ЮГОЗАПАДЕН УНИВЕРСИТЕТ
„НЕОФИТ РИЛСКИ“

Стопански факултет
Катедра Финанси и отчетност

ДОКТОРСКА ПРОГРАМА
ФИНАНСИ, ПАРИЧНО ОБРЪЩЕНИЕ, КРЕДИТ
И ЗАСТРАХОВКА

АВТОРЕФЕРАТ

на дисертация за придобиване на образователна и научна
степен „Доктор”
Професионално направление 3.8 „Икономика”

„Финансовите разходи за кибер риск в бизнеса и публичния сектор в Гърция“

Докторант: Мария Стефанос Куцари
Научен ръководител: доц. д-р Владимир Ценков

Благоевград, 2025г.

Дисертационният труд е обсъден и предложен за защита на заседание на катедра „Финанси и счетоводство“ към Стопански факултет на ЮЗУ „Неофит Рилски“, гр. Благоевград на ..... 2025 г.

В съдържанието си дисертацията увод, три глави, заключение, едно приложение и преглед на литературата.

Текстът е с обем от 153 страници, включващи 22 таблици и 30 фигури. Цитираната литература обхваща 111 източника.

Защитата на дисертационния труд ще се проведе на ..... година от ..... ч. в зала..... , 8-и корпус на ЮЗУ “Неофит Рилски” - Благоевград, пред научно жури.

Материалите по защитата се намират в канцеларията на катедра „Финанси и счетоводство“ на първия етаж, сграда 8 на Югозападния университет „Неофит Рилски“ – Благоевград.

СЪДЪРЖАНИЕ

УВОД

Уместност на темата

Анализирането на последиците от кибератаките става все по-значимо през последните години, особено след като цифровизацията продължава да оформя както публичния, така и частния сектор в световен мащаб. В Гърция значението на разбирането и смекчаването на киберриска е по-голямо поради нарастващата зависимост на различни индустрии и нарастващата зависимост от цифровата инфраструктура. Кибер инцидентите, вариращи от пробиви на данни до сложни фишинг атаки, имат потенциала да причинят значителни финансови щети, да нарушат основните услуги и да накърнят общественото доверие. Уместността на тази дисертация се крие в нейния фокус върху количественото определяне на финансовото въздействие на киберриска в гръцкия бизнес и публичния сектор, област, която не е проучена задълбочено въпреки критичната си важност. Разбирането на тези разходи е от решаващо значение за разработването на ефективни стратегии за противодействие на киберсигурността, насочването на политическите решения и гарантирането на устойчивостта на икономиката на Гърция пред лицето на нарастващи киберзаплахи.

Предмет, цели и основни задачи на изследването

Основната цел на това изследване е да се определят количествено финансовите разходи, свързани с киберриска както в частния, така и в публичния сектор в Гърция, с акцент върху разбирането как тези разходи влияят на по-широката икономика. Дисертацията има за цел да постигне няколко конкретни цели:

1. **Идентифициране на финансовите разходи**: Да се идентифицират и категоризират различните видове финансови разходи (преки, непреки и алтернативни разходи), които организациите понасят в резултат на кибер инциденти.
2. **Корелационен анализ:** Да се изследва връзката между честотата на киберинцидентите и финансовите разходи, поети от различни индустрии, като по

този начин се определи въздействието на киберриска върху системния индустриален риск.

3. **Оценка на въздействието:** Да се оцени общото финансово въздействие на киберинцидентите върху гръцката икономика, като се предостави информация за това как тези рискове влияят върху конкурентоспособността и устойчивостта на ключови индустрии.

4. **Прогнозно моделиране:** Да се разработи прогнозен модел, който може да оцени финансовите разходи за кибер инциденти въз основа на специфични за индустрията променливи като приходи, процент на инциденти и брой служители.

5. **Препоръки за политики:** Да се предоставят приложими препоръки за политици и бизнес лидери относно подобряването на мерките за киберсигурност и намаляване на финансовите загуби вследствие на кибер заплахи.

Методи на изследване

Изследователската методология, използвана в тази дисертация, е емпирична и количествена по своята същност и се основава на солиден набор от данни, извлечен от различни източници в Гърция и Европейския съюз. Основните методи включват:

1. **Събиране на данни:** Данните са събрани от надеждни източници като Агенцията на Европейския съюз за киберсигурност (ENISA), Гръцкия екип за реагиране при инциденти с компютърна сигурност (CSIRT) и годишните отчети на IBM за разходите за нарушаване на данните. Тези данни включват информация за кибер инциденти, финансови разходи и специфични за индустрията променливи.

2. **Изчисляване на процента на инциденти:** Процентът на инциденти (IR) беше изчислен като мярка за честотата на кибер инцидентите спрямо броя на играчите във всяка индустрия. Този показател беше използван за измерване на излагането на различни сектори на киберзаплахи.

3. **Логаритмичен регресионен анализ**: Беше използван логаритмичен регресионен модел за анализ на връзката между финансовите разходи и различни специфични за индустрията фактори, включително приходи, процент на инциденти и брой служители. Този модел позволява изследване на експоненциални зависимости, които може да не бъдат обхванати от линейна регресия.

4. **Анализ на системния риск:** Системният риск беше оценен чрез изследване на съотношението дълг/приходи на ключови индустрии, включвайки кибер инцидентите като фактор, влияещ върху този риск. Този анализ помага да се разберат по-широките икономически последици от киберриска.

5. **Двумерен анализ:** Тестовете за корелация, включително tau на Pearson и Kendall, бяха използвани за изследване на връзките между различни променливи, като процент на инциденти, финансови разходи и системен риск.

Обект на изследването

Обектът на изследването обхваща финансовото въздействие на киберриска върху ключови индустрии в частния и публичния сектор на Гърция. По-конкретно, изследването се фокусира върху седем основни индустрии: енергетика, комуникации, здравеопазване, търговия на дребно, банкиране и финанси, цифрова инфраструктура и държавни услуги. Тези индустрии бяха избрани поради критичната им роля в икономиката на Гърция и различните им нива на излагане на киберзаплахи. Проучването също така разглежда по-широкия европейски контекст, като използва данни от подобни индустрии в страни като Германия, Италия, Франция и Обединеното кралство, за да направи сравнения и да подобри устойчивостта на констатациите.

Структура на изследването

Дисертацията е структурирана в няколко ключови глави, всяка от които разглежда различни аспекти на изследването:

1. **Увод**: Предоставя общ преглед на темата на изследването, нейното значение и основните цели на изследването.

2. **Преглед на литературата:** Преглед на съществуващата литература относно киберриска, финансовите разходи и системния риск, подчертавайки празнините, които настоящото изследване има за цел да запълни.

3. **Избор на данни и методология:** Подробности за източниците на данни, процеса на събиране на данни и емпиричните методи, използвани в анализа, включително изчисляването на процента на инциденти и настройката на регресионните модели.

4. **Емпиричен анализ**: Представя резултатите от логаритмичния регресионен анализ, двумерни тестове и оценка на системния риск, като се обсъждат последиците от тези открития.

5. **Дискусия и заключение:** Обобщава основните констатации, обсъжда тяхното значение както за академичната общност, така и за лицата, вземащи решения в индустрията, и предоставя препоръки за политики.

6. **Приложения:** Включва подробни таблици, графики и допълнителни данни, които подкрепят емпиричния анализ.

Глава 1: Концепцията за кибер риск и обща характеристика

През последните години нарастващото развитие на нови технологии и използването на информационни системи, които се приписват главно на Интернет, наводниха живота ни. Използването на Интернет се счита за необходимост и стойността му за всеки бизнес в частния и публичния сектор, независимо от неговия вид, размер или географско местоположение, е безспорна.

Интернет има своите корени в ARPANET (Мрежа на Агенцията за перспективни изследователски проекти) и представлява неговата еволюция на ARPA мрежа, която започна да се развива експериментално в края на 60-те години в Съединените щати. Пионерите на интернет Лари Робъртс и Джоузеф Карл Робнет Ликлайдър в опит за по-нататъшно проучване на развитието на програмите на Пентагона ARPA (Агенция за напреднали изследователски проекти), започна да експериментира с взаимно свързване на отдалечени компютри един с друг и първоначално създаде мрежата ARPANET. В първата си фаза програмата имаше за цел да експериментира с нова технология, известна като превключване на пакети, която ще позволи на много потребители да предават и споделят данни, разделени на пакети през една и съща линия. През 1973 г. учените проведоха ново експериментално изследване, което заключи в нова техника, известна като Интернет протокол (IP), според която различни мрежи, които използват и споделят един и същ IP протокол, могат да бъдат свързани и да комуникират от една единствена мрежа. През 1983 г. ARPANET е окончателно внедрена за академична и изследователска употреба, приета от университети и организации. През 1990 г. се преименува на ИНТЕРНЕТ.

