MINISTERUL EDUCAŢIEI
UNIVERSITATEA „VALAHIA” DIN TÂRGOVIŞTE
IOSUD – ŞCOALA DOCTORALĂ DE ŞTIINŢE ECONOMICE ŞI UMANISTE
DOMENIUL FUNDAMENTAL *ŞTIINŢE ECONOMICE*
DOMENIUL *MANAGEMENT*

REZUMATUL TEZEI DE DOCTORAT

„MANAGEMENTUL RISCULUI INFORMAȚIONAL AL PROIECTELOR DE SECURITATE CIBERNETICĂ DIN CADRUL INFRASTRUCTURILOR CRITICE”

CONDUCĂTOR DE DOCTORAT,
Prof. univ. dr. habil. Mihai MIEILĂ

DOCTORAND,
Mihaela Hortensia HOJDA

TÂRGOVIŞTE
2024

CUPRINSUL REZUMATULUI TEZEI DE DOCTORAT

1. CUPRINSUL TEZEI DE DOCTORAT 3
2. CUVINTE CHEIE 6
3. SINTEZA LUCRĂRII 7
4. CURRICULUM VITAE 23
5. LISTA ARTICOLELOR PUBLICATE 26
6. CONTENTS OF THE DOCTORAL THESIS 29
7. KEYWORDS 30
8. SUMMARY 31

1. CUPRINSUL TEZEI DE DOCTORAT

INTRODUCERE

CAPITOLUL 1. STADIUL ACTUAL AL CUNOAȘTERII ÎN DOMENIUL MANAGEMENTULUI PROIECTELOR DE SECURITATE CIBERNETICĂ

1.1. Importanța proiectelor din domeniul securității cibernetice din infrastructurile critice

1.2. Similitudini și diferențieri între managementul organizațiilor axate pe proiecte și cel al organizațiilor care nu sunt axate pe proiecte

1.3. Caracteristicile esențiale ale managementului în organizațiile axate pe proiecte

1.4. Funcțiile de previziune, organizare și coordonare

1.5. Comunicarea în cadrul proiectelor din domeniul securității cibernetice

1.6. Funcțiile de antrenare și de control-evaluare

CAPITOLUL 2. MANAGEMENTUL SECURITATII INFORMATIEI ÎN INFRASTRUCTURILE CRITICE

2.1. Definiții în managementul securității informației

2.2. Tendințe în securitatea informației

2.3. Strategia în domeniul securității informatice

2.4. Sistemul de management al securității informației (SMSI)

2.5. Evoluția amenințărilor la adresa securității cibernetice

2.6. Provocări cheie în securitatea cibernetică a infrastructurilor critice

2.7. Aspecte juridice

2.8. Conformitatea specifică sectorului

2.9. Strategii de conformitate pentru infrastructurile critice

2.10. Integrarea standardelor internaţionale

CAPITOLUL 3. CADRUL CONCEPTUAL EPISTEMOLOGIC, METODOLOGIC ȘI ONTOLOGIC AL DEMERSULUI ȘTIINȚIFIC

3.1. Definiția cercetării

3.2. Procesul de cercetare

3.3. Metodologie

3.4. Cadrul ontologic al demersului științific

3.5. Cadrul metodologic al demersului științific

CAPITOLUL 4. ABORDAREA SECURITĂȚII CIBERNETICE A INFRASTRUCTURILOR CRITICE

4.1. Studiu de caz – Atacul GANDCRAB

4.1.1. Modelarea conceptuală a datelor

4.1.2. Modelarea logică a datelor

4.3 Integrarea abordărilor C4ISR și SIIMA în cadrul proiectelor de securitate cibernetică – element nodal în funcționalitatea infrastructurilor critice

4.4 Asigurarea integrității referențiale a sistemului de securitate cibernetică

4.5 Actualizarea (back-up-ul) bazei de date și variabilele utilizate, pe tipuri de clase

4.6.1.Zona privată a clasei

4.6.2.Zona publică a clasei

4.7. Interfața aplicației și acțiunile utilizatorilor

CAPITOLUL 5. GHID DE BUNE PRACTICI PENTRU ÎMBUNĂTĂȚIREA EFICACITATII ÎN GESTIONAREA RISCURILOR INFORMAȚIONALE PENTRU PROIECTELE DE SECURITATE cibernetică ÎN CADRUL INFRASTRUCTURILOR CRITICE

5.1 Evaluarea și analiza riscurilor. Fundamentele securității în infrastructurile critice. Stabilirea unui cadru cuprinzător de gestionare a riscurilor

5.2. Tehnici de modelare a amenințărilor. Obiective. Tehnici practice

5.3. Rolul conducerii și dezvoltarea unei culturi cibernetice

5.4. Colaborare parteneriate publice-private și partajarea informațiilor în securitatea cibernetică

5.5. Răspunsul la incidente: tehnologii avansate și supraveghere permanentă. Elaborarea unui plan de răspuns la incidente și protocoale de comunicare

5.6. Tehnologii și infrastructură. Măsuri de securitate pentru puncte terminale

5.7. Tehnologii emergente în domeniul securității cibernetice, Blockchain pentru securitate

5.8 Evaluarea continuă

5.9. Gestionarea riscurilor furnizorilor, bugetarea și auditurile de securitate ale terților în securitate cibernetică

5.10. Rentabilitatea investițiilor în securitatea cibernetică

5.11. Lecții învățate din incidentele de securitate cibernetică

5.12. Recomandări

CONCLUZII CONTRIBUȚII PROPRII ȘI DIRECȚII VIITOARE DE CERCETARE

Concluzii ale cercetării științifice

Contribuții proprii privind demersul științific

Direcții viitoare de cercetare științifică

ABSTRACT OF THE DOCTORAL THESIS

BIBLIOGRAFIE

ANEXE

2. CUVINTE CHEIE

Teza de doctorat ***„Managementul riscului informațional al proiectelor de securitate cibernetică din cadrul infrastructurilor critice*”** își propune atingerea obiectivelor și validarea ipotezelor fiind utilizate următoarele cuvinte-cheie:

Securitate cibernetică

Infrastructură critică

Atacuri cibernetice

GANDCRAB

Cele mai bune practici

Management de proiect

Metodologii IT

Managementul riscului

Indicatori de performanță

3. SINTEZA LUCRĂRII

Importanța, actualitatea și noutatea temei

Importanța tematicii

Importanţa administrării infrastructurii critice şi protejarea proiectelor de securitate cibernetică este una din cele mai complexe sarcini, în prezentul context al provocărilor şi al riscurilor globale. Construirea rezilienţei şi a bunei adaptabilităţi este un exemplu de leadership şi de creare de bune practice, ghiduri de acţiune şi menţinerea unui climat de lucru de continuitate în funcţionare normală a societăţii *(eng. going concern)*.

Multe infrastructuri critice încă funcționează pe sisteme preluate, care s-ar putea să nu dispună de caracteristicile robuste de securitate ale tehnologiilor moderne. Aceste sisteme, care astăzi sunt perimate, au fost adesea proiectate fără a lua în considerare amenințările contemporane la adresa securității cibernetice, făcându-le susceptibile de exploatare. Echilibrarea necesității de modernizare a sistemului cu cerințele operaționale ale serviciilor critice reprezintă o provocare semnificativă. Îmbunătățirea sistemelor preluate nu este o sarcină simplă, deoarece necesită o planificare atentă, investiții financiare substanțiale și poate necesita întreruperi temporare ale serviciilor esențiale.

Infrastructurile critice se bazează adesea pe sisteme interconectate, creând o rețea complexă de dependențe. Gestionarea riscurilor de securitate cibernetică devine o provocare din cauza interacțiunii dintre diferite componente și a potențialelor efecte în cascadă ale unei încălcări a securității.

Evoluția rapidă a amenințărilor cibernetice prezintă provocări semnificative pentru integritatea și reziliența infrastructurilor critice, cuprinzând sectoare precum energia, transportul, asistența medicală și finanțele.

Într-o lume din ce în ce mai interconectată și complexă, infrastructurile critice joacă un rol esențial în asigurarea funcționării normale a societății. Aceste infrastructuri care includ sectoare vitale precum energia, transporturile, telecomunicațiile și sănătatea sunt fundamentale pentru stabilitatea economică, securitatea națională și bunăstarea publică. Totuși, creșterea vulnerabilităților și riscurilor asociate cu aceste infrastructuri a devenit evidentă, ceea ce impune o analiză aprofundată și o abordare strategică pentru a le proteja. Această lucrare își propune să

exploreze importanța infrastructurilor critice, să identifice principalele provocări cu care se confruntă și să ofere soluții pentru îmbunătățirea securității acestora.

Prin urmare este important să înţelegem funcţionarea infrastructurii critice în buna activitate a societăţii moderne, dar şi pentru modul de operare al securităţii naţionale şi de a adresa într-un mod anticipativ atacurile şi a preveni riscruile prin mecanismele de îmbunătățire continuă şi proceduri solide capabile să facă faţă, în special, situaţiilor neprevăzute.

Rezultatele negative ale politicilor publice care vizează slăbirea capacităților de criptare în anumite ţări și susținerea cenzurii impuse de anumite state vor persista din cauza eforturilor organizațiilor neguvernamentale și ale militanților pentru protejarea vieții private. Există deja o „asistență voluntară" din partea industriei în legătură cu noi tehnologii și servicii aflate în dezvoltare. Pe acest fond, cererea utilizatorilor și grupărilor criminale pentru instrumente de criptare a comunicațiilor și de protejare a activității online va crește.

