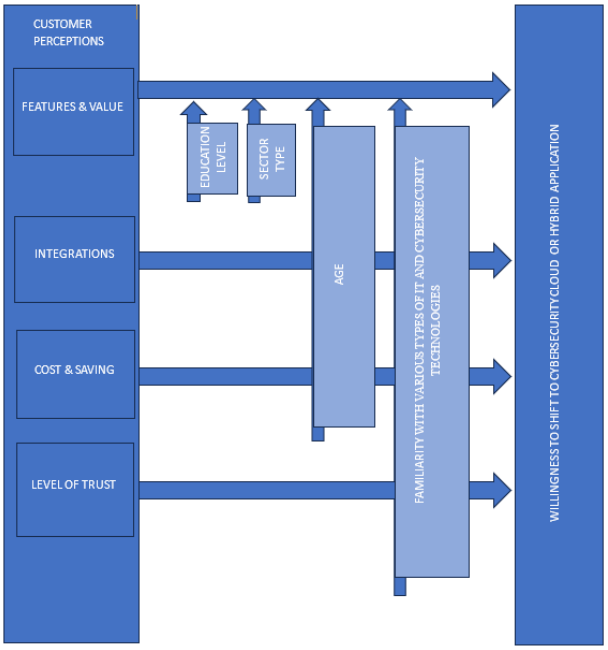

Figura 7.8.2: Modelul extins de adoptare a cloud-ului în securitate cibernetică CLIFFDO dezvoltat

7.9 Recomandări pentru Propunerea de Valoare

Pe baza modelului CLIFFDO, recomandările pentru un plan de propunere de valoare, exemplificate prin propunerea „Shift2CyberCloud Plus," pun accent pe caracteristici îmbunătățite,

integrare fără întreruperi, potențial de economisire a costurilor, securitate de încredere și educație personalizată pentru diferite sectoare, adresând nevoile diverse ale clienților.

7.10 Sumar și Implicații

Constatările iluminează dinamica care afectează dorința clienților de a migra către aplicațiile cloud în securitatea cibernetică. Corelațiile pozitive identificate subliniază necesitatea ca furnizorii să prioritizeze îmbunătățirea caracteristicilor, integrarea ecosistemului, economiile de costuri și strategiile de construire a încrederii. Recunoașterea influențelor demografice permite dezvoltarea unor strategii de marketing direcționate, echipând în cele din urmă organizațiile pentru a promova eficient adoptarea cloud-ului și a optimiza angajamentul clienților în peisajul în continuă schimbare al securității cibernetice.

Capitolul 8 — A treia etapă a cercetării: Analiza calitativă — Sesiuni Delphi cu experți

8.1 Scop și Obiective

Sesiunile Delphi cu experți au fost desfășurate cu un grup de eșantion format din opt experți în securitate cibernetică din diverse industrii. Scopul principal a fost de a valida și de a atinge consensul asupra modelului care explică comportamentul consumatorilor în timpul tranziției de la tehnologiile de securitate cibernetică on-premises la soluții cloud sau cloud hibrid, precum și de a valida și rafina planul de propunere de valoare propus.

8.2 Întrebarea principală de cercetare

Întrebarea principală de cercetare pentru această etapă a fost: Ce componente și considerații pot dezvolta un plan de propunere de valoare pentru furnizorii de software de securitate care migrează clienții de la soluțiile tradiționale on-premises către cloud sau un cloud hibrid?

8.3 Pilot și Instrument de Cercetare

Ghidul inițial al chestionarului, bazat pe modelul CLIFFDO de securitate cibernetică, a fost dezvoltat și pilotat cu trei experți: un expert în securitate, un expert în marketing și un expert în sociologia educației. Pilotul a rafinat chestionarul prin îmbunătățirea clarității, structurii și includerea întrebărilor deschise, asigurând validitatea conținutului și alinierea acestuia cu obiectivele de cercetare. Feedback-ul primit a dus la o versiune revizuită, care a fost finalizată pentru utilizare în prima rundă a sesiunilor Delphi cu experți.