В съвременната реалност съвместната поява на интернет, информационните системи и човешкия фактор е известна като киберпространство, което представлява виртуална среда с глобално въздействие. Киберпространството и Информационните и комуникационни технологии (ИКТ) улесняват комуникацията, сътрудничеството, обмена на идеи, незабавния достъп до голямо количество информация и като разширение фундаменталната трансформация и развитие на глобалната икономика. Социалните мрежи, електронната търговия, облачните изчисления, автоматизираните процеси, новите технологии и електронните услуги са нагледни примери, които преобладават в ежедневието на индивида и постигането на бизнес целите на една компания. Освен това, киберпространството и гореспоменатите технологии осигуряват не само подобрения в сектори като

здравеопазване, образование, но също така и за производителността и рентабилността на финансовите сектори.

Информационните технологии (ИТ) се превърнаха в критичен компонент на добре функциониращите икономики, подкрепяйки икономическия растеж през последните десетилетия. Организациите както в публичния, така и в частния сектор стават все по-взаимосвързани и разчитащи на ИТ продукти и услуги, тъй като опасенията относно киберриска се засилиха, тъй като икономиката и финансовата система се цифровизират. През последните години нарастването на целенасочените кибератаки срещу правителства и фирми подчертава необходимостта от подобряване на защитата. Организациите трябва да се справят с киберинцидентите, тъй като нападателите старателно проучват своите цели, анализират слабостите им и използват тази информация, за да приспособят своите атаки. След неотдавнашните нашумели кибератаки, като инцидента с WannaCry през май 2017 г., обществената осведоменост за тези заплахи нараства.

В Гърция, според скорошно проучване, проведено от Check Point Software Technologies[1], една организация е атакувана средно 479 пъти седмично само през първата половина на годината. В сравнение с май 2020 г. има 52% увеличение на броя на кибератаките в страната. От само себе си се разбира, че има много фактори, които допринасят за появата на кибер риск във финансовите институции, включително внедряването и използването на бързо развиващи се технологии, нарастващата взаимозависимост между финансовата система и инфраструктурата на информационните технологии, нарастващата сложност на киберпрестъпниците и присъщата природа на бизнеса и услугите на финансовите институции. Като взеха предвид нарастващата сложност на киберрисковите инциденти, надзорните и регулаторните органи започнаха да предприемат стъпки срещу киберриска във финансовите институции, включително подобряване на способностите за устойчивост и прилагане на планове за ефективен отговор и възстановяване от кибератаки.

През последните години финансовият сектор възприема блокчейн технологията и криптовалутите. Тези иновации предлагат нови, децентрализирани, прозрачни и сигурни методи за транзакции. Приложението на Blockchain във финансовите услуги може

[1] "Check Point Software Technologies Ltd. (www.checkpoint.com) е водещ доставчик на решения за киберсигурност за правителства и корпоративни предприятия в световен мащаб".

допълнително да демократизира достъпа до финансовата система, особено за трансгранични транзакции и парични преводи (www.searchmyexpert.com, 2024 г.). Освен това, иновативното използване на изкуствен интелект (AI) и машинно обучение (ML) във финансовите услуги трансформира индустрията. AI и ML подпомагат създаването на персонализирани финансови продукти, подобряват оценката на риска, откриват измами и подобряват обслужването на клиентите, правят финансовите услуги по-достъпни, ефективни и сигурни, като по този начин допринасят значително за финансовото включване (Световна банка, 2022 г.).

През последните години в областта на финансите можем да споменем, че дефиницията на риск не е ясна, но може да се формулира като вероятност крайната възвращаемост (печалба и загуба) да се различава от очакваната.

Като цяло, рискът изразява несигурност относно бъдещи ситуации, развития, чиито резултати могат да повлияят на постигането на краткосрочните и дългосрочните цели на компанията. Можем да идентифицираме риска като мярка за несигурност, която показва несигурност относно резултата от резултатите, които могат да се различават от очакваното по положителен или отрицателен начин. Количественото определяне на несигурността се измерва с помощта на статистически величини като стандартно отклонение. С други думи, ние се опитваме да създадем измерване на вероятността реализираното представяне да се различава от очакваното.

Гърция има актуализирана национална стратегия за киберсигурност, базирана на 5 общи оси, 15 конкретни цели и повече от 50 действия.

От решаващо значение е организациите да предприемат мерки, за да се защитят по-добре от кибератаки. По-специално, организациите трябва да създадат цялостни програми за управление на риска и киберсигурност под ръководството на отдела за ИТ ръководители, главния изпълнителен директор или главен служител по риска, докладващ на главния изпълнителен директор.

Независимо от ролята на публичния и частния сектор в управлението срещу заплахите за киберсигурността, има други фактори, които могат да подкрепят това важно начинание. Всеки отделен индивид като единица носи отговорността да защитава собствената си система и данни и като цяло цялата общност. Не е достатъчно правителствата да осигурят информираност на гражданите, ако те не желаят да прилагат

знанията, които са получили. С други думи, в съответствие с правилните инструкции лицата трябва да предприемат технически мерки за сигурност, поведенчески мерки за сигурност и да докладват за кибер инциденти.

Таблица 1: Частен и публичен сектор и тяхното представяне в кибернетичното управление

Частен сектор	1. Техническа сигурност 2. Политики за сигурност 3. Повишаване на осведомеността (имейли, уебсайтове) 4. Одити и оценки 5. Планове за киберкризи 6. Подкрепете правоприлагащите органи 7. Насърчаване на международните норми 8. Противопоставяне на терористичните актове и дезинформацията
Правителство	Закони 2. Извършване на периодични доклади за състоянието на киберсигурността 3. Упражнения и одити за съответствие на киберсигурността 4. Научноизследователска и развойна дейност 5. Работни групи 6. Подкрепете служители, граждани и малки и средни предприятия 7. Техническа охрана 8. Повишаване на осведомеността (обучения)

Източник: Авторски труд (2023)

На първо място има прости технически и поведенчески превантивни мерки, които можем да предприемем, като заключване на екрана, когато компютърът е деактивиран, криптиране на чувствителна информация, преди да я изпратим на външни получатели, споделяне на чувствителна информация само с оторизирани субекти и проверка на имейл адресите на получателите, преди да изпратите имейли. (Reveron D.S. & Savage J.E. 2020).

Освен това има много квалифицирани образователни институции, които могат да предоставят на служителите в публичния и частния сектор и на всеки желаещ индивид дигитални знания и умения за всичко, свързано със защитата на техния дигитален свят и особено как да предотвратяват кибер заплахи.

Глава 2: Изследване на цифровите финансови услуги в стратегиите за киберсигурност в Гърция

Киберсигурността в Гърция обхваща широк набор от дейности и агенции, насочени към защита както на частния, така и на публичния сектор от киберзаплахи. Една година след въвеждането от страна на ЕС на неговата първоначална стратегия за киберсигурност, отделът за киберпрестъпления беше създаден в рамките на гръцката полиция (Президентски указ № 178/2014). Този отдел има за цел да предотвратява, разследва и спира престъпления и антисоциално поведение, извършвани онлайн или чрез други електронни платформи. Едновременно с това, след първоначалната директива за NIS, беше създаден Националният орган за киберсигурност (NCSA) (Президентски указ № 82/2017) и определен като национален компетентен орган на страната за киберсигурност (N. 4577/2018). Освен това през 2019 г. Гърция замени своето Министерство на цифровата политика, комуникацията и медиите от 2016 г. с актуализираното Министерство на цифровото управление (Президентски указ № 81/2019), което се фокусира върху ускоряване на цифровата трансформация на публичния сектор, намаляване на бюрократичните препятствия, привеждане на цифровите политики в съответствие с електронното управление и обществени услуги и подобряване на оперативната съвместимост на всички нива. Тази промяна, съчетана с пандемията Covid-19, доведе до повишена зависимост от интернет за различни дейности, насърчаване на дигиталната грамотност и модернизирането на услугите в гръцкото общество. Освен това Гърция активно участва в международното сътрудничество в областта на киберотбраната, включително инициативите на НАТО за киберотбрана и програмите на Европейския съюз за киберсигурност.

Националната разузнавателна служба (EYP) също играе ключова роля, като се фокусира върху защитата на националната сигурност от шпионаж, тероризъм и киберпрестъпления, действайки като национален екип за реагиране при компютърни спешни ситуации - CERT (NCERT-GR, RFC2350). Въпреки че не е акредитиран от TI, GRNET-CERT - националната организация за реагиране на инциденти в сферата на киберсигурността в Гърция, създадена през 2003 г. и хостван от Националните инфраструктури за изследвания и технологии, е единственият акредитиран CERT. Наскоро EYP придоби известност поради предполагаемото използване на шпионски софтуер

Predator за наблюдение на мобилни телефони на политици, журналисти и бизнес лидери (politico.eu). Въпреки че този инцидент има кибернетични елементи, той остава вътрешен проблем, който се разследва и следователно не е в центъра на тази теза. Въпреки това тази ситуация повлия на неотдавнашното допълнение към гръцката конституция със Закон № 5002/2022, който се отнася до разсекретяването на комуникациите, подобряването на операциите на EYP, защитата на поверителността на комуникацията срещу софтуер за наблюдение, укрепването на националната киберсигурност и защитата на поверителността на данните на гражданите (Sotiropoulou, 2023).