Actualitatea subiectului

Actualitatea temei este una recurentă dat fiind activitatea organizațiilor a căror operare se regăsește în domeniul infrastructurilor critice trebuie să fie în concordanță cu dinamica globală și regională, care poate avea un impact asupra peisajului de risc. De exemplu, schimbările în relațiile internaționale sau apariția unor noi amenințări cibernetice ar putea prezenta riscuri semnificative la adresa securității informațiilor. Respectarea reglementărilor și a standardelor care evoluează intră, de asemenea, în domeniul de aplicare. Managementul organizațiilor trebuie să își adapteze practicile de gestionare a riscurilor pentru a face față reglementărilor legale în schimbare.

Se estimează că numărul amenințărilor informatice a fost de aproximativ un miliard în 2020, nivel care se va majora în anii ce urmează. Firmele de securitate informatică anticipează că atacurile vor deveni din ce în ce mai sofisticate, având consecințe devastatoare pentru activitățile oamenilor și pentru companii. Cunoașterea trendului actual al manifestărilor amenințărilor informatice permite organizarea măsurilor tehnice și organizatorice care trebuie adoptate de către organizații pentru protejarea informațiilor.

Numărul de peste 20 de miliarde de dispozitive inteligente conectate reprezintă un stimulent semnificativ pentru atacatori să identifice noi gadgeturi vulnerabile. În absența standardelor minime impuse producătorilor - în special în ceea ce privește actualizările de securitate, politica de colectare și procesare a datelor, și remedierea problemelor apărute pe

parcursul utilizării - hackerii și crackerii vor continuă să exploateze vulnerabilitățile, fie ele noi sau deja identificate, pentru a dezvolta rețele tot mai mari de dispozitive inteligente. Aceste rețele vor putea fi utilizate pentru a ataca infrastructuri, în special infrastructuri industriale critice.

În SUA costul mediu per incident cibernetic al infrastructurii critice sau în afara ei este de aproximativ 10 milioane de dolari şi se estimează că pentru 2025 costurile vor cumula 10 milioarde de dolari, conform unui studiu realizat de Universitatea Tusla din Oklahoma.

Dezvoltarea tehnologiilor deepfake în scopuri de criminalitate informatica va genera o noua oportunitate de atac pentru infractori. Apelurile telefonice bazate pe voci ale unor persoane reale sunt folosite în înselatorii menite să păcăleasca angajaţi din companii să transfere bani către conturile atacatorilor, aşa cum s-a întâmplat deja. Din păcate cel mai mult vor fi afectaţi bunii platnici.

Infrastructurile critice reprezintă ținte atractive pentru actori răuvoitori, inclusiv teroriști și state ostile, care ar putea încerca să le compromită pentru a crea haos și instabilitate. Protejarea acestor infrastructuri este, așadar, esențială pentru menținerea securității și stabilității unei națiuni.

Noutatea abordării

Recenzia literaturii de specialitate dovedeşte că până în prezent abordarea infrastructurii critice şi a riscurilor aferente prezintă o persepctivă tehnică majoră. Prezenta lucrare contribuie la un nou mod de înţelegere al managementului riscului informaţional al proiectelor de securitate cibernetică din cadrul infrastrcturilor critice.

Noutatea constă în perspectiva protejării infrastrcturii critice, pe care în prezenta teză nu o considerăm doar o chestiune tehnică, ci și o responsabilitate strategică și etică. Garantarea continuității și securității acestor infrastructuri esențiale necesită angajamentul și cooperarea tuturor actorilor implicați - de la guverne și sectorul privat la comunități și cetățeni. Investițiile în tehnologie, educație și politici publice sunt cruciale pentru a construi o societate mai sigură și rezilientă.

Într-o eră de evoluție rapidă a amenințărilor și de creștere a complexității interdependențelor, abordarea protecției infrastructurilor critice reprezintă o provocare continuă ce trebuie gestionată cu seriozitate și inovație. Doar printr-o abordare proactivă și coordonată putem asigura protecția acestor resurse vitale, garantând astfel securitatea și prosperitatea societăţii infromaţionale şi a societăţii in general.

Gestionarea securității cibernetice nu este doar o chestiune tehnică, ci o prioritate strategică pentru protejarea serviciilor esențiale. Investițiile în securitate, colaborarea între sectoare și educarea publicului sunt esențiale pentru construirea unei societăți mai sigure și mai reziliente. Fără o abordare integrată și cuprinzătoare a securității cibernetice, riscurile la adresa infrastructurilor critice vor continuă să crească, amenințând nu doar funcționarea eficientă a serviciilor esențiale, ci și bunăstarea generală a cetățenilor.

Astfel, prioritizarea securității cibernetice devine nu doar o responsabilitate a conducerii organizațiilor care operează aceste servicii, ci și o necesitate colectivă în fața provocărilor globale. Prin colaborare, educație și inovație, putem asigura că serviciile esențiale rămân disponibile și sigure, contribuind la un viitor mai stabil și mai prosper pentru toți. Este crucial să înțelegem că, în era digitală, securitatea cibernetică nu este opțională, ci o imperativă a societății contemporane.

Perspectiva abordării este una de îmbunătățirea continuă prin studii de caz şi și exemplele din lumea reală discutate evidențiază natura dinamică și evolutivă a provocărilor de securitate cibernetică, subliniind necesitatea îmbunătățirii și adaptării continue. Studiile de caz, povești de succes și cele mai recente evoluții în materie de securitate cibernetică reprezintă pârghii consistente prin care organizațiile își pot perfecționa continuu strategiile. Rămânând informate cu privire la amenințările emergente, colaborând cu comunitatea de securitate cibernetică și adoptând o poziție proactivă, persoanele care activează în organizații pot naviga în mod eficace în arealul complex al riscurilor informaționale din infrastructurile critice.

Într-un context de securitate cibernetică în permanentă schimbare, angajamentul față de îmbunătățirea continuă și strategiile adaptive vor fi esențiale pentru a asigura reziliența infrastructurilor critice împotriva amenințărilor informatice care evoluează.

În organizații trebuie să se acorde prioritate strategiilor proactive de gestionare a riscurilor, cum ar fi confidențialitatea începând cu momentul conceperii, divulgarea responsabilă a vulnerabilităților și o abordare bazată pe riscuri a alocării resurselor, pentru a-și spori reziliența generală în materie de securitate cibernetică.

Recomandările pentru îmbunătățiri viitoare în gestionarea riscurilor informaționale includ încurajarea colaborării inter-funcționale, în special între departamentele IT, de securitate, juridice și alte departamente relevante. Eforturile de colaborare asigură o abordare holistică a alocării resurselor și a atenuării riscurilor.

Astfel, unul din elementele cheie pe care se fundamentează această lucrare de doctorat este rolul leadershiului în prevenirea problemelor și implementarea de standarde ISO pentru suplimentarea legislației, pentru o abordare mai solidă.

Provocări, amenințări, oportunități și soluții

Înțelegerea naturii dinamice a amenințărilor cibernetice este esențială pentru anticiparea și atenuarea riscurilor potentiale la adresa infrastructurilor critice. În contextul infrastructurilor critice, domeniul de aplicare include securitatea sistemelor IT și considerente legate de elementul uman, precum instruirea angajaților, sensibilizarea și aderarea la politicile de securitate.

Percepția și tratarea vulnerabilităților în procesele de afaceri constituie componente integrante ale gestionării riscurilor informaționale, deoarece aceste procese implică adesea gestionarea informațiilor sensibile care pot fi susceptibile la riscuri care decurg din surse interne sau externe.

Factorii externi care contribuie la domeniul de aplicare al gestionării riscurilor informaționale includ evenimentele geopolitice, condițiile economice și modificările la nivel de reglementare.

Implementarea unei abordări bazate pe riscuri a conformității nu este un efort unic, ci un proces continuu care evoluează odată cu natura dinamică a amenințărilor cibernetice. Reevaluarea periodică a riscurilor și a strategiilor de conformitate este esențială pentru a se asigura reziliența organizațiilor la amenințările emergente și la modificările cadrului normativ.

Mecanismele de îmbunătățire continuă, cum ar fi revizuirile periodice și actualizările evaluărilor riscurilor, permit organizațiilor să își adapteze strategiile de conformitate la peisajul amenințărilor care evoluează, menținând astfel o apărare proactivă și eficace împotriva potențialelor amenințări cibernetice. Conformitatea este un proces continuu care necesită o monitorizare constantă pentru a evidenția beneficiile implementării unor sisteme robuste de monitorizare, care facilitează asigurarea conformității, cu scopul de a detecta abaterile cu promptitudine și de a înlesni acțiunile corective în timp util.

Monitorizarea continuă este o piatră de temelie a strategiilor eficiente de conformitate pentru infrastructurile critice. Implementarea unor sisteme robuste de monitorizare le permite organizațiilor să mențină vizibilitatea în timp real asupra situațiilor de securitate cibernetică, asigurându-se că respectă în mod consecvent cerințele de reglementare.

Pentru ca standardele internaționale să fie eficace în contextul infrastructurilor critice, membrii organizațiilor trebuie să le adapteze aplicarea la specificul fiecărui sector. Deși standardele internaționale sunt fundamentale, adaptarea este crucială pentru a face față cerințelor și provocărilor unice ale diverselor sectoare de infrastructură critică.