8.4 Designul Cercetării și Metodologia

Această cercetare a implicat sesiuni Delphi cu experți, având ca scop validarea modelului de comportament al consumatorilor și rafinarea planului de propunere de valoare. Un chestionar bazat pe modelul CLIFFDO a fost dezvoltat și testat pilot pentru a asigura claritatea și validitatea acestuia.

8.5 Procesul de Colectare a Datelor

Participanții au fost selectați prin eșantionare stratificată și intenționată prin LinkedIn și recrutați prin WhatsApp, rezultând într-un grup final de opt profesioniști israelieni în securitate și IT, fiecare având peste cinci ani de experiență relevantă și autoritate de decizie. Datele au fost colectate prin interviuri individuale pe Zoom, de aproximativ 45 de minute, cu răspunsurile înregistrate și notițe pe teren. Au fost utilizate cinci runde pentru a atinge consensul, a înțelege limitările și considerațiile și a rafina planul de propunere de valoare în consecință.

8.6 Analiza Datelor și Insight-uri

Analiza de conținut a fost utilizată pentru a analiza datele din sesiunile Delphi, rafinând codurile și categoriile pe baza feedback-ului participanților. Acest proces iterativ a asigurat că temele erau aliniate cu obiectivele de cercetare și au fost validate prin consensul experților.

8.7 Constatări și Temele

Sesiunile Delphi au identificat unsprezece teme cheie pentru modelul CLIFFDO și cinci teme suplimentare pentru planul de propunere de valoare. S-a ajuns la consens cu privire la mai mulți factori critici care influențează adoptarea cloud-ului, inclusiv valoarea percepută a caracteristicilor, încrederea și potențialul de economii de costuri. Insight-urile cheie au inclus rolul încrederii în respectarea cerințelor de conformitate și reglementare, instrumentele de migrare pentru a simplifica tranziția către cloud și potențialul de economii de costuri, care variază în funcție de modelul de implementare și nevoile organizaționale. Feedback-ul suplimentar a subliniat utilizarea formatelor interactive, a resurselor educaționale și a studiilor de caz pentru a demonstra valoarea. Toate considerațiile și feedback-ul au fost incorporate în planul revizuit de propunere de valoare pentru a-i spori eficiența în promovarea adoptării cloud-ului.

8.8 Concluzie și Implicații

Sesiunile au validat cu succes modelul de aplicație cloud în securitate cibernetică CLIFFDO și au oferit insight-uri valoroase pentru rafinarea planului de propunere de valoare. Departamentele de marketing ar trebui să se concentreze pe caracteristici avansate, integrare fără întreruperi și construirea încrederii clienților, în timp ce subliniază și inițiativele educaționale pentru a comunica eficient beneficiile soluțiilor cloud. Această abordare cuprinzătoare sporește atractivitatea ofertelor cloud și atenuează riscurile asociate cu tranziția de la produsele on-premises.

CONCLUZII

Această cercetare a dezvoltat un plan de propunere de valoare pentru furnizorii de securitate cibernetică, concentrându-se pe comportamentul consumatorilor în timpul tranziției de la aplicațiile on-premises la aplicațiile cloud. Pe măsură ce organizațiile migrează din ce în ce mai mult către cloud, furnizorii se confruntă cu provocări în păstrarea clienților, în special atunci când introduc produse exclusiv pentru cloud. Utilizând o abordare mixtă, studiul a început cu interviuri calitative, urmate de un sondaj cantitativ adresat experților IT și în securitate. Constatările au relevat că organizațiile privesc tranziția într-o lumină pozitivă, subliniind importanța funcționalităților extinse, integrărilor personalizate, economiilor de costuri și încrederii în securitatea cloud-ului, ducând la crearea modelului CLIFFDO pentru a explica comportamentul consumatorilor.

Faza finală a implicat sesiuni Delphi cu experți pentru a valida și rafina modelul CLIFFDO și planul de propunere de valoare, sporind fiabilitatea acestora pentru strategiile de marketing. Această cercetare subliniază necesitatea de a aborda preocupările clienților, permițând furnizorilor să își adapteze eficient mesajele de marketing. Implicațiile modelului CLIFFDO se extind dincolo de securitatea cibernetică către industrii precum sănătatea și finanțele, oferind o bază pentru cercetările viitoare axate pe îmbunătățirea strategiilor de marketing și a relațiilor cu clienții în adoptarea tehnologiilor.