На практическо ниво Атина беше мястото на един от първите пет подготвителни семинара за встъпителното Общоевропейско учение по киберсигурност за защита на критичната информационна инфраструктура (CIIP), наречено „Кибер Европа 2010“ през септември 2010 г.

Това събитие, подкрепено от ENISA (Агенция на Европейския съюз за киберсигурност) и Съвместния изследователски център, беше предназначено да насърчи сътрудничеството между европейските нации за справяне с експанзивни кибер заплахи. Освен това, Гърция ръководи и два проекта на PESCO (постоянно структурирано сътрудничество в рамките на Европейския съюз), свързани с киберсигурността: Платформата за споделяне на информация за киберзаплахи и реагиране при инциденти и командния пункт (CP) за малки съвместни операции (SJO) на тактическото командване и контрол (C2) на разполагаемите сили за специални операции (SOF) – известни като SOCC за SJO. През 2022 г. увеличаването на кибератаките срещу критична инфраструктура и тези, свързани с конфликта в Украйна, въведе нови стратегии за управление на кибер рисковете. Те включват разработването на независима оперативна система, наречена Thorax, която ще се интегрира в Трети отдел на Генералния щаб на националната отбрана на Гърция. Thorax има за цел да използва големи данни, изкуствен интелект и различни алгоритми за управление на огромния ежедневен приток на информация за откриване на заплахи и автоматизиране на отговорите. Освен това Инструментът за техническа помощ и обмен на информация на Европейската комисия, в сътрудничество с гръцките министерства на външните работи и цифровото управление, проведе семинар в Солун през юни 2022 г. на тема „Ролята на кибер екосистемата на ЕС в глобалната стабилност на киберсигурността“ (ENISA, 2022a). Инициирана от Европейския колеж по сигурност и отбрана и ENISA, с

участието на партньори от Западните Балкани, тази конференция улесни ценен обмен между регионални експерти и политици, повишавайки доверието и устойчивостта. Това е в съответствие с две стратегически цели на ЕС и Гърция: киберсигурността и интегрирането на Западните Балкани в тези рамки. Освен това Международният панаир в Солун през 2022 г. приветства ENISA за първи път в подкрепа на дейностите на Европейската година на младежта 2022 г., целящи насърчаване на по-приобщаващо цифрово бъдеще и повишаване на осведомеността относно уменията за киберсигурност. Тези усилия включват създаването на платформа за уведомяване за инциденти, разработена в партньорство с известна международна организация, известна като CSIRT (Екип за реагиране при инциденти с компютърната сигурност). CSIRT всъщност е подразделение на военното разузнаване и по този начин отговаря за разработването на разпоредби, системи за сертифициране и допринася за предотвратяването и реагирането на кибератаки в цялата страна.

Тази усъвършенствана рамка за киберсигурност изигра ключова роля за това Гърция да се нареди на 7-мо място в Националния индекс за киберсигурност (NCSI), сравнявайки нейните мерки за киберсигурност с други нации в световен мащаб от 2016 г. до 2023 г. Индекс NCSI. Придържайки се към систематична стратегия за развитие, Гърция напредна значително, за да си осигури челна позиция сред 160 държави през 2019 г. Този индекс оценява мерките, приложени от различни съответни гръцки органи, като отдела за киберотбрана, отдела за киберпрестъпност, националния CERT, гръцкия орган за комуникационна сигурност и гръцкия орган за защита на данните, и др.

Подходът на гръцкото правителство към киберсигурността също така включва образователни инициативи за гражданите и политиките на банковия сектор относно образованието по киберсигурност, заедно с ролята на изкуствения интелект (AI) за подобряване на киберсигурността. Гръцкото правителство призна важността на киберсигурността и работи активно за подобряване на способностите на нацията за киберотбрана. Това включва създаването на национална стратегия за киберсигурност, която очертава визията и плана за действие на правителството за подобряване на киберсигурността във всички сектори. Стратегията набляга на защитата на критичната национална инфраструктура, подобряването на сътрудничеството между публичния и частния сектор и привеждането в съответствие с международните стандарти и най-добри практики за киберсигурност. За да образова гражданите относно киберсигурността,

гръцкото правителство, често в сътрудничество с Европейския съюз, стартира различни кампании за осведомяване. Тези инициативи имат за цел да повишат общественото разбиране за киберрисковете и да насърчат безопасно онлайн поведение. Образователни програми и ресурси, като съвети за онлайн безопасност, работни срещи и семинари, се предоставят на обществеността, за да помогнат на хората да се защитят от киберзаплахи (Бойко, Василенко и Кухаренко, 2019).

Бизнес пейзажът в Гърция реагира на нарастващите киберзаплахи. С нарастващите кибератаки, насочени към бизнеса – от малки и средни предприятия до големи предприятия – гръцките компании инвестират повече в решения за киберсигурност. Тази инвестиция надхвърля простото спазване на Общия регламент за защита на данните на ЕС (GDPR) и се придвижва към по-холистичен подход към киберустойчивостта. Това включва приемане на усъвършенствани технологии за киберсигурност, обучение на служители и прилагане на стабилни стратегии за реакция при инциденти. От самото си създаване гръцката NCSA е приложила различни закони и разпоредби, които са оформили гръцкия пейзаж на киберсигурността на бизнес ниво. Тези инициативи служат като образцови модели за други нации, осигурявайки солидна основа за предизвикателните последващи фази на изпълнение и прилагане. Сред резултатите е рамка за оценка на зрелостта, която позволява на организациите прогресивно да повишават зрелостта си по отношение на киберсигурността.

Този процес включва стабилизиране на текущото ниво, преди да се премине към по-високи нива чрез текущи организационни подобрения. Това се постига чрез използване както на количествени, така и на качествени данни за вземане на решения. Например, на ниво на зрялост 2, организациите преминават от "ad hoc" подход към "управлявано" ниво чрез установяване на стабилни контроли и процеси за сигурност. Освен това тази рамка може да бъде приета на европейско ниво, за да ръководи приоритизирането на плановете за смекчаване и финансирането на киберсигурността. В сценарии, при които пълен преглед на сигурността не е осъществим, провеждането на ефективни оценки на риска за киберсигурността и прилагането на смекчаване в големи критични инфраструктури може да послужи като временен подход (Maglaras et al., 2020 г.)

От средата на 90-те гръцките банки работят за укрепване на пазарната си позиция и повишаване на оперативната си ефективност. Това усилие до голяма степен е мотивирано от промени в европейския банков сектор и инвестиционни перспективи в Югоизточна

Европа. Въпреки това банковият сектор на Гърция в момента е изправен пред изключителни предизвикателства, включително проблеми, свързани с ликвидността и рентабилността. Тези предизвикателства се дължат основно на фискалния и макроикономическия спад в Гърция, както и на многобройните понижения на суверенния кредитен рейтинг на страната. През последните години обаче кибератаките се превърнаха в сериозна и нарастваща загриженост. Честотата на кибератаките срещу финансови институции в Гърция остава несигурна, тъй като четирите основни системни банки не публикуват официални доклади или записи. Смята се, че десетки хиляди инциденти се случват годишно, като услугите за електронно банкиране са основният фокус на тези кибер нападатели, поради факта, че фишингът и нарушенията на данните могат да доведат до значителни финансови загуби за институциите, като същевременно генерират значителни печалби за нападателите.

Тъй като банковата система на Гърция е напълно включена в регулаторната рамка на Европейската централна банка, гръцките институции се придържат към така наречените Директиви за платежни услуги (PSD), които се издават от Европейската централна банка (ЕЦБ) на годишна база. Целта на тези директиви е да изградят защитен щит върху платежните услуги и финансовите транзакции в Европейското икономическо пространство. Наскоро ревизираното законодателство за PSD2 прие технологията API (интерфейс за програмиране на приложения), позволяваща на банките да намалят рисковете за сигурността при платежните транзакции чрез архитектурен модел на API. Този модел включва допълнителни слоеве за защита от измами и удостоверяване, тъй като позволява интегрирането на функции за сигурност като контрол на достъпа и откриване на заплахи директно в услугите за споделяне на данни. Този проактивен подход позволява засилени мерки за сигурност. Освен това, с консенсус относно единна техническа спецификация, всички системи в ЕС биха могли потенциално да се сближат с един или ограничен брой технически стандарти на API (Gounari et al., 2024).