Există diferite metodologii de modelare a amenințărilor, fiecare adaptată la diferite nevoi și scenarii organizaționale. Metodologiile comune includ STRIDE (Spoofing, Modificare, Repudiere, Dezvaluirea informatiilor, Refuzul serviciului, Ridicarea privilegiului) și DREAD (Daune, Reproductibilitate, Exploatare, Utilizatori afectati, Descoperire). Aceste metodologii oferă cadre structurate pentru identificarea și evaluarea amenințărilor pe baza diferiților parametri, ajutând organizațiile în evaluarea sistematică a riscurilor potențiale.

Un alt aspect important este educaţia. Într-un articol pe blogul Google din 2021, Kent Walker, președinte al Afacerilor Globale și Director Juridic al Google & Alphabet, a susținut că există un angajament de 10 miliarde USD în următorii cinci ani pentru a consolida securitatea cibernetică, inclusiv prin extinderea programelor, asigurarea aprovizionării cu software și îmbunătățirea securității open-source pe întregul lanț. Pe lângă această măsură, Google a lansat și un program de educare a utilizatorilor cu privire la analiza datelor, pe care peste 100.000 de americani l-au finalizat cu succes. Acest instrument educațional al Google se poate dovedi util, în cazul în care oamenii sunt efectiv interesați să îl acceseze, în special pentru citirea lucrărilor de cercetare publicate de Google despre securitatea computerelor, abuzuri etc., compania înființând și un grup de analiză a amenințărilor. Recomandările pentru îmbunătățiri viitoare includ:

Instruirea periodică și dezvoltarea abilităților: Investiți în programe periodice de formare și dezvoltare a competențelor pentru profesioniștii din domeniul securității cibernetice, pentru a vă asigura că aceștia sunt la curent cu cele mai recente amenințări și tehnologii.

- ✓ Integrarea AI și a automatizării: Explorarea integrării inteligenței artificiale (AI) și a automatizării pentru a îmbunătăți detectarea amenințărilor, timpii de răspuns și eficacitatea generală a securității cibernetice.
- ✓ Cercetare și dezvoltare colaborativă: Implicarea în inițiative de cercetare și dezvoltare în colaborare cu colegii din industrie, instituțiile de cercetare și agențiile guvernamentale pentru a rămâne în fruntea inovației în domeniul securității cibernetice.
- ✓ Participarea la inițiative de schimb de informații, exerciții comune și forumuri de colaborare pentru a aborda provocările colective de securitate cibernetică.

Utilizatorul reprezintă primul strat de apărare împotriva amenințărilor cibernetice, fiind adesea primul care identifică pericolele și, atunci când este necesar, semnalează aceste probleme către responsabilul IT al organizației. Capacitatea utilizatorului de a preveni daune semnificative, atât pentru sine cât și pentru organizație, este esențială.

Astfel, pentru a îmbunătăți securitatea cibernetică a unei organizații, sunt importante următoarele aspecte:

- Elaborarea unei viziuni și a unor principii care să stea la baza unei politici de securitate a informațiilor;
- Implementarea acestei politici în întreaga organizație și stabilirea clară a rolurilor și responsabilităților;
- Cultivarea unei culturi organizaționale și a unei atitudini adecvate, prin aplicarea consecventă a principiilor de securitate a informațiilor.

Evaluarea riscurilor poate fi realizată fie prin metode cantitative, fie calitative. Instrumentele cantitative includ analiza Monte Carlo, simulările, tehnica PERT (Project Evaluation and Review Technique), analiza modurilor de defectare și efectelor (FMEA) și evaluările probabilistice de siguranță (PSA). Totuși, în practică, proiectele dispun adesea de date insuficiente pentru efectuarea unei analize cantitative detaliate a riscurilor.

PROBLEMATICĂ ȘI IPOTEZE

Obiectivul general

Obiectivul general al tezei este influenţat de gândinrea lui Francis Bacon care avansat ideea că cunoașterea autentică trebuie să fie fundamentată pe observațiile empirice ale lumii reale. Pe baza acestei premise, Bacon a accentuat că dobândirea cunoștințelor trebuie să fie o activitate empirică.

La nivel pragmatic, lucrarea urmărește să ajute nu doar la identificarea variantelor de soluții de securitate cibernetică aferente riscului informațional din infrastructurile critice, ci și la alegerea soluției celei mai adecvate de către management, folosind metode de selecție inovative.

Obiectivele generale ale tezei, sunt de a deschide o nouă adordare şi spaţiu de cercetare prin analizearea elementelor non-tehnice şi non birocratice din cadrul infrastrcturii critice prin

introducerea managementelui, eticii şi strategiei ca piloni de bază în analiza şi răspunsul la situaţii ce privesc gestiuea de riscuri informaţionale în infrastrcutrua critică.

Lucrearea încearcă să capteze transformările rapide din mediul economic și tehnologic şi cum acestea exercită o presiune considerabilă asupra structurilor organizaționale tradiționale, adesea birocratice şi rezistente la schimbările din mediul extern.

Studiul managementului proiectelor devine crucial pentru organizațiile moderne, fie ele corporații sau instituții publice, deoarece sunt implicate în implementarea inovațiilor, cum ar fi dezvoltarea de produse și servicii noi, realizarea de construcții și aplicarea unor procese noi. Cercetarea managementului ca știință a relevat apariția unor noi tendințe globale în ultimele decenii.

Obiectivul activităților științifice întreprinse pe parcursul perioadei de documentare, precum și în etapa de conceptualizare și redactare a lucrării, a constat în identificarea și elaborarea unei noi perspective asupra asigurării securității naționale. Această abordare vizează crearea unor conexiuni și relații logice, interdependente, între concepte precum organizația, managementul informației, arealul cibernetic, supranaționalismul/realismul, diplomația, cultura de securitate cibernetică și securitatea națională.

Obiectivele specifice

Obiectivele specice ale tezei deriva din obiectivele generale şi acestea sunt:

- Înțelegerea motivelor pentru care o anumită tehnologie a fost implementată cu succes într-o organizație, dar a eșuat în alta, poate varia semnificativ în funcție de perspectiva teoretică adoptată.
- Elaborarea acestor bune practici se îndeamnă membrii organizațiilor să adopte o mentalitate proactivă și să dezvolte soluții inovatoare care să asigure că infrastructurile critice rămân funcționale și reziliente în fața unei game tot mai mari de amenințări cibernetice.
- Armonziarea stadardelor tehnice şi implementarea lor paralel cu legislaţia statelor pentru gestionarea riscurilor informaționale.

- Analiza evoluției gestionării riscurilor în infrastructura critică, precum și modul în care birocrația se adaptează pentru a spori reziliența și a se alinia la cele mai bune practici internaționale.

Întrebările de cercetare şi ipotezele de lucru

- Cum se decid bunele practici și cum se adaptează cunoștințele în cadrul managementului de securitate?
- În ce măsură managementul de securitate este afectat de cunoștințele tehnice și dacă lipsa acestora poate fi suplinită printr-un management de excelență?
- Cât de repede se adaptează managementul la schimbare și ce determină schimbarea la nivel de bune practici?
- Care sunt tendințele cheie moderne în managementul riscului informațional al proiectelor de securitate cibernetică în cadrul infrastructurilor critice și cum se aliniază ele cu modelele internaționale de bune practici?
- Cum diferă diferitele infrastructuri critice în abordarea lor față de managementul riscului informațional în proiectele de securitate cibernetică și care sunt implicațiile pentru modelele internaționale de bune practici?
- Care sunt principalele provocări și obstacole cu care se confruntă organizațiile în implementarea modelelor internaționale de bune practici pentru managementul riscului informațional în proiectele de securitate cibernetică din cadrul infrastructurilor critice?
- Cum influențează tehnologiile emergente practicile de gestionare a riscurilor informaționale în proiectele de securitate cibernetică din cadrul infrastructurilor critice și ce adaptări sunt necesare în modelele internaționale de bune practici?
- Care sunt potențialele strategii și recomandări pentru îmbunătățirea eficacității managementului riscului informațional în proiectele de securitate cibernetică din cadrul infrastructurilor critice, bazate pe o analiză cuprinzătoare a tendințelor moderne și a modelelor internaționale de bune practici?

Există dovezi consistente care susțin ipoteza că adoptarea abordărilor proactive de informații despre amenințări și de vânătoare a amenințărilor este mai eficace în atenuarea riscurilor cibernetice în infrastructurile critice, comparativ cu strategiile reactive tradiționale. Această

eficiență sporită se datorează capacității de a preveni, detecta și răspunde rapid în fața amenințărilor emergente.

Numeroase studii de caz și cercetări demonstrează că implementarea standardului ISO/IEC 27001 conduce la o îmbunătățire semnificativă a securității informațiilor, prin reducerea incidentelor și creșterea eficienței în răspunsul la evenimentele de securitate. Certificarea ISO/IEC 27001 oferă credibilitate organizațiilor, asigurând clienții și partenerii de existența unor măsuri adecvate de protecție a informațiilor. Totodată, adoptarea acestui standard impune o analiză sistematică a riscurilor și dezvoltarea de politici și proceduri de răspuns.

În ceea ce privește tehnologiile emergente, cum ar fi AI și machine learning, acestea au început să aducă îmbunătățiri în managementul riscurilor cibernetice. Aceste tehnologii permit identificarea rapidă a modelelor și anomaliilor și automatizează răspunsurile, însă provocările de implementare, inclusiv costurile ridicate și necesitatea unui personal specializat, limitează integrarea pe scară largă. Evaluarea impactului acestor tehnologii este încă în curs de desfășurare, iar preocupările etice și legate de încredere în deciziile automatizate persistă.

Importanța culturii organizaționale este subliniată ca fiind crucială în succesul inițiativelor de management al riscurilor. O cultură care promovează conștientizarea securității și care încurajează comportamente proactive contribuie la eficiența implementării măsurilor de securitate. Leadershipul joacă un rol esențial în formarea și menținerea acestei culturi, iar investițiile în formarea angajaților se traduc în rezultate mai eficiente.

De asemenea, este analizat impactul factorilor geopolitici și rolul reglementărilor guvernamentale, evidențiind cum influențele externe pot dicta strategiile de management al riscurilor. Colaborarea între organizații și agențiile guvernamentale este esențială pentru prevenirea atacurilor, facilitând partajarea rapidă a informațiilor despre amenințări. În concluzie, abordările proactive, cum sunt threat intelligence și threat hunting, se dovedesc a fi mai eficiente în gestionarea riscurilor cibernetice comparativ cu metodele reactive, având capacitatea de a preveni și a răspunde rapid la amenințările emergente.

STRUCTURA TEZEI DE DOCTORAT

Structura tezei

Structura lucrării este concepută pentru a prezenta la nivel gradual, dar și în paralel, evoluțiile sistemelor de management și cel al securității cibernetice, după cum urmează:

Capitolul 1 subliniază nevoia de adaptabilitate și inovație continuă în abordările de management ale proiectelor, în special în domeniile puternic influențate de tehnologie, cum ar fi securitatea cibernetică, dar şi nevoie de comunicare la nivel înalt. Evoluțiile rapide și complexitatea mediilor de proiecte necesită o abordare metodică pentru planificare, execuție și control, care să includă o combinație între expertiză tehnică și abilități interpersonale puternice, esențiale pentru gestionarea eficace a echipelor într-o lume interconectată şi dinamică.

Capitolul 2 subliniază tendințele actuale din domeniul securității informației, evidențiind faptul că numărul amenințărilor cibernetice crește continuu, iar atacurile devin tot mai sofisticate. Utilizarea algoritmilor de inteligență artificială și tehnicilor de inginerie socială reprezintă provocări semnificative pentru securitatea informației, aspect care impune adoptarea de măsuri tehnice și organizatorice inovatoare.

O componentă esențială a acestui capitol este utilizarea standardelor ISO/IEC 27, care oferă un cadru de referință pentru dezvoltarea și implementarea sistemelor de management al securității informației (SMSI). Adoptarea acestor standarde permite organizațiilor să protejeze eficient informațiile financiare, proprietățile intelectuale și datele personale, asigurând astfel continuitatea și succesul operațional.

Capitolul 3 demonstrează importanța unei metodologii de cercetare bine fundate pentru a oferi o contribuție semnificativa la domeniul securității cibernetice. Integrarea metodei calitative și a realismului critic s-a dovedit adecvată pentru documentarea și înțelegerea fenomenelor complexe și dinamice specific acestui domeniu, asigurând în același timp o aliniere teoretică și practică ce va ghida cercetările viitoare.

Utilizarea chestionarelor structurate, alături de analiza datelor primare și secundare, a oferit rezultate complexe care au demonstrat rigoarea științifică și relevanța practică a cercetării. Studiul de caz GandCrab a servit ca punct focal pentru aplicarea teoriei în practică. El reliefează importanța unei abordări integrate și multidimensionale în înțelegerea și gestionarea riscurilor de securitate cibernetică.

Capitolul 4 analizează impactul ransomware-ului GandCrab asupra infrastructurilor critice, evidențiind metodele sale de operare și implicațiile cibernetice. GandCrab, un ransomware extrem de sofisticat, a fost activ din 2018 și a folosit tehnici avansate de criptare pentru a bloca accesul la datele utilizatorilor, solicitând răscumpărări în Bitcoin.

Studiul de caz prezentat se concentrează pe un atac specific asupra unei firme de contabilitate din Statele Unite, unde un angajat a deschis un e-mail infectat, ce a dus la criptarea rapidă a fișierelor esențiale.

Compania, cu măsuri de securitate minimale, a fost nevoită să plătească o răscumpărare semnificativă pentru a recupera datele, ceea ce a afectat atât operațiunile interne, cât și reputația sa exterioară. Lecțiile învățate subliniază importanța măsurilor proactive de securitate cibernetică, inclusiv educația angajaților și backup-uri regulate.

Capitolul abordează, de asemenea, modul în care comunitatea de securitate cibernetică s-a adaptat la amenințările emergente, promovând măsuri precum gestionarea corectă a corecturilor software, autentificarea multifactor și formarea în domeniul securității cibernetice.

Secțiunea referitoare la integrarea abordărilor C4ISR și SIIMA subliniază importanța unui sistem informatic integrat pentru gestionarea fluxurilor informaționale și a securității în organizațiile critice. Aceasta abordează conceptele fundamentale ale securității cibernetice – confidențialitate, integritate, disponibilitate, autentificare și control al accesului – și modul în care acestea trebuie implementate pentru a proteja datele esențiale.

Capitolul 5 abordează gestionarea riscurilor informaționale în cadrul infrastructurilor critice, evidențiind importanța unei abordări sistematice de identificare, evaluare și prioritizare a riscurilor. Stabilirea unui cadru cuprinzător de gestionare a riscurilor, conform îndrumărilor oferite de NIST, este esențială, incluzând etape precum clasificarea sistemelor informatice, selectarea și implementarea controalelor de securitate, evaluarea eficacității acestora și monitorizarea continuă a gradului de securitate. Evaluările periodice ale riscurilor sunt necesare pentru a menține o înțelegere actualizată a amenințărilor și vulnerabilităților în infrastructurile critice.

În plus, secțiunea discută despre importanța formării continue și a educației angajaților în crearea unei culturi de securitate cibernetică. Se recomandă utilizarea de tehnici de modelare a amenințărilor, precum STRIDE și DREAD, pentru a identifica și evalua riscurile specifice, și implementarea unui plan de răspuns la incidente care să includă proceduri clare de comunicare și roluri bine definite.

Colaborarea între sectoarele public și privat, prin parteneriate și platforme de schimb de informații, este esențială pentru consolidarea securității cibernetice. Comunicarea transparentă și partajarea informațiilor ajută la îmbunătățirea capacităților de răspuns la riscuri, fiind esențial să se stabilească cadrele legale și protocoalele necesare pentru un schimb de informații eficient.

În cadrul capitolului 5, am explorat importanța gestionării riscurilor informaționale în securitatea cibernetică a infrastructurilor critice. Gestionează eficacitatea acestor riscuri printr-o abordare sistematică care implică identificarea, evaluarea și prioritizarea riscurilor asociate. Un cadru cuprinzător de gestionare a riscurilor este esențial pentru a asigura o securitate robustă pe parcursul întregului ciclu de viață al proiectelor de securitate cibernetică. Metodele standardizate precum RMF de la NIST oferă un proces structurat pentru acest tip de gestionare.

Evaluările periodice ale riscurilor sunt fundamentale, deoarece mențin o înțelegere actualizată a amenințărilor și vulnerabilităților. Identificarea activelor critice și a controalelor de securitate este necesară pentru a prioritiza resursele și a proteja eficient infrastructurile critice. Personalizarea cadrelor existente pentru a se adapta nevoilor specifice ale sectorului cristic, cum ar fi energia sau finanțele, este un alt aspect esențial. In plus, rolul conducerii este vital pentru dezvoltarea unei culturi a securității cibernetice.

De asemenea, se evidențiază necesitatea unei structuri solide pentru planul de răspuns la incidente, împreună cu utilizarea tehnologiilor avansate, pentru a proteja infrastructurile critice de amenințările cibernetice în continuă schimbare. Un plan eficient trebuie să includă proceduri clare pentru detectarea, clasificarea și gestionarea incidentelor, iar atribuirea responsabilităților în echipele de răspuns este esențială pentru a evita confuziile. Testarea constantă și adaptarea acestuia la situații reale sunt cruciale pentru eficiența răspunsului în fața incidentelor.

Totodată, se subliniază importanța unui cadru cuprinzător pentru gestionarea riscurilor asociate furnizorilor terți, evidențiind necesitatea evaluărilor riguroase ale practicilor de securitate cibernetică ale acestora. Realizarea auditurilor de securitate este esențială pentru a asigura conformitatea furnizorilor cu standardele necesare, iar definirea clară a obligațiilor contractuale referitoare la securitate cibernetică contribuie la stabilirea unor așteptări și responsabilități bine conturate în relația cu aceștia.

CONCLUZII GENERALE

Lucrarea concluzionează prin accentuarea responsabilității personale și organizaționale în adoptarea unei mentalități proactive de securitate. Într-o lume interconectată, fiecare entitate, fie ea guvernamentală, corporativă sau individuală, joacă un rol în menținerea unei infrastructuri de securitate cibernetică robustă și reziliență.

În lumina analizelor și concluziilor extrase, se propune un model holistic de gestionare a riscurilor care să fie aplicat nu doar pentru a rezolva problemele actuale, ci și pentru a pregăti viitorul în fața amenințărilor neprevăzute. Acest model ar trebui să fie adoptat cu flexibilitatea necesară adaptării la schimbările rapide din peisajul cibernetic global. Astfel, lucrarea servește ca un ghid comprehensiv și un apel la acțiune pentru toți cei implicați în protejarea infrastructurilor critice împotriva provocărilor cibernetice ale secolului XXI.

Concluzia generală reiterează necesitatea implementării și adaptării continue a soluțiilor de securitate cibernetică în cadrul infrastructurilor critice. Prin utilizarea eficientă a metodologiilor propuse, combinată cu un angajament puternic din partea tuturor actorilor implicați, se poate asigura nu doar stabilitatea organizațională, ci și securitatea națională – un obiectiv vital în lumea interconectată de astăzi.

Pentru a proteja eficient infrastructurile critice împotriva amenințărilor cibernetice, membrii organizațiilor trebuie să adopte strategii prompte și să se angajeze într-un proces continuu de evaluare, adaptare și îmbunătățire a securității. Numai printr-o abordare coerentă și integrată vor putea acestea să navigheze în peisajul riscurilor cibernetice tot mai complexe și să asigure o protecție adecvată a datelor și sistemelor lor critice.

Practicile robuste de gestionare a riscurilor trebuie să cuprindă măsuri de prevenire, detectare și răspuns la incidentele de tip ransomware, cum ar fi efectuarea de copii de rezervă regulate ale datelor, instruirea angajaţilor și planuri de răspuns la incidente adaptate la rezilienta infrastructurii critice.

Armonizarea standardelor internațional şi implementarea lor va furnizeaza un cadru consistent și recunoscut global pentru gestionarea riscurilor informaționale, suplimentar legilor naţionale şi portiţelor existente prin interpretarea legislativă.

APORTURILE ŞTIINŢIFICE ALE TEZEI DE DOCTORAT PERSPECTIVE DE CERCETARE

- Construirea unei recenzii a literaturii de specialitate la zi şi prezentarea într-un cadru structurat a teoriilor existe şi a rezultatelor obţiunute de alţi cercetători dintr-o perspectivă critică şi identificarea unor nişe de cercetare.
- Prezentarea perspectivelor de metdologie calitativă, cantitativă şi mixtă în cadrul variantelor de cercetare, dar şi a logicii inductive şi deductive în argumentare şi a unui

spectru large de perspective metodologice şi filosofice pentru tema aleasă oferind o perspectivă completă a variantelor de cercetare existente.

- Contribuirea la o înțelegere globală a gestionării riscurilor informaționale în contextul infrastructurilor critice;
- Prezentarea perspectivelor practice și strategii de acțiune pentru îmbunătățirea eficacității proiectelor de securitate cibernetică;
- Informarea organizațiilor în vederea stabilirii unui cadru robust de securitate cibernetică prin care să se alinieze cerințelor de reglementare și standardelor în materie.
- Promovarea unei culturi a colaborării, a conștientizării și a îmbunătățirii continue în domeniul securității cibernetice a infrastructurilor critice.

CONTRIBUȚII PERSONALE

Contribuţiile personale sunt ceea ce dau valoare unei teze de doctorat atât la nivel de cercetare academică , cât şi de aport la îmbunătăţirea practicilor în lumea profesionlă, cu rezultate testate, venite din perspectivă independentă.

Contribuţia personală se rezumă la alegerea făcută de cercetător în ceea ce priveşte metodologia şi perspectiva cercetării. Anume, noutatea constă în studiul de caz ales pe GandCrab şi ISO 27001 şi departarea de aspectul tehnic deja cercetat din acest unghi evident. Ca aport personal, am încercat să am o abordare nouă în protejarea infrastrcturii critice, non-tehnică, dar ca o chestiune tehnică, ci și o responsabilitate strategică și etică, unde u doar experţii sunt respinsabili ci şi utilizatorii, care trebuie să devină responsabili şi educaţi în recunoaşterea şi adresarea riscurilor.

Astfel, am avut în vedere elaborarea unei viziuni și a unor principii care să stea la baza unei politici de securitate a informațiilor prin cultivarea unei culturi organizaționale și a unei atitudini adecvate în societate, nu numai în mediile specializate.

POSIBILE ERORI ȘI LIMITE ALE STUDIULU

Pe măsură ce transformarea digitală se accelerează, studiul de caz şi propunerile făcute vor fi depăsite din punct de vedere al soluţiilor propuse.

Viitorul multor organizații este strâns legat de capacitatea lor de a valorifica potențialul Tehnologiei Informației, dar şi ale bunelor practici manageriale şi de leadership care sunt în continuă transformare, şi atât bunele practici trebuie să ţină pasul cu activitatea dinamică din piaţă, cât şi piaţa să raspundă pozitiv la modul de administrare public şi la nevoile din mediul privat.

Eroarea de analiza poate surveni din observaţiile cercetătoarei şi raportarea la subiect ca observator obiectiv şi neutru, dar şi din limitarea cunoaşterii la momentul efectuării cercetării. Prin prezentarea unei palete largi metodologice şi a avantajelor şi a dezavantajelor existente ca de exemplu limitarea posibilităţii de generalizare, erori de analiza şi de atribuţie pot apărea, însă demersul ştiinţific al unei lucrări academice şi etica profesională limitează partinirea sau prezentarea datelor într-un mod nereal.

Ca perspective viitoare de cercetare considerăm:

- Construirea unei recenzii a literaturii de specialitate la zi şi prezentarea într-un cadru structurat a teoriilor existe şi a rezultatelor obţiunute de alţi cercetători dintr-o perspectivă critică şi identificarea unor nişe de cercetare.
- Prezentarea perspectivelor de metdologie calitativă, cantitativă şi mixtă în cadrul variantelor de cercetare, dar şi a logicii inductive şi deductive în argumentare şi a unui spectru larg de perspective metodologice şi filosofice pentru tema aleasă oferind o perspectivă completă a variantelor de cercetare existente.
- Contribuirea la o înțelegere globală a gestionării riscurilor informaționale în contextul infrastructurilor critice;
- Prezentarea perspectivelor practice și strategii de acțiune pentru îmbunătățirea eficacității proiectelor de securitate cibernetică;
- Informarea organizațiilor în vederea stabilirii unui cadru robust de securitate cibernetică prin care să se alinieze cerințelor de reglementare și standardelor în materie.
- Promovarea unei culturi a colaborării, a conștientizării și a îmbunătățirii continue în domeniul securității cibernetice a infrastructurilor critice.

4. CURRICULUM VITAE

INFORMAŢII PERSONALE

HOJDA Mihaela-Hortensia

Strada Soldat Enache Ion nr. 15, sectror 4, Bucuresti, Romania, 042082

+40 756168099

hmihaelah@gmail.com

Sexul F | Data naşterii 19/05/1990 | Naţionalitatea Romana

EXPERIENŢA PROFESIONALĂ

August 2019 - Prezent
Consilier Parlamentar Serviciul Relații Bilaterale Externe
Senatul României

Septembrie 2016 – Mai 2019
Asistent MEP
Parlamentul European – Norica Nicolai

Septembrie 2016 – Septembrie 2018
Voluntar
Scoala Gimnaziala 308, sector 5, Bucuresti

zbruarie 2016 – August 2016
Consilier
Primaria sectorului 4, Bucuresti

Mai 2015 – Februarie 2016
Manager Marketing si Comunicare
S.C. MECOTRANSREGAL S.R.L., sector 4 Bucuresti

Aprilie 2012 – Aprilie 2015
Administrator
P.F.A. HOJDA MIHAELA HORTENSIA

2009 – Iulie 2014
Consilier Relatii Publice si Comunicare
Parlamentul European – Norica Nicolai

15 Iulie – 15 Septembrie 2011
Voluntar
ONG Salvati Copiii

EDUCAŢIE ŞI FORMARE

Octombrie 2021 – Prezent

Doctorand
Scoala Doctorală de Științe Economice și Umaniste, Universitatea “Valahia” din Târgoviște -IOSUD, domeniul Management.

Ianuarie 2024 – iunie 2024

Stagiu Erasmus UPEC- Franta, Paris

Septembrie 2017 – iunie 2019

MASTER – Relatii Internationale si Studii de Intelligence
Academia Nationala de Informatii „Mihai Viteazul”

Septembrie 2014 – Februarie 2016

MASTER – Dreptul Penal al afacerilor
Universitatea Hyperion, Bucuresti

Martie 2015 – Iunie 2015

Crainic TV
INTACT MEDIA ACADEMY

Februarie – Martie 2015

Eticheta si Protocol in Diplomatie
Institutul Diplomatic Roman

Iunie 2012 – Septembrie 2014

LICENTA - Comunicare si Relatii Publice
European University - International Economic Relations / Communication and PR Montreux, Switzerland

2009 - 2011

Studenta – schimb de experienta
American University of Paris – Social and Polical Studies, Paris, Franta

Septembrie 2007 – Iulie 2009

Diplama de Bacalaureat
International School for Young Ladies Surval Mont-Fleuri, Montreux, Switzerland

COMPETENTE PERSONALE

Limba maternă: Romana

Alte limbi străine cunoscute

	INTELEGERE		VORBIRE		SCRIERE
	Ascultare	Citire	Participare la conversaţie	Discurs oral	
Engleza	C2	C2	C2	C2	C2
Franceza	C2	C2	C2	C2	C2
Spaniola	C2	C2	C2	C2	C2

Rusa	A1	A1	A1	A1	A1

Competenţe de comunicare

- Discretie si loialitate
- Disciplinata si ordonata la locul de munca si in societate.
- Organizata, convingãtore si constiinciosa.
- Capacitate de relationare cu persoane ce provin din medii culturale si etnice diverse.
- Adaptabilitate in fata unor situatii noi sau neprevazute.

Permis de conducere

B

INFORMATII SUPLIMENTARE

Referinte

- Norica Nicolai – Europarlamentar – 0723633810
- Marilena Stroescu – Inspector Scolar – 0740209777
- Dr. Ioana Stancel - 0744499317

Competenţe organizaţionale/manageriale

- Abilitati în planificarea activitatii, creativitate si initiativa.
- Abilitati de evaluare si coordonare a echipelor din subordine
- Abilitati în aplicarea si respectarea regulilor.
- O buna cunoastere a procedurilor de lucru specifice departamentului.
- Pot actiona ca interfat cu departamentele corespunzatoare pentru a rezolva problemele aparute si a imbunatati procesul de comunicare/solutionare aproblemelor aparute.

5. LISTA ARTICOLELOR PUBLICATE

A. LUCRĂRI PUBLICATE

1. Manole, A.M., Sima, A., Mieilă, C., **Hojda, M.H.,** (2024), Quality of Public Communication, as a Determinant of Romanian Citizens' Trust in Public Institutions *Annals of "Dunarea de Jos" University of Galati, Fascicle I. Economics and Applied Informatics*, 30(2), 92 – 99. ISSN-L 1584-0409, indexată **ERIH+,** RePEc DOAJ, ULRICH, WorldCat, EconLit, EBSCO, ECONIS, ZBW. https://doi.org/10.35219/eai15840409415

2. Isac, N., Hoinaru, R., Cismasu, I.D., **Hojda, M.H.,** Yousaf, Z., (2024), Strategic Business Performance in Digital Paradigm: Interplay Among Digital Orientation, Competence, and Team Creativity, Journal of the Knowledge Economy (2024) eISSN 1868-7873, JIF 4ș https://doi.org/10.1007/s13132-024-02199-y

3. **Hojda, M.H.,** (2022), Resilience for the future: between economic value and ESG struggle to deliver value. *The Journal Contemporary Economy*. 7(1): 96 – 103. ISSN 2537 – 4222. BDI: EconPapers (RePEC), IDEAS, BASE, SCIPIO, OAJI, CEEOL. http://www.revec.ro/images/images_site/articole/article_b3712ed0382cdd07cb5335a0b8bce6f2.pdf

4. **Hojda, M.H.,** (2022), Information security economics: cyber security threats. *Proceedings of the International Conference on Business Excellence*. 16(1): 584-592. eISSN 2558-9652. https://sciendo.com/article/10.2478/picbe-2022-0056

B. PARTICIPĂRI LA CONFERINȚE INTERNAȚIONALE

1. **Hojda, M.H.,** Dafina, L.C., Necula, A.I., (2024), Big data's economic impact on policy making: the way forward? *International Scientific Conference "Accounting and Finance – The Global Languages in Business"* 9th Edition. Pitești, 26 Aprilie. https://univcb.ro/storage/app/media/uploaded-files/brosura-conferinta-AFISC2024_ultvar.pdf

2. Necula, A.I., Constantin, M., **Hojda, M.H.**, Dafina, L.C., (2024), Exploring the intersection of computer science and accounting: an overview, *International Scientific Conference "Accounting and Finance – The Global Languages in Business,* 9th Edition. Pitești, 26 Aprilie.
https://univcb.ro/storage/app/media/uploaded-files/brosura-conferinta-AFISC2024_ultvar.pdf

3. **Hojda, M.H.**, (2022), Information security economics: cyber security threats. *International Conference on Business Excellence*. Fabiz, Academia de Studii Economice București, 24-25 martie.
https://bizexcellence.ro/icbe-conference/past-conferences/

4. **Hojda, M.H.,** (2022), Big Data's economic impact for policy making: the way forward? *International Conference on Innovational Challenges in Economics, Business and Applied Psychology* (*CEBAP*), May, 7 – 8.
https://issr-education.com/past-conferences/

MINISTRY OF EDUCATION
"VALAHIA" UNIVERSITY FROM TÂRGOVIȘTE
IOSUD – DOCTORAL SCHOOL OF ECONOMIC SCIENCES AND HUMANITIES
FUNDAMENTAL FIELD *ECONOMIC SCIENCES*
FIELD *MANAGEMENT*

PhD THESIS SUMMARY

„RISK MANAGEMENT OF INFORMATION IN CYBERSECURITY PROJECTS WITHIN CRITICAL INFRASTRUCTURES"

SCIENTIFIC SUPERVISOR,
Prof. Mihai MIEILĂ, PhD

PhD CANDIDATE,
Mihaela Hortensia HOJDA

TÂRGOVIŞTE
2024

6. CONTENTS OF THE DOCTORAL THESIS

"Risk management of information in cybersecurity projects within critical infrastructures"

Part I – The Current State of Knowledge in the Field of Information Risk Management within Critical Infrastructures

- **Chapter 1:** Current State of Knowledge in Cybersecurity Project Management
- **Chapter 2:** Information Security Management in Critical Infrastructures
- **Chapter 3:** Epistemological, Methodological, and Ontological Framework of the Scientific Approach

Part II – Strategies and Practices in the Field of Information Risk Management within Critical Infrastructures

- **Chapter 4:** Approach to Cybersecurity of Critical Infrastructures
- **Chapter 5:** Best Practices Guide for Improving Effectiveness in Information Risk Management for Cybersecurity Projects within Critical Infrastructures

Conclusions, Personal Contributions and Future Research Directions

Abstract Of The Doctoral Thesis

Bibliography

Appendix

7. KEYWORDS

The doctoral thesis ***"Risk management of information in cybersecurity projects within critical infrastructures"*** aims to achieve the objectives and validate the hypotheses using the following keywords:

Cybersecurity

Critical infrastructure

Cyber attacks

GANDCRAB

Best practices

Project management

IT methodologies

Risk management

Performance indicators

8. SUMMARY

Importance, Relevance, and Novelty of the Topic

Importance of the Subject The significance of managing critical infrastructure and safeguarding cybersecurity projects is one of the most complex tasks, especially in the current context of global challenges and risks. Building resilience and adaptability exemplifies leadership and the creation of best practices, action guidelines, and maintaining a working climate of continuity in the normal functioning of society (i.e., going concern).

Many critical infrastructures still operate on outdated systems that may lack the robust security features of modern technologies. These systems, which are now obsolete, were often designed without considering contemporary cybersecurity threats, making them susceptible to exploitation. Balancing the need for system modernization with the operational requirements of critical services poses a significant challenge. Upgrading legacy systems is not a straightforward task, as it requires careful planning, substantial financial investments, and may necessitate temporary interruptions of essential services.

Critical infrastructures often rely on interconnected systems, creating a complex web of dependencies. Managing cybersecurity risks becomes challenging due to the interplay between different components and the potential cascading effects of a security breach. The rapid evolution of cyber threats presents significant challenges to the integrity and resilience of critical infrastructures, encompassing sectors such as energy, transportation, healthcare, and finance.

Relevance of the Topic

The relevance of the theme is recurring, given that the activities of organizations engaged in the field of critical infrastructures must align with global and regional dynamics that may impact the risk landscape. For example, changes in international relations or the emergence of new cyber threats could pose significant risks to information security. Compliance with evolving regulations and standards also falls within the scope. Organizations' management must adapt their risk management practices to comply with changing legal regulations.

It is estimated that the number of cyber threats was approximately one billion in 2020, a level expected to rise in the coming years. Cybersecurity companies anticipate that attacks will

become increasingly sophisticated, with devastating consequences for individual activities and companies. Understanding the current trends in cyber threat manifestations allows organizations to organize the technical and organizational measures necessary to protect information.

The number of over 20 billion connected smart devices represents a significant incentive for attackers to identify new vulnerable gadgets. In the absence of minimum standards imposed on manufacturers—particularly concerning security updates, data collection and processing policies, and remediation of issues arising during use—hackers and crackers will continue to exploit vulnerabilities, whether new or previously identified, to develop increasingly larger networks of smart devices. These networks could be used to attack infrastructures, especially critical industrial infrastructures.

In the USA, the average cost per cyber incident for critical infrastructure or beyond is approximately $10 million, and it is estimated that by 2025, costs will accumulate to $10 billion, according to a study conducted by the University of Tulsa in Oklahoma. The development of deepfake technologies for cybercrime will generate new opportunities for attacks for criminals. Voice calls based on real people's voices are used in scams meant to trick employees into transferring money to the attackers' accounts, as has already happened. Unfortunately, good payers will be the most affected.

Critical infrastructures represent attractive targets for malicious actors, including terrorists and hostile states, who may attempt to compromise them to create chaos and instability. Protecting these infrastructures is, therefore, essential for maintaining a nation’s security and stability.

Novelty of the Approach

The review of the specialized literature shows that, until now, the approach to critical infrastructure and its associated risks presented a major technical perspective. This work contributes to a new understanding of the information risk management of cybersecurity projects within critical infrastructures. The novelty lies in the perspective of protecting critical infrastructure, which the author of this thesis does not consider merely a technical matter but also a strategic and ethical responsibility. Ensuring the continuity and security of these essential infrastructures requires the commitment and cooperation of all involved parties—from governments and the private sector to communities and citizens. Investments in technology, education, and public policies are crucial for building a safer and more resilient society. In an era of rapidly evolving threats and increasing complexity of interdependencies, addressing the

protection of critical infrastructures presents an ongoing challenge that must be managed with seriousness and innovation. Only through a proactive and coordinated approach can we ensure the protection of these vital resources, thereby guaranteeing the security and prosperity of the information society and society in general.

Managing cybersecurity is not just a technical issue but a strategic priority for protecting essential services. Investments in security, collaboration between sectors, and educating the public are essential for building a safer and more resilient society. Without an integrated and comprehensive approach to cybersecurity, the risks to critical infrastructures will continue to grow, threatening not only the efficient operation of essential services but also the overall well-being of citizens.

Thus, prioritizing cybersecurity becomes not only a responsibility of the leadership of the organizations operating these services but also a collective necessity in the face of global challenges. Through collaboration, education, and innovation, we can ensure that essential services remain available and secure, contributing to a more stable and prosperous future for all. It is crucial to understand that, in the digital age, cybersecurity is not optional but an imperative of contemporary society.

The perspective of the approach is one of continuous improvement, with case studies and real-world examples discussed highlighting the dynamic and evolving nature of cybersecurity challenges, emphasizing the need for ongoing enhancement and adaptation. By remaining informed about emerging threats, collaborating with the cybersecurity community, and taking a proactive stance, individuals working in organizations can effectively navigate the complex terrain of information risks within critical infrastructures.

In an ever-changing cybersecurity context, the commitment to continuous improvement and adaptive strategies will be essential for ensuring the resilience of critical infrastructures against evolving cyber threats. Organizations should prioritize proactive risk management strategies, such as privacy from the design stage, responsible disclosure of vulnerabilities, and a risk-based approach to resource allocation, to enhance their overall cybersecurity resilience.

Recommendations for future improvements in information risk management include encouraging cross-functional collaboration, particularly between IT, security, legal, and other relevant departments. Collaborative efforts ensure a holistic approach to resource allocation and risk mitigation.

Therefore, one of the key elements on which my doctoral thesis relies is the role of leadership in preventing issues and implementing ISO standards to supplement legislation for a more robust approach.

Challenges, Threats, Opportunities, and Solutions

Understanding the dynamic nature of cyber threats is essential for anticipating and mitigating potential risks to critical infrastructures. Within the context of critical infrastructures, the scope includes the security of IT systems and considerations related to the human element, such as employee training, awareness, and adherence to security policies. Perception and addressing vulnerabilities in business processes constitute integral components of information risk management, as these processes often involve managing sensitive information that may be susceptible to risks arising from internal or external sources.

External factors contributing to the scope of information risk management include geopolitical events, economic conditions, and regulatory changes.

Implementing a risk-based approach to compliance is not a one-time effort but a continuous process that evolves alongside the dynamic nature of cyber threats. Periodic reassessment of risks and compliance strategies is essential to ensure organizations' resilience to emerging threats and changes in the regulatory landscape.

Continuous improvement mechanisms, such as periodic reviews and updates of risk assessments, enable organizations to adapt their compliance strategies to the evolving threat landscape, thereby maintaining proactive and effective defense against potential cyber threats. Compliance is an ongoing process that requires constant monitoring to highlight the benefits of implementing robust monitoring systems, facilitating timely detection of deviations and enabling timely corrective actions.

Continuous monitoring is a cornerstone of effective compliance strategies for critical infrastructures. Implementing robust monitoring systems enables organizations to maintain real-time visibility over their cybersecurity posture, ensuring consistent adherence to regulatory requirements.

To ensure that international standards are effective within critical infrastructures, organizations must adapt their implementation to the specificities of each sector. While

international standards are fundamental, adaptation is crucial to address the unique requirements and challenges of various critical infrastructure sectors.

Various threat modeling methodologies are available, each tailored to different organizational needs and scenarios. Common methodologies include STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability). These methodologies provide structured frameworks for identifying and assessing threats based on various parameters, assisting organizations in systematically evaluating potential risks.

Another important aspect is education. In a 2021 blog post, Google's Global Affairs President and Legal Director Kent Walker stated that there is a commitment of $10 billion over the next five years to enhance cybersecurity, including through expanding programs, ensuring software supply, and improving open-source security across the board. In addition to this measure, Google has also launched a user education program focused on data analysis, which over 100,000 Americans have successfully completed. This educational tool from Google can prove helpful, provided individuals are genuinely interested in accessing it, particularly for reading research papers published by Google on computer security, abuse, etc., as the company has established a threat analysis group. Recommendations for future improvements include:

- **Periodic Training and Skill Development**: Invest in ongoing training programs for cybersecurity professionals to ensure they stay updated with the latest threats and technologies.
- **Integration of AI and Automation**: Explore the integration of artificial intelligence (AI) and automation to enhance threat detection, response times, and overall cybersecurity effectiveness.
- **Collaborative Research and Development**: Engage in collaborative research and development initiatives with industry peers, research institutions, and government agencies to remain at the forefront of cybersecurity innovation.
- **Participation in Information Sharing Initiatives**: Engage in information-sharing initiatives, joint exercises, and collaborative forums to address collective cybersecurity challenges.

The user represents the first line of defense against cyber threats, often being the first to identify dangers and, when necessary, report these issues to the organization's IT lead. The user's ability to prevent significant harm, both to themselves and the organization, is essential.

Thus, to enhance an organization's cybersecurity, the following aspects are important:

- Formulating a vision and principles that underlie an information security policy.
- Implementing this policy organization-wide and clearly defining roles and responsibilities.
- Cultivating an organizational culture and appropriate attitudes through the consistent application of information security principles.

Risk assessment can be conducted through either quantitative or qualitative methods. Quantitative tools include Monte Carlo analysis, simulations, PERT (Project Evaluation and Review Technique), Failure Modes and Effects Analysis (FMEA), and probabilistic safety assessments (PSA). However, in practice, projects often have insufficient data for a detailed quantitative risk analysis.

PROBLEMATIC AND HYPOTHESES

General Objective

The general objective of the thesis is influenced by Francis Bacon's thinking, who posited that genuine knowledge must be founded on empirical observations of the real world. Based on this premise, Bacon emphasized that acquiring knowledge must be an empirical activity. Practically, the work aims not only to identify alternative cybersecurity solutions related to information risk within critical infrastructures but also to assist management in choosing the most appropriate solution using innovative selection methods.

The general objectives of the thesis are to open a new approach and research space by analyzing the non-technical and non-bureaucratic elements within critical infrastructure by introducing management, ethics, and strategy as foundational pillars in the analysis and response to situations related to the management of information risks in critical infrastructure.

The work seeks to capture the rapid transformations in the economic and technological environment and how these exert considerable pressure on traditional organizational structures, often bureaucratic and resistant to changes in the external environment.

Studying project management becomes crucial for modern organizations, whether they are corporations or public institutions, as they are involved in implementing innovations such as

developing new products and services, conducting construction projects, and applying new processes. Research in management as a science has revealed the emergence of new global trends in recent decades.

The objective of the scientific activities undertaken during the documentation phase, as well as during the conceptualization and writing stage of the thesis, has been to identify and develop a new perspective on ensuring national security. This approach aims to create logical, interdependent connections and relationships between concepts such as organization, information management, cyberspace, supranationalism/realism, diplomacy, cybersecurity culture, and national security.

Specific Objectives

The specific objectives of the thesis derive from the general objectives and are:

- Understanding the reasons why a certain technology has been successfully implemented in one organization but failed in another may vary significantly depending on the theoretical perspective adopted.
- Elaborating these best practices encourages organization members to adopt a proactive mindset and develop innovative solutions that ensure critical infrastructures remain functional and resilient against an increasingly diverse range of cyber threats.
- Harmonizing technical standards and implementing them in parallel with the legislation of states for managing information risks.
- Analysis of the evolution of risk management in critical infrastructure, as well as how bureaucracy is adapting to enhance resilience and align with international best practices

Research Questions and Hypotheses

- How are best practices decided and how is knowledge adapted within security management?
- To what extent is security management affected by technical knowledge and can a lack of it be compensated for by excellence in management?
- How quickly does management adapt to change and what determines changes in best practices?

- What are the key modern trends in information risk management for cybersecurity projects within critical infrastructures and how do they align with international best practice models?
- How do different critical infrastructures differ in their approach to information risk management in cybersecurity projects and what are the implications for international best practice models?
- What are the main challenges and obstacles organizations face in implementing international best practice models for information risk management in cybersecurity projects within critical infrastructures?
- How do emerging technologies influence information risk management practices in cybersecurity projects within critical infrastructures and what adaptations are necessary in international best practice models?
- What are the potential strategies and recommendations for improving the effectiveness of information risk management in cybersecurity projects within critical infrastructures, based on a comprehensive analysis of modern trends and international best practice models?

There is consistent evidence supporting the hypothesis that adopting proactive threat intelligence and threat hunting approaches is more effective in mitigating cyber risks in critical infrastructures compared to traditional reactive strategies. This increased effectiveness stems from the ability to prevent, detect, and rapidly respond to emerging threats.

Numerous case studies and research demonstrate that implementing the ISO/IEC 27001 standard leads to a significant improvement in information security by reducing incidents and enhancing the efficiency of responses to security events. ISO/IEC 27001 certification provides credibility to organizations, assuring clients and partners of the existence of adequate information protection measures. Additionally, adopting this standard mandates a systematic risk analysis and the development of response policies and procedures.

Regarding emerging technologies such as AI and machine learning, these have begun to improve the management of cyber risks. These technologies enable the rapid identification of patterns and anomalies and automate responses; however, implementation challenges, including high costs and the need for specialized personnel, limit widespread integration. The impact of these technologies is still being assessed, and ethical concerns regarding trust in automated decisions persist.

The importance of organizational culture is emphasized as crucial for the success of risk management initiatives. A culture that promotes security awareness and encourages proactive behaviors contributes to the effectiveness of implementing security measures. Leadership plays a vital role in shaping and maintaining this culture, and investments in employee training translate into more effective outcomes.

Moreover, the text analyzes the impact of geopolitical factors and the role of government regulations, highlighting how external influences can dictate risk management strategies. Collaboration between organizations and government agencies is essential for preventing attacks, facilitating the rapid sharing of threat information. In conclusion, proactive approaches, such as threat intelligence and threat hunting, prove to be more effective in managing cyber risks compared to reactive methods, having the capacity to prevent and respond swiftly to emerging threats.

STRUCTURE OF THE DOCTORAL THESIS

Thesis Structure

The structure of the paper is designed to present, in a gradual manner but also in parallel, the developments of management systems and cybersecurity, as follows:

Chapter I emphasizes the need for adaptability and continuous innovation in project management approaches, especially in areas heavily influenced by technology, such as cybersecurity, as well as the need for high-level communication. Rapid developments and the complexity of project environments necessitate a methodical approach to planning, execution, and control, which includes a combination of technical expertise and strong interpersonal skills essential for effectively managing teams in an interconnected and dynamic world.

Chapter II highlights current trends in information security, noting that the number of cyber threats continues to grow, with attacks becoming increasingly sophisticated. The use of artificial intelligence algorithms and social engineering techniques presents significant challenges for information security, necessitating the adoption of innovative technical and organizational measures. A key component of this chapter is the utilization of ISO/IEC 27 standards, which provide a reference framework for developing and implementing information security management systems (ISMS). Adopting these standards allows organizations to effectively protect financial information, intellectual property, and personal data, ensuring operational continuity and success.

Chapter III demonstrates the importance of a well-founded research methodology to provide a significant contribution to the field of cybersecurity. The integration of qualitative methods and critical realism has proven suitable for documenting and understanding the complex and dynamic phenomena characteristic of this field, while ensuring a theoretical and practical alignment that will guide future research. The utilization of structured questionnaires, alongside the analysis of primary and secondary data, has yielded complex results demonstrating the scientific rigor and practical relevance of the research. The GandCrab case study served as a focal point for applying theory in practice, highlighting the importance of an integrated and multidimensional approach to understanding and managing cybersecurity risks.

Chapter IV analyzes the impact of the GandCrab ransomware on critical infrastructures, highlighting its operating methods and cyber implications. GandCrab, an extremely sophisticated ransomware, has been active since 2018, using advanced encryption techniques to lock users' access to data, demanding ransom payments in Bitcoin. The presented case study focuses on a specific attack on an accounting firm in the United States, where an employee opened an infected email, leading to the rapid encryption of essential files. The company, with minimal security measures, was forced to pay a significant ransom to recover the data, affecting both internal operations and its external reputation. The lessons learned underline the importance of proactive cybersecurity measures, including employee education and regular backups.

The chapter also addresses how the cybersecurity community has adapted to emerging threats, promoting measures such as proper software patch management, multifactor authentication, and cybersecurity training. The section regarding the integration of C4ISR and SIIMA approaches highlights the importance of an integrated information system for managing information flows and security in critical organizations. Fundamental concepts of cybersecurity—confidentiality, integrity, availability, authentication, and access control—are examined along with how they should be implemented to protect essential data.

Chapter V discusses the management of information risks within critical infrastructures, emphasizing the importance of a systematic approach to identifying, assessing, and prioritizing risks. Establishing a comprehensive risk management framework following NIST guidelines is essential, including steps such as classifying information systems, selecting and implementing security controls, assessing their effectiveness, and continuously monitoring security levels.

Periodic risk assessments are crucial for maintaining an updated understanding of threats and vulnerabilities within critical infrastructures.

Additionally, the section discusses the importance of continuous training and employee education in fostering a cybersecurity culture. It is recommended to use threat modeling techniques such as STRIDE and DREAD to identify and assess specific risks and to implement an incident response plan that includes clear communication procedures and well-defined roles.

Collaboration between the public and private sectors, through partnerships and information sharing platforms, is vital for enhancing cybersecurity. Transparent communication and information sharing help improve risk response capabilities, making it essential to establish the necessary legal frameworks and protocols for effective information exchange.

Within Chapter V, I explored the importance of managing information risks in the cybersecurity of critical infrastructures. It addresses the effectiveness of these risks through a systematic approach involving the identification, assessment, and prioritization of associated risks. A comprehensive risk management framework is essential for ensuring robust security throughout the entire lifecycle of cybersecurity projects. Standardized methods such as NIST's RMF offer a structured process for this type of management.

GENERAL CONCLUSIONS

The thesis concludes by emphasizing personal and organizational responsibility in adopting a proactive security mindset. In an interconnected world, every entity—whether governmental, corporate, or individual—plays a role in maintaining a robust and resilient cybersecurity infrastructure. In light of the analyses and conclusions drawn, a holistic risk management model is proposed that should be applied not only to address current issues but also to prepare for the future against unforeseen threats. This model should be adopted with the necessary flexibility to adapt to rapid changes in the global cyber landscape. Thus, the thesis serves as a comprehensive guide and a call to action for all those involved in protecting critical infrastructures against the cybersecurity challenges of the 21st century.

The general conclusion reiterates the necessity for the continuous implementation and adaptation of cybersecurity solutions within critical infrastructures. By effectively utilizing the proposed methodologies, combined with a strong commitment from all involved actors, it is possible to ensure not only organizational stability but also national security—a vital objective in today's interconnected world.

To effectively protect critical infrastructures against cyber threats, organization members must adopt prompt strategies and engage in an ongoing process of evaluation, adaptation, and improvement of security. Only through a coherent and integrated approach will they be able to navigate the increasingly complex landscape of cyber risks and provide adequate protection for their critical data and systems.

Robust risk management practices must include prevention, detection, and response measures for ransomware incidents, such as conducting regular data backups, employee training, and incident response plans tailored to the resilience of critical infrastructure. Harmonizing international standards and implementing them will provide a consistent and globally recognized framework for managing informational risks, supplementing national laws and existing loopholes through legislative interpretation.

SCIENTIFIC CONTRIBUTIONS OF THE DOCTORAL THESIS - RESEARCH PERSPECTIVES

- Building a current literature review and presenting existing theories and results obtained by other researchers from a critical perspective, identifying research niches.

- Presenting qualitative, quantitative, and mixed methodology perspectives within research variants, as well as inductive and deductive reasoning, offering a broad range of methodological and philosophical perspectives for the chosen theme.

- Contributing to a global understanding of information risk management in the context of critical infrastructures.

- Presenting practical perspectives and action strategies to improve the effectiveness of cybersecurity projects.

- Informing organizations to establish a robust cybersecurity framework that aligns with regulatory requirements and standards.

- Promoting a culture of collaboration, awareness, and continuous improvement in the cybersecurity of critical infrastructures.

PERSONAL CONTRIBUTIONS

Personal contributions are what add value to a doctoral thesis, both in terms of academic research and in improving practices in the professional world, with tested results coming from an independent perspective. The personal contribution boils down to the researcher's choice regarding the methodology and perspective of the research. Specifically, the novelty lies in the chosen case study of GandCrab and ISO 27001 and the departure from the already researched technical aspect from this evident angle.

As a personal contribution, I aimed to take a new approach to protecting critical infrastructure—not only as a technical matter but also as a strategic and ethical responsibility, where not only experts are responsible, but also users, who must become responsible and educated in recognizing and addressing risks. Thus, I considered developing a vision and principles that underpin an information security policy by cultivating an organizational culture and appropriate attitudes within society, not only in specialized environments.

POSSIBLE ERRORS AND LIMITATIONS OF THE STUDY

As digital transformation accelerates, case studies and the proposals made may become outdated in terms of the solutions proposed. The future of many organizations is closely linked to their ability to harness the potential of Information Technology, as well as good managerial and leadership practices that are continually evolving. Both practices must keep pace with the dynamic market activity, and the market must respond positively to public management and the needs of the private sector. Analysis errors may arise from the researcher's observations and their objective and neutral stance on the subject, as well as from the limitation of knowledge at the time of research. By presenting a wide methodological palette and the existing advantages and disadvantages, such as the limitation of generalization possibilities and analysis and attribution errors, can occur. However, the scientific approach of an academic work and professional ethics limit bias or the presentation of data unrealistically. Future research perspectives we consider include:

- Building an up-to-date literature review and presenting existing theories and results obtained by other researchers in a structured framework from a critical perspective, identifying research niches.

- Presenting qualitative, quantitative, and mixed methodology perspectives within research options, as well as inductive and deductive logic in argumentation and a broad spectrum of methodological and philosophical perspectives for the chosen topic, providing a comprehensive view of existing research options.

- Contributing to a global understanding of information risk management in the context of critical infrastructures.

- Presenting practical perspectives and action strategies to improve the effectiveness of cybersecurity projects.

- Informing organizations to establish a robust cybersecurity framework aligned with regulatory requirements and standards.

- Promoting a culture of collaboration, awareness, and continuous improvement in the cybersecurity of critical infrastructures.