Contribuția la Literatură

Implicațiile acestor constatări sunt semnificative și contribuie la literatura existentă, așa cum este prezentat în Tabelul 9.1.

Tabelul 9.1: Întrebările de Cercetare, Conexiunile cu Literatura, Contribuțiile Personale și Concluzii

Întrebarea de Cercetare / Componentă	**Relația cu Literatura Actuală**	**Contribuția la Literatură și Concluzie**
IPC & ISC1 Caracteristici și Funcționalități Extinse Percepute de Valoare	Boillat & Legner (2013), Sobragi et al. (2014), Liu et al. (2008), Ajzen (1985)	CLIFFDO pune accent pe caracteristicile avansate ale cloud-ului (automatisme, AI) pentru a diferenția ofertele, consolidând loialitatea și sprijinind tranzițiile de la soluțiile on-premises (Waizel, 2024).
IPC & ISC2 Integrarea Ecosistemului Percepută	Dimitrakos (2014), Pfeffer & Salancik (2003), Gonaygunta (2023)	CLIFFDO subliniază integrarea fără întreruperi pentru o scalabilitate și eficiență îmbunătățite, oferind avantaje strategice pentru furnizori în abordarea barierelor de integrare.
IPC & ISC3 Economii de Costuri Percepute	Kundra (2011), Sobragi (2012), Rogers (1995), Howard & Sheth (1969), Murphy (2024)	CLIFFDO demonstrează reduceri de costuri în adoptarea cloud-ului, punând accent pe eficiența operațională și economiile de resurse pentru a preveni pierderea clienților.
IPC & ISC4 Nivelul Perceput al Încrederii	Tawfique & Vejseli (2018), UTAUT (Peake, 2018; Slade et al., 2015; Carter & Bélanger, 2005; Venkatesh et al., 2003), Fishbein & Ajzen (1975), Ables (2023); Praveenraj et al. (2023)	CLIFFDO integrează factori de încredere (securitate, transparență, fiabilitatea furnizorului), ajutând furnizorii să cultive încrederea clienților și să faciliteze tranzițiile line către adoptarea cloud-ului (Waizel, 2024; Waizel & Zait, 2024).
IPC Efecte de Moderare		CLIFFDO recunoaște factorii de moderare (familiaritate, vârstă, educație, sector) care influențează adoptarea cloud-ului, permițând furnizorilor să adapteze eficient mesajele de marketing.

LIMITE ȘI DIRECȚII VIITOARE DE CERCETARE

Această cercetare oferă o bază pentru înțelegerea comportamentului consumatorilor în tranziția de la soluțiile de securitate cibernetică on-premises la mediile cloud, dar are limitări care subliniază domeniile ce necesită studii viitoare. Se concentrează în principal pe percepțiile clienților privind adoptarea cloud-ului, fără a captura perspectiva furnizorului asupra strategiilor de migrare. Cercetările viitoare ar putea investiga modul în care furnizorii de securitate cibernetică formulează strategii de marketing și abordează preocupările clienților, oferind o viziune mai cuprinzătoare asupra provocărilor pieței. În plus, aplicarea modelului CLIFFDO în diverse industrii ar putea oferi insight-uri despre diferite abordări ale adoptării cloud-ului.

EXTRACTE DIN 155 DE REFERINȚE

Ables, J. (2023). Explainable intrusion detection systems using white box techniques (Order No. 30812542). Available from ProQuest Dissertations & Theses Global. https://www.proquest.com/dissertations-theses/explainable-intrusion-detection-systems-using/docview/2903798888/se-2

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. User Modeling and User-Adapted Interaction, 29, 701-750. https://doi.org/10.1007/s11257-019-09298-2

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. (Eds.), Action control: From cognition to behavior (pp. 11-39). Springer.

Ajzen, I., & Fishbein, M. (2000). Attitudes and the attitude-behavior relation: Reasoned and automatic processes. European review of social psychology, 11(1), 1-33.

Al Kiswani, J. H. A., & Hasan Ahmed, R. (2019). Smart-Cloud: A Framework for Cloud Native Applications Development. Doctoral dissertation, University of Nevada, Reno.