Не на последно място, банките в Гърция също играят важна роля в обучението на гражданите относно киберсигурността. Признавайки, че финансовите услуги са основна цел за кибератаки, гръцките банкови институции са приложили мерки за повишаване на осведомеността сред своите клиенти (Бойко, Василенко и Кухаренко, 2019). Например Националната банка на Гърция, една от водещите банкови институции в страната, редовно разпространява информационни листовки за киберсигурност, за да образова своите

корпоративни клиенти и клиенти на дребно. Те включват предоставяне на информация за това как да разпознавате фишинг имейли, сигурни практики за онлайн банкиране и значението на защитата на личната и финансова информация. Много банки предлагат ресурси на уебсайтовете си и провеждат разяснителни кампании, за да информират клиентите за най-новите кибер заплахи и как да ги избегнат (nbg.gr).

След неотдавнашен подобен мандат на Асоциацията на бизнеса и индустрията (BSE), всяка компания е длъжна да назначи главен служител по сигурността на информацията (CISO) и да създаде екип, отговорен за разработването и наблюдението на стратегията за киберсигурност. Ако мащабът на бизнеса не гарантира подобни роли, би било полезно да се координират усилията за осигуряване на безопасни цифрови операции и осигуряване на обучение за участващите. Според същата образователна директива отговорностите за киберсигурност се простират извън ИТ отдела; Всички служители трябва да са бдителни, тъй като по -голямата част от нарушенията се случват чрез фишинг имейли или спам, че всеки служител може по невнимание да отвори. Ето защо е жизненоважно последователно провеждането на програми за обучение и информационни кампании (обхващащи най -добри практики, казуси и т.н.), за да се подготви персоналът да реагира ефективно на цифрови заплахи.

Изкуственият интелект (AI) се превърна в мощен инструмент в борбата срещу кибер заплахите, предлагайки нови възможности за засилване на киберсигурността в Гърция и извън него. AI може да анализира огромни количества данни, за да идентифицира модели и да открие аномалии, които могат да показват кибератака. Това позволява ранното откриване на заплахи и бърз отговор на потенциални нарушения на сигурността. AI-задвижваните системи за сигурност могат да автоматизират мониторинга на мрежовия трафик, да идентифицират уязвимостите и дори да предскажат бъдещи вектори за атака въз основа на текущите тенденции. Освен това AI може да помогне за справяне с разликата в уменията за киберсигурност чрез автоматизиране на рутинните задачи, което позволява на човешките експерти да се съсредоточат върху по -сложни предизвикателства. Важно е също така да се отбележи, че с напредването на технологията AI киберпрестъпниците могат също да използват AI за злонамерени цели, което налага непрекъснати иновации и адаптиране в стратегиите за киберсигурност (Citictel-CPC.com, 2023).

Въз основа на Европейската агенция за отбрана (EDA) Гърция активно инвестира в технологии за изкуствен интелект (AI) за военни цели и е участник в няколко европейски инициативи за отбрана. Гръцките отбранителни индустрии, включително Хеленската аерокосмическа индустрия, Intracom отбранителна електроника и EFASSYS, са ключови играчи в разработването на AI-управлявани системи, специализирани в електрониката, комуникациите и безпилотните системи. Гърция участва в множество финансирани от Европа програми за AI, насочени към подобряване на военните възможности и операции. Те включват програмата LOTUS за разработване на ниско наблюдавани тактически безпилотни въздушни системи, програмата SMOTANET, фокусирана върху тактическите мрежови устройства, и проекта INDY, който изучава съхранението и разпределението на енергията за военни звена. Допълнителните проекти включват COMMANDS за операции с управлявани и безпилотни системи, Европейската инициатива за патрул CORVETTE И ACHILLES, която има за цел да развие рояци от безпилотни превозни средства за отбрана. Други забележителни инициативи включват AVICOM за подобряване на комуникациите в сценарии за бедствия и Agile 4.0, проекта за подобряване на цифровите иновации и пъргавото производство в сектора на индустрията (eda.europa.eu). На фона на геополитическите предизвикателства, породени от регионалната динамика и Турция, Гърция има за цел да засили своите отбранителни възможности чрез AI, което може да осигури стратегически предимства пред численото превъзходство. За да може Гърция да използва напълно AI в отбраната, тя трябва да преодолее вътрешните ограничения и да обхване по -широка визия, която включва културно наследство, образователна реформа, опазване на биоразнообразието и засилени съюзи в средиземноморието и извън него. Този цялостен подход е от съществено значение за подобряване на геополитическата позиция на Гърция и насърчаване на продуктивен и иновативен национален етос.

Глава 3: Анализ на финансовите разходи за кибер риск в бизнеса и публичния сектор в Гърция

Като цяло е трудно да се определят количествено точните финансови разходи за киберриск, тъй като тези разходи могат да варират в широки граници в зависимост от размера и вида на бизнеса или организацията, както и от специфичното естество и въздействие на киберинцидента. Въпреки това, все още можем да оценим средните разходи за киберинцидент, като използваме външни надеждни финансови отчети и да ги използваме за целите на тази дисертация. Тези парични преки или косвени средни разходи ще ни позволят да тестваме корелационния ефект, както и степента на въздействието им върху компонента на системния риск на съответната бизнес индустрия, от една страна, и общата връзка между разходите и типовете кибер инциденти, от друга. Следователно, нашето изследване беше проведено въз основа на хипотезата, че: Кибер рисковете като цяло в гръцката икономика представляват реална измерима финансова опасност, но не са фактор за увеличаване на системния риск. Вероятността от отделни киберрискови събития с големи щети е значителна и е свързана не само с настъпването на по-големи финансови щети и разходи за компаниите, но и с вероятността за въздействие върху системния риск като цяло.

Накрая ще направим опит да отговорим на един жизненоважен въпрос, който буквално интересува политиците, независимо дали оперират в частния или публичния сектор: до каква степен са проблем киберинцидентите?

С други думи, ще се опитаме да измерим загубите, причинени от киберриска, като процент от приходите на индустрията, върху която се фокусираме, и по този начин да предоставим полезни насоки на вземащите решения относно киберинвестициите, които трябва да предприемат, за да повишат киберсигурността на организацията и да смекчат последствията от кибератаките.

Обобщение на емпиричните резултати

Описателен анализ на киберинциденти

1. Класификацията на киберрисковете въз основа на честотата на възникването им като процент от общия брой киберинциденти показва, че докладите за нарушаване на данните представляват мнозинството (32%) сред 171 наблюдения през годините 2014-2021

във всички индустрии, следвани от атаки със зловреден софтуер (25%), фишинг (23%) и накрая нарушения на поверителността (20%).

2. Докладите за нарушаване на данните са се увеличили трикратно от малко над 15 000 през 2017 г. до над 45 000 през 2021 г., аналогично, подобно на идеята за нарушаване на данните, нарушенията на поверителността са се увеличили рязко в това времево пространство от само няколко хиляди случая през 2014 г. до над 40 000 инцидента през 2021 г.

3. Напротив, зловреден софтуер и фишинг атаки през периода 2014-2021 г. показват относително постоянна динамика, когато става дума за абсолютен брой записи на инциденти.

4. Що се отнася до абсолютния брой наблюдения, свързани с всички видове киберинциденти по сектори и по процент на инциденти, можем да посочим, че секторът на търговията на дребно се откроява от останалите по размер (повече участници и по-високи приходи), поради което повечето от нашите наблюдения и последващи записи на инциденти идват от този конкретен сектор - 32% от всички наблюдения.

5. Държавните служби, по отношение на абсолютния брой наблюдения, свързани с всички видове киберсъбития, изпитват относително много киберинциденти – 27% от всички наблюдения.

6. По абсолютен брой инциденти, свързани с всички видове киберсъбития, най-малко са инцидентите в енергетиката, здравеопазването и дигиталната инфраструктура.

7. По отношение на показателя „Процент на инциденти по сектори“ – секторите на комуникациите, енергетиката и цифровата инфраструктура поемат по-голямо въздействие на киберриска поради по-висок процент на инциденти.

8. Що се отнася до киберрисковете от пробиви на данни и злонамерени софтуерни атаки, секторите на банковата и цифровата инфраструктура показват висока волатилност в периода 2014-2021 г. по отношение на средната цена на инцидент. От друга страна, както държавните услуги, така и пазарният сектор на дребно не претърпяват значителни променливи промени през изследвания период по отношение на средните разходи за киберсъбитие на инцидент; нарушение на данните в правителствения сектор може да доведе до средни разходи от 3 млн. €, докато атака със зловреден софтуер в сектора

на търговията на дребно може да доведе до по-малко от 1 млн. € финансови и корпоративни загуби.

Описателна статистика

1. Пробивът на данни се счита за най-сериозният инцидент сред всички видове, независимо от обхвата на бизнеса, средната стойност на средните финансови разходи, причинени от нарушение на данните, е 2,43 милиона евро. Нарушенията на данните водят до подобни финансови и корпоративни разходи във всички индустрии, представляващи интерес.

2. Въз основа на индикатора за средна цена на инцидент (ACC), класирането на видовете киберриск е както следва: нарушение на данните с 2,43 милиона евро на инцидент; нарушения на поверителността с 2,34 милиона евро на инцидент; фишинг събития с €2 милиона на инцидент; злонамерена софтуерна атака с 1,80 милиона евро на инцидент.

3. Въз основа на описателната статистика за различните видове киберинциденти и разделянето на наблюдаваните случаи на отделни квартили според размера на претърпените щети, можем да посочим, че средните стойности на първите 25% от наблюденията (Квартил 4) показват два пъти по-висока средна цена на инцидент в сравнение с тези за цялата група наблюдения: нарушения на данните € 5,26 милиона за Q4 срещу € 2,43 милиона за Q4 цялото население; нарушения на поверителността 5,01 милиона евро за Q4 срещу 2,34 милиона евро за цялото население; софтуерни атаки 4,93 милиона евро за Q4 срещу 1,80 милиона евро за съвкупността; фишинг събития 4,90 милиона евро за Q4 срещу 2,00 милиона евро за съвкупността.

Тези данни показват, че докато средната цена на инцидент за всички индустрии е относително ниска, в 25% от случаите (Q4) загубите от кибер инциденти могат да бъдат многократно по-големи от средното очакване като цяло. Това повдига не само въпроса за значението на киберсигурността като цяло, но и въпроса за значителната възможност при 25% от инцидентите размерът на щетите от реализирането на различни видове киберрискове да бъде двойно по-голям от средното за индустрията очакване. Този проблем е особено важен за големите корпорации, където поради по-големия мащаб можем да очакваме да реализираме по-големи щети от възникването на някой от кибер рисковете. Въпросът придобива допълнително значение, като се има предвид фактът, че най-високите

средни стойности през Q4 са регистрирани специално за кибер събития с най-висок запис на регистрирани събития - пробиви на данни (32%) (Q4 - €5,26 милиона), атаки на зловреден софтуер (25%) (Q4 - €4,93 милиона), фишинг (23%) (Q4 - €4,90 милиона) и накрая нарушения на поверителността (20%) (Q4 - 5,01 милиона евро).

Ако в 25% от случаите (квартил Q4) средната цена на инцидент надвишава приблизително два пъти тази референтна стойност, типична в останалите 75% от случаите, възниква въпросът компаниите от кои сектори са най-застрашени от тези по-високи загуби. Като се имат предвид данните, представени за индикатора „Процент на инциденти по отрасли“ (Фигура 14), бихме могли да предположим, че потенциално това са компании главно в секторите на цифровата инфраструктура, комуникациите, енергетиката и банкирането. Отчитайки другия показател „Средни разходи по отрасли” можем да предположим, че основната заплаха идва от банковия и правителствения сектор. Въпреки че техният процент на инциденти е по-нисък в сравнение с IR на секторите на цифровата инфраструктура, комуникациите, енергетиката, средните разходи по отрасли за правителствения и банковия сектор са приблизително два пъти по-високи: а) банков 44,93 (милиона евро) и правителствен (публичен) сектор 39,58 (милиона евро), срещу б) енергетика 22,34 (милиона евро) и цифров 19,84 (милиона) евро).

Секторът на комуникациите може да се разглежда като подобен на правителствения и банковия сектор - има много сходен процент на инциденти (приблизително 0,22 срещу 0,21 за банковия и публичния сектор) и сравнително високи средни разходи от 29,29 милиона евро.

Секторът на търговията на дребно, въпреки че има най-високи средни разходи, има приблизително пет пъти по-нисък „Процент на инциденти по отрасли“.

4. По отношение на показателя „Средни разходи по отрасли” (ACI) данните показват следната класификация: Сектори търговия на дребно 16 985,46 млн. евро; здравеопазване 114,18 милиона евро; банково дело 44,93 милиона евро; държавен (публичен) сектор 39,58 млн. евро; комуникации 29,29 млн. евро; енергетика 22,34 млн. евро; цифрови технологии 19,84 млн. евро;

Секторът на търговията на дребно, поради естеството и мащаба си, обхваща дейностите на много компании, както големи мултинационални, така и малки семейни фирми, така че е разбираемо, че този сектор отбелязва най-високите средни разходи,

свързани с кибератаки. Големият мащаб на сектора, обусловен от големия брой работещи компании, предопределя и най-високите общи обеми на инциденти и следователно най-високите общи финансови разходи поради неговия размер. Трябва да се отбележи, че въпреки че поради своя размер секторът на търговията на дребно показва най-висока стойност на показателя „Средни разходи по отрасли“, този сектор се характеризира и с най-ниска стойност на показателя „Инцидент по отрасли“. От друга страна, публичният сектор и банковият сектор регистрират баланс на показателите „Средни разходи по отрасли“ и „Процент на инциденти по отрасли“ (IR), показващи средни нива и за двата показателя, водещи до извода за наличие на рискова експозиция, предполагаща относително висока IR, придружена от значителни средни разходи, свързани с прилагането на кибер рискове. Останалите индустрии показват или висок IR, придружен от ниска средна цена по индустрия и обратно.

Компаниите за цифрова инфраструктура в Гърция имат най-ниските финансови разходи като цяло в сравнение с останалите индустрии. Може би това се случва, защото тези компании не се занимават с чувствителни потребителски данни, а по-скоро прилагат нови технологии, за да поддържат и подобряват съществуващите цифрови мрежи в името на икономиката като цяло.

5. Когато става въпрос за разглеждане на въздействието на киберрисковете в контекста на влиянието, което те могат да окажат върху големите компании от типа „твърде големи, за да фалират“ (Too Big to Fail – TBTF) и съответно върху системния риск като цяло, следва да се отбележи, че през периода 2014-2021 г. частните компании от категорията TBTF, и по-специално тези в банковия сектор, показват стабилно намаляване на експозицията към риск. Обратно, публичният сектор не само запазва постоянна експозиция към риск за целия изследван период, но и регистрира високи стойности на показателя „Средна цена на инцидент“, което показва висока вероятност успешните и мащабни кибератаки да попаднат в горния квартил (Q4) на вредоносните инциденти, характеризиращи се с голяма средна цена на инцидент. В резултат на това единичните киберинциденти имат значително въздействие върху системния риск като цяло.

6. Наличието на ясна вероятност киберрискови събития да доведат до значителни щети се посочва от описателната статистика на показателите „Честота на инцидентите“ и „Приходи на индустрията“ за всички сектори (Таблица 11). Наблюдаваните разпределения

на тези два показателя регистрират наличието на „дебели опашки“, което показва възможността за възникване на киберрискови събития с голям мащаб на реализираните щети. Средните и медианните стойности сочат, че поне 15% от индустриалните участници преживяват един или повече инциденти годишно. Горепосочените факти допринасят за характеризиране на риска в гръцкия публичен сектор, тъй като те не само посочват статистическата вероятност за възникване на киберрискови събития като цяло, но и по-пропорционално – вероятността от щети, които надвишават стойността на отделните такива събития. Това, наред с факта, че публичният сектор също демонстрира по-високи стойности на показателя „Средна цена по индустрии“ за единичен киберрисков инцидент, отново подчертава проблема с повишената експозиция на гръцкия публичен сектор към киберрискове.

Резултати от двувариантния анализ

1. Съществува положителна статистически значима корелация между „Средни разходи за инцидент – ACI“ (скаларна променлива) и „Честота на инцидентите по индустрии за съответната година – IR“ (ординална променлива). Коефициентът на корелация показва слаба до умерена положителна връзка между двете променливи (0.23).

2. Измерването на връзката между „Честота на инцидентите по индустрии – IR” и „Системен риск – SR” показа наличието на отрицателна корелация между двете променливи от -0.20, която е статистически значима на ниво 0.01 (0.007).

3. Наблюдава се и отрицателна корелация между показателите за „Честота на инцидентите“ и „Приходи в индустрията“ – корелационният коефициент е отрицателен (-0,48) при критично ниво на значимост 0,01. Резултатите показват, че когато обемът на киберинцидентите в дадена индустрия се увеличава, общите приходи на индустрията намаляват. Тази обратна връзка е силно изразена, като при всяко единично увеличение на киберинцидентите приходите намаляват с 0,5 единици.

4. Корелационният анализ на връзката между „Тип инцидент“ и „Средни разходи“ от една страна и „Системен риск“ от друга показва: когато „Средните разходи на инцидент“ се разглеждат като зависима променлива, се наблюдава много слаба, но положителна корелация с „Тип инцидент“ (0,165); както и слаба, но статистически значима положителна корелация между „Системен риск“ и „Тип инцидент“ (0.176).

Логаритмичен анализ – Уравнение (4)

Резултатите от регресионния анализ на уравнение (4), използвайки данни от всички изследвани индустрии, показват:

1. Съществува слаба отрицателна връзка между индустриалните приходи (IREV) и средните разходи на киберинцидент (ACC), т.е. увеличаването на приходните квоти може потенциално да намали финансовото въздействие (средно) на кибератака. Резултатите от логаритмичната регресия показват (коефициент от -0,0005, Фигура 18), че 10% увеличение на индустриалните приходи се очаква да доведе до 0,005% намаление на средните разходи на киберинцидент. От друга страна, когато се разглежда очакваната стойност на разходите за един киберинцидент (или IR=1) = 0,0032 (Фигура 18), корпорациите, които принадлежат към индустрия с оборот от 1 милиард евро, биха понесли средни разходи от 0,0032 млрд. € или 3,2 милиона € на киберинцидент.

2. Съществува слаба положителна връзка между честотата на инцидентите (IR) и средните разходи на киберинцидент (ACC), т.е. увеличаването на броя на инцидентите може потенциално да доведе до по-високи средни финансови загуби от кибератака. С други думи, колкото повече киберинциденти се случват, толкова по-голямо е средното им финансово въздействие. Това може да се дължи на факта, че честите атаки изискват повече ресурси за справяне с тях или че натрупващите се инциденти водят до по-големи щети:

- Резултатите от логаритмичната регресия показват (коефициент 0,0005, Фигура 19), че 10% увеличение на честотата на инцидентите е свързано с 0,0005% увеличение на разходите. В индустриален мащаб този ефект може да изглежда незначителен, но от гледна точка на отделна компания въздействието може да бъде значително.

- Що се отнася до очакваната стойност на разходите за един киберинцидент (или IR=1) = 0,0033 (Фигура 19), резултатите също така показват, че ако всички индустриални участници претърпят поне един инцидент (IR = 1), те ще трябва да се справят със средни финансови разходи от 0,0033 млрд. € или 3,3 милиона €.

Заслужава да се отбележи, че посоката на влияние на IREV и IR върху ACC съответства на очакванията – увеличаването на средните разходи на киберинцидент води до отрицателна корекция на индустриалните приходи (IREV), а положителната връзка с броя на киберинцидентите (IR) показва, че увеличаването на IR е съпроводено с нарастване на ACC. Трябва да се отбележи, че въпреки противоположния знак, влиянието на IREV и IR върху

ACC е почти еднакво по големина (коефициент в абсолютна стойност от 0,0005). Подобна близост на степента на отговор се наблюдава и при очакваната стойност на разходите за един киберинцидент, където коефициентът спрямо IREV (0.0032) е приблизително равен на този, свързан с IR (0.0033). Тъй като при изчисляването на тези коефициенти се използват агрегирани данни за всички индустрии и типове киберинциденти, можем да предположим, че получените стойности представляват средни оценки за всички регистрирани инциденти в изследването, независимо от техния мащаб. Това води до формирането на усреднена оценка, която може съществено да се различава от същата метрика на взаимодействие между ACC, IREV и IR, когато става въпрос за инциденти с по-значителни щети. Осъзнаването на последното е пряко свързано както с общото ниво на национална експозиция на киберрискове, така и с времевата динамика на вероятността от киберинциденти, характерна за отделните индустрии.

3. Съществува слаба отрицателна връзка между общия брой служители в индустрията и средните разходи на киберинцидент (ACC) (Фигура 20), т.е. увеличаването на броя на служителите може потенциално да намали средния финансов ефект от кибератака. Резултатите от регресионния анализ показват, че 10% увеличение на броя на заетите в индустрията се очаква да доведе до 0.003% намаление на средните разходи на киберинцидент. Що се отнася до очакваната стойност на разходите за един киберинцидент (IR=1) = 0.0036 (Фигура 20), в парично изражение, индустрии и компании, които оперират в сектор с 100 000 заети, биха понесли средни разходи от 0.0036 млрд. € или 3,6 милиона € на киберинцидент.

Логаритмичен анализ – Уравнение (5)

1. Съществува силна положителна връзка между системния риск (SR) и размера на индустрията по отношение на приходите (IREV) (Фигура 21), т.е. увеличаването на приходните квоти потенциално може да увеличи нивото на системния риск. Резултатът от логаритмичната регресия показва (коефициент 1,8752, Фигура 21), че 1% увеличение на индустриалните приходи може потенциално да увеличи системния риск с 1,875%.. От друга страна, що се отнася до очакваната стойност на разходите за един киберинцидент (или IR=1) = -1,8088 (Фигура 21), резултатите показват, че при осъществяване на всеки единичен киберинцидент, който допринася за системния риск, се постига намаление на

очакваната стойност на разходите за един киберинцидент с 1.80, ако се елиминира ефектът на растежа на приходите върху увеличаването на системния риск, изразен чрез усреднения коефициент 1.8752 (Фигура 21), т.е. ако приходите на индустрията останат постоянни или намалеят. По този начин се постига взаимно компенсиращ ефект – ако изследваните индустрии реализират икономически и финансов растеж, водещ до увеличаване на приходите им и съответно на системния риск (1.8752), то едновременно с това този ефект от растежа се компенсира от намаляване на очакваната стойност на разходите за един киберинцидент (-1.8088) (Фигура 21). Противодействието на този компенсиращ ефект предполага, че увеличаването на системния риск на макроравнище, вследствие на нарастването на приходите на индустрията, обикновено е придружено от увеличаване на честотата на киберинцидентите. Ако такова увеличение на IR не е налице, тогава въздействието на отделните прояви на киберрискове може да не доведе до нарастване на системния риск за изследваните индустрии като цяло.

2. Съществува сравнително слаба отрицателна връзка между системния риск (SR) и честотата на инцидентите (IR) (Фигура 22), т.е. увеличаването на честотата на инцидентите потенциално може да доведе до намаляване на нивата на системния риск. Резултатът от логаритмичната регресия показва (коефициент -0.541, Фигура 22), че 1% увеличение на честотата на инцидентите е свързано с 0.54% намаление на нивата на системния риск. Очакваната стойност на разходите за един киберинцидент (или IR=1) = 1.298 (Фигура 22) показва, че единично проявление на киберриск има потенциала да увеличи очакваната стойност на разходите за отделни киберинциденти, които определят нивото на системния риск, с приблизително 1.30 пункта. С други думи, ако усреднениият коефициент на регресия от -0,541 предполага, че увеличението на IR по-скоро води до намаляване на SR за индустрията като цяло, то на базата на единична проява на киберриск, включен в SR, средната очаквана стойност на разходите за един киберинцидент увеличава киберзагубите, определящи нивото на SR, с 1.30 пункта. Така, докато на макроравнище увеличената честота на инцидентите (IR) не води пряко до увеличаване на системния риск (SR), на микроравнище стойността на единичен инцидент, формиращ SR, може да доведе до по-значителни очаквани загуби. Или казано иначе, на микроравнище нивото на загубите от един киберинцидент може да бъде по-съществено, отколкото общата макрооценка на SR за индустрията би предположила.

Тази посока на въздействие на единичните прояви на киберрискове от IR към приблизително 1.30 пункта увеличение на очакваната стойност на разходите за един киберинцидент, обхванат от системния риск (SR), може също да се разглежда в контекста на комбинирано или верижно проявление.

Както беше обсъдено по-горе по отношение на влиянието на растежа на приходите в изследваните индустрии върху растежа на системния риск (SR), това увеличение на системния риск на ниво индустрия може да се случи само ако е съпътствано от увеличение на IR. Следователно, от една страна, увеличението на IR директно ще предизвика увеличение на SR чрез повишаване на киберщетите от единичен инцидент (коефициент на регресия 1.298) (Фигура 22), но от друга страна, в контекста на бизнес растежа и увеличените приходи, ще доведе до допълнително нарастване на SR, както подсказва коефициентът на логаритмичната регресия (Фигура 21) от 1.8752.

3. Съществува силна положителна връзка между системния риск (SR) и общия брой служители в индустрията (Фигура 23), т.е. увеличаването на общия брой служители, работещи в дадена индустрия, може потенциално да увеличи системния риск:

- Резултатът от логаритмичната регресия показва (коефициент 1.3076, Фигура 23), че увеличение на общия брой служители с 1% е свързано с увеличение на системния риск с 1.30%.
- Очакваната стойност на разходите за един кибер инцидент (или IR=1) = -3.2006 (Фигура 23) предполага, че еднократно възникване на кибер риск има потенциала да намали очакваната стойност на разходите на единични кибер инциденти, определящи нивото на системен риск с 3.20 пункта, ако ефектът от увеличаването на броя на служителите върху увеличението на системния риск се отстрани като заместител на осреднения коефициент на 1.3076 (Фигура 23). Това, което прави впечатление тук е, че осредненият коефициент на въздействие на служителите върху системния риск (1.3076) е приблизително два и половина пъти по-нисък от коефициента на очакваната стойност на разходите за един кибер инцидент (-3.2006). Това предполага, че като цяло, ако увеличаването на служителите води до увеличаване на системния риск, тогава ако броят на служителите остане постоянен, това ще доведе до по-ниски щети от появата на един киберинцидент, отколкото би предвидила осреднената цялостна макрооценка за въздействието на заетостта върху системния риск.

4. Анализът на връзката между индустриалния системен риск (SR) и честотата на индустриалните инциденти (IR) в контекста на изследваните киберрискове (пробиви в сигурността на данните, пробиви в поверителността на данните, атаки със зловреден софтуер и фишинг атаки) показва следното:

Резултатите от регресионното уравнение за фишинг атаките (Фигура 27) показват най-високата стойност на коефициента, отразяващ въздействието на честотата на инцидентите (IR) от този риск върху системния риск (SR) на изследваните индустрии (-1.261). Коефициентите на регресионното уравнение за другите изследвани киберрискове, подредени по големина, показват следната класификация:

- Пробиви в сигурността на данните (-0.797) (Фигура 24);
- Пробиви в поверителността на данните (-0.434) (Фигура 25);
- Атаки със зловреден софтуер (-0.115) (Фигура 26);

Но по отношение на очакваната стойност на разходите за един киберинцидент, най-високият киберрисков показател демонстрират атаките със зловреден софтуер (2.0733) (Фигура 26), следвани от:

- Пробиви в сигурността на данните (1.0564) (Фигура 24);
- Фишинг атаки (0.683) (Фигура 27);
- Пробиви в поверителността на данните (0.5591) (Фигура 25).

Отрицателната корелация между системния риск (SR) и честотата на инцидентите (IR), установена от регресионните уравнения за отделните изследвани киберрискове (Фигури 22 и от 24 до 27), може да се обясни с факта, че киберпрестъпната дейност е пряко свързана с икономическия растеж.

5. В среда на нарастващ БВП системният риск обикновено намалява, но икономическият растеж провокира по-голяма киберпрестъпна активност и стимулира увеличаването на киберпрестъпния риск. От друга страна, при икономически растеж приходите в икономиката се увеличават, а при относително постоянни нива на дълга, коефициентът на системния риск намалява съгласно Уравнение (2), приложено в това изследване: % SRi,t = Debti,t / Revenuej,t

В същото време, при същите условия на икономически растеж и при относително постоянен брой участници в дадена индустрия, увеличаването на честотата на инцидентите поради засилената киберрискова активност води пряко до нарастване на коефициента на

честотата на инцидентите (IR) съгласно Уравнение (1): % IR =Брой инциденти / Брой участници и в индустрията).

Следователно, тъй като отрицателният знак на коефициентите на определяне между SR и IR може да се обясни с логическата последователност: икономическа дейност--> SR (Дълг/Приходи) --> IR --> Кибер разходи (ACC, ACI), те трябва да се анализират главно като абсолютна стойност.

6. Отрицателната регресионна връзка между системния риск (SR) и честотата на инцидентите (IR) може също да се дължи на факта, че в контекста на малки по стойност единични загуби от киберрискове, увеличаването на броя на инцидентите като цяло и на тяхната обща стойност изостава спрямо общото подобрение на икономическата среда. Това води до намаляване на системния риск (SR), който компенсира по-честите на брой инциденти (IR). Тази ситуация на „маскиране“на нарастващия отрицателен потенциал на увеличената честота на киберрисковете (IR), вследствие на икономическия растеж и увеличените приходи на изследваните индустрии, може да доведе до натрупване на разрушителен потенциал. Това натрупване се проявява в поява на единични киберинциденти с по-голям обем на щетите. Например, когато се случват инциденти с обем на щетите, попадащи в най-горните 25% от наблюденията (Четвърти квартил) въз основа на средните стойности на ACC, е възможно увеличаването на IR да доведе до нарастване на SR. Регресионните резултати за SR, свързани с честотата на инцидентите в дадена индустрия (Фигура 22), показват, че очакваната стойност на разходите за един киберинцидент (IR=1) е 1.298, при стойност на осреднения регресионен коефициент за въздействието на IR върху SR от -0.541. Допълнителна подкрепа за тезата, че агрегирани и осреднени резултати (регресионни коефициенти), основани на общия брой инциденти, формиращи IR, могат да доведат до заключения, че въздействието на отделните детерминанти е по-слабо като осреднен коефициент, но в същото време да предизвикват по-силно въздействие при единична проява на индивидуалния фактор, може да бъде намерена и в регресионната връзка между средните киберразходи (ACC) и честотата на инцидентите (IR) (Фигура 19). Стойността на коефициента, показващ осреднения ефект на IR върху ACC, е 0.0005, но стойността на очакваната стойност на разходите за един киберинцидент (IR=1) е приблизително 6 пъти по-голяма, или коефициент от 0.0033.

7. Анализирайки горните резултати в контекста на резултатите от прилагането на теста за причинност на Грейнджър, можем да посочим, че когато разглеждаме резултатите от връзката между SR, REV и IR, измерени само през годините, в които са регистрирани вредоносни киберинциденти от съответния тип, и само за данните от индустриите, които отчитат тези инциденти, можем да направим следните заключения:

- Когато става въпрос за фишинг атаките – причинно-следствената връзка на Грейнджър между SR4, REV4 и IR4 съществува само при първия лаг, което показва сравнително краткотрайно взаимодействие между тестваните променливи. При директно сравнение на резултатите от теста за причинност на Грейнджър за тези променливи в целия набор от тествани лагове и типове киберрискове можем да отбележим, че само при фишинг атаките се наблюдава толкова краткотрайно взаимодействие – само при един лаг (лаг 2). Това ни дава основание да предположим по-съществения ефект на случайността при проявлението на фишинг атаките и тяхното въздействие върху причинно-следствените връзки между SR, REV и IR. Също така можем да забележим влиянието на тази краткосрочна случайност, когато анализираме посоката на влияние между тестваните променливи: при SR4 и REV4 то е двупосочно, докато между SR4 и IR4 причинността е от системния риск към честотата на инцидентите – тоест, интензивността на киберинцидентите, свързани с фишинг атаки, се определя пряко от състоянието на системния риск в дадена индустрия.

- Що се отнася до атаките със зловреден софтуер (Malware), те регистрират най-високия коефициент на регресия за очакваната стойност на разходите за един киберинцидент (IR=1) (Фигура 26). Наблюдаваната причинно-следствена връзка на Грейнджър между SR3, REV3 и IR3 е с по-висока степен на устойчивост във времето в сравнение с фишинг атаките. Относно влиянието на нивото на системния риск върху проявлението на киберинцидентите, свързани с Malware атаки, върху приходите на съответната индустрия, трябва да отбележим, че тази причинно-следствена връзка се проявява при всички изследвани лагове (2, 4, 6 и 8), като посоката на причинност е винаги от SR3 към REV3. Когато разглеждаме причинността между SR3 и IR3, категоричността на горепосочените резултати отслабва – причинността на Грейнджър между системния риск и

честотата на инцидентите се наблюдава само при лагове 2 и 4, а връзката между тях е двупосочна.

- За разлика от най-силното въздействие на IR върху SR по статистическа тежест (-1.261), наблюдавано при фишинг атаките (Фигура 27), можем да разгледаме киберриска, свързан с изтичане на данни (Data breaches). Този риск не само показва второто най-голямо въздействие по сила (-0.797) (Фигура 24), но и значително въздействие на инцидентно ниво (1.0564). Причинно-следствената връзка на Грейнджър между SR, REV и IR за този тип киберинциденти демонстрира най-висока устойчивост сред всички изследвани киберрискове и лагове. Именно при изтичанията на данни се регистрират най-много причинно-следствени връзки на Грейнджър – между SR1 и REV1 (лагове 2, 4, 6 и 8) и между SR1 и IR1 (лагове 2, 4 и 6). С увеличаването на лаговете при тестването на причинността между SR1 и REV1 се наблюдава промяна в посоката на влияние: при лаг 2 тя е от SR1 към REV1, но при останалите лагове връзката става двупосочна. Относно причинността между SR1 и IR1 се наблюдава обратен модел: при лаг 2 връзката е двупосочна, но при лагове 4 и 6 причинността е еднопосочна – от SR1 към IR1. Това показва, че в сравнително дългосрочен план интензивността на проявление на този киберриск, изразена чрез броя на инцидентите (IR), се определя пряко от състоянието на системния риск.

- Комбинирайки резултатите от теста за причинност на Грейнджър между SR и IR, както и тези от регресионните зависимости (Фигури 24 и 27), за двата киберриска с най-голямо въздействие (Фишинг атаки и Изтичане на данни), можем да определим тяхното комбинирано влияние. В краткосрочен план (лаг 2) върху нивото на системния риск (SR) най-съществено въздействие оказва интензивността на проявление (IR) на киберриска Фишинг атаки. Въпреки това, по-устойчивата във времето причинност и детерминираност между SR и IR се проявява чрез въздействието на киберриска Изтичане на данни. Допълнителен аргумент за финансовата значимост на Изтичането на данни като киберриск е фактът, че сред всички изследвани рискове именно този показва най-високите средни щети на инцидент (ACC) – 2.43 млн. евро за цялата изследвана популация и 5.26 млн. евро за най-засегнатите 25% от наблюденията (Четвърти квартил).

Заключение

Вярваме, че анализът, представен в тази дисертация, ще бъде много полезен по различни начини за бъдещата литература, корпорациите, политиците, доставчиците на софтуер за киберсигурност и, разбира се, потребителите в Гърция и Европа. Въпреки значителната липса на данни относно инциденти, свързани с киберрискове и финансовите разходи, успяхме да съберем информация не само от Гърция, но и от европейското вътрешноикономическо пространство.

В заключение, перспективите за финансовото дигитално включване са обещаващи, белязани от значителен напредък и иновации. Интеграцията на нововъзникващи технологии, укрепването на регулаторните рамки, насърчаването на партньорства между публичния и частния сектор, както и фокусът върху изграждането на доверие и приобщаване са ключови стъпки към постигането на тази цел. Въпреки че предизвикателства като рисковете за киберсигурността и дигиталното разделение продължават да съществуват, общата тенденция в Гърция и по света е към по-инклузивна финансова екосистема. Тази еволюция обещава да създаде финансова среда, която е по-достъпна, ефективна и сигурна за всички, особено за недостатъчно обслужваните групи. С развитието на дигиталния пейзаж в Гърция, непрекъснатото сътрудничество, иновациите и ангажиментът към справянето с тези предизвикателства ще бъдат от съществено значение за формирането на по-инклузивно финансово бъдеще.

И не на последно място, включихме процента на загубите по индустрии като функция на годишните приходи. Установихме, че търговският сектор в Гърция изпреварва останалите индустрии по отношение на финансовите загуби и предложихме обоснована методология, която описва всички необходими стъпки за определяне на подходящ годишен бюджет за киберсигурност. Тази методология може да бъде използвана от корпоративните политици в Гърция за намаляване на финансовите разходи, свързани със съвременните киберрискове.

В крайна сметка, нашият емпиричен анализ потвърждава хипотезата, че увеличените инциденти, свързани с киберрискове в Гърция, корелират с по-високи финансови разходи за бизнеса и оказват влияние върху системния индустриален риск, подчертавайки критичната необходимост от цялостни стратегии за киберсигурност.

Научен принос

1. Извършен е анализ и класификация на актуалната кибер рискова експозиция в Гърция в периода 2014 – 2021 г. на база показатели за честота на възникване и степен на реализираните щети. Динамиката на направената рискова класификация е анализирана в контекста на проявление в основните икономически сектори, като по този начин е изготвена актуална оценка на степента на опасност от кибер рисковете специфицирана по отделни стопански сектори. Извършена е класификация на отделните икономическия сектори, както по обща степен на кибер уязвимост, така и по отношение на влиянието на отделните видове изследвани кибер рискове върху тях.

2. Използвайки показателите Average cost per incident, Average cost by industry и Incident rate by industry е направена количествена оценка на влиянието на кибер рисковата експозиция спрямо системния риск като цяло. Също така, разгледано е въздействието на проявлението на кибер рисковете спрямо големите "Too Big to Fail (TBTF)" компаниите, а оттам и на системния риск като цяло. Направен е анализ на динамиката на влиянието на кибер рисковете върху системния риск свързан с тези компании, като ясно е очертано както актуалното състояние, така и времевата динамика отразяваща предприетите мерки от TBTF компаниите по отделните сектори за ограничаване на кибер рисковете.

3. Установено е влиянието на кибер рисковете върху системния риск, като използваната методология позволи да се определи, като общото въздействие на кибер рисковете върху системния риск, така и да се очертае диференциация на установените взаимовръзки определена от големината единичните кибер инциденти.

Публикации

1. Koutsari, M. (2022). Internet financial risk managment. *Entrepreneurship*, 10 (2), 70-79 DOI: *10.37708/ep.swu.v10i2.7*

2. Koutsari, M. (2023). The financial impact of cyber risk: empirical evidence from Greece and the European economical zone. *Електронно научно списание – Финанси (Electronic scientific journal - Finance)*, 69-82. https://espisanie.financebg.com/wp-content/uploads/2024/02/finance-br-1-2023.pdf

3. Koutsari, M. (2024). Exploring bivariate correlations in cyber risk on an industrial level: empirical evidence from Greece and the European economic area. *Entrepreneurship*, 12 (1), 8 - 20 https://doi.org/10.37708/ep.swu.v12i1.2

SOUTH-WEST UNIVERSITY
"NEOFIT RILSKI"

Faculty of Economics

Department of Finance and Accounting

PhD PROGRAM:

FINANCE, MONEY CIRCULATION, CREDIT AND INSURANCE

ABSTRACT OF PHD THESIS

For acquiring of educational and scientific degree "Doctor",

Area of high education: 2. Social, Economic and Legal Sciences, Professional field: 3.8 "Economics"

"The financial costs of cyber risk in the business and public sector in Greece"

PhD Candidate: Maria Stefanos Koutsari

Scientific Supervisor: Assoc. Prof. Vladimir Tsenkov, PhD

Blagoevgrad, 2025

The dissertation work was discussed and proposed for defense at a meeting of the Department of Finance and Accounting at the Faculty of Economics of the South-west University "Neofit Rilski" - Blagoevgrad on …….. 2025.

In its content, the dissertation includes an introduction, three chaptes, conclusions, one appendix and literature review.

The text is in a volume of 153 pages, which includes 22 tables, 30 figures. The cited literature covers 111 titles.

The defense of the dissertation will be held on …… year from … h. in Hall ……, 8 Corpus of SWU "Neofit Rilski" - Blagoevgrad, before a scientific jury.

The defense materials are available at the office of the Finance and Accounting Department on the first floor, 8 Building of South - West University "Neofit Rilski" – Blagoevgrad

CONTENT

Introduction

Relevance of the Topic

Analyzing the implications of cyber-attacks has become more and more significant the past recent years, particularly as digitalization continues to shape both the public and private sectors globally. In Greece, the importance of understanding and mitigating cyber risk is greater due to the growing dependence of various industries and the increasing reliance on digital infrastructure. Cyber incidents, ranging from data breaches to sophisticated phishing attacks, have the potential to cause substantial financial damage, disrupt essential services, and damage public trust. This dissertation's relevance lies in its focus on quantifying the financial impact of cyber risk within Greece's business and public sectors, an area that has not been extensively studied despite its critical importance. Understanding these costs is crucial for developing effective counter cybersecurity strategies, guiding policy decisions, and ensuring the resilience of Greece's economy in the face of growing cyber threats.

Subject, Goals, and Main Tasks of the Research

The primary objective of this research is to quantify the financial costs associated with cyber risk in both private and public sectors in Greece, with an emphasis on understanding how these

costs affect the broader economy. The dissertation aims to achieve several specific goals:

1. **Identification of Financial Costs:** To identify and categorize the various types of financial costs (direct, indirect, and opportunity costs) that organizations incur as a result of cyber incidents.
2. **Correlation Analysis:** To investigate the correlation between the frequency of cyber incidents and the financial costs borne by different industries, thereby determining the impact of cyber risk on systemic industrial risk.
3. **Impact Assessment:** To assess the overall financial impact of cyber incidents on the Greek economy, providing insights into how these risks influence the competitiveness and sustainability of key industries.
4. **Predictive Modeling:** To develop a predictive model that can estimate the financial costs of cyber incidents based on industry-specific variables such as revenue, incident rate, and the number of employees.
5. **Policy Recommendations:** To provide actionable recommendations for policymakers and business leaders on how to enhance cybersecurity measures and mitigate financial losses due to cyber threats.

Research Methods

The research methodology employed in this dissertation is empirical and quantitative in nature, relying on a robust dataset derived from various sources across Greece and the European Union. The primary methods include:

1. **Data Collection:** Data was gathered from credible sources such as the European Union Agency for Cybersecurity (ENISA), the Hellenic Computer Security Incident Response Team (CSIRT), and IBM's Cost