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organizations. Telematics and Informatics, 35(1), 38-54. https://doi.org/10.1016/j.tele.2017.10.001

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organizations. Telematics and Informatics, 35(1), 38-54. https://doi.org/10.1016/j.tele.2017.10.001

Boillat, T., & Legner, C. (2013). From on-premise software to cloud services: The impact of cloud computing on enterprise software vendors' business models. Journal of Theoretical and Applied Electronic Commerce Research, 8(3), 39-58. https://doi.org/10.4067/S0718-18762013000300005

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. British Journal of Management, 17(4), 263-282. https://doi.org/10.1111/j.1467-8551.2006.00500.x

Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.

FutureScape, IDC. (2022). IDC FutureScape: Worldwide IT industry 2022 predictions.

Gai, K. (2014). A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. International Journal of Computer Applications, 95(3), 40-44. https://doi.org/10.5120/16915-9207

Gonaygunta, H. (2023). Factors influencing the adoption of machine learning algorithms to detect cyber threats in the banking industry. Doctoral dissertation. Available from ProQuest Dissertations & Theses Global.

Gonaygunta, H., & Liu, S. (2023). Integrating AI-driven security measures in cloud environments: Threat detection and mitigation strategies. Journal of Cloud Computing and Cybersecurity, 5(2), 98-114. https://doi.org/10.1007/jccc.2023.0976

Gusman, J. (2024). The deployment of artificial intelligence and machine learning within the field of cybersecurity for intelligent decision-making: A qualitative study. ProQuest Dissertations & Theses Global. Available from Publicly Available Content Database. https://www.proquest.com/dissertations-theses/deployment-artificial-intelligence-machine/docview/2863689117/se-2

Hacks, C. (2024). Federated learning: A paradigm shift in data privacy and model training. Medium. https://medium.com/@cloudhacks_/federated-learning-a-paradigm-shift-in-data-privacy-and-model-training-a41519c5fd7e

Ivan, T. R., & Ille, E. E. (2021). Applying multi-criteria decision-making to the technology investment decision-making process. Acquisition Research Program.

NIST. (2011). Managing information security risk: Organization, mission, and information system view (NIST Special Publication No. 800-39). https://doi.org/10.6028/NIST.SP.800-39

Pearson, S. (2013). Privacy, security, and trust in cloud computing. In Privacy and security for cloud computing (pp. 3-42). Springer.

Pfeffer, J., & Salancik, G. R. (2003). The external control of organizations: A resource dependence perspective. Stanford University Press.

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers in Human Behavior, 62, 61-69. https://doi.org/10.1016/j.chb.2016.04.027

Shultz, A. (2016). Controlling the emerging data dilemma: Building policy for unstructured data access. In Information Security Management Handbook (Vol. 5, pp. 229-242). Auerbach Publications.

Sobragi, C. G., Maçada, A. C. G., & Oliveira, M. (2014). Cloud computing adoption: A multiple case study. BASE: Revista de Administração e Contabilidade da Unisinos, 11(1), 75-91. https://doi.org/10.4013/base.2014.11.1.07

Waizel, G. (2023a). A qualitative analysis of cloud adoption in the public and private sectors from cybersecurity vendors' perspective. Review of Economic and Business Studies, 31, 19-37.

Waizel, G. (2023b). The potential effects of recent EU cybersecurity and resilience regulations on cloud adoption and EU cyber resilience. Centre for European Studies (CES) Working Papers, 15(3).

Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings (Vol. 1, pp. 141-156).

Wang, Y., Yan, Q., Ivanov, N., & Chen, X. (2023). A practical survey on emerging threats from AI-driven voice attacks: How vulnerable are commercial voice control systems? Journal of Cybersecurity and Privacy, 1(2), 123-146. https://doi.org/10.3390/jcp1020008

Zhang, L., & Vrizlynn, L. L. T. (2021). Three decades of deception techniques in active cyber defense: Retrospect and outlook. Cornell University Library, arXiv.org. https://doi.org/10.1016/j.cose.2021.102288

Zhang, X., & Yue, W. T. (2020). Integration of on-premises and cloud-based software: The product bundling perspective. Journal of the Association for Information Systems. https://doi.org/10.17705/1jais.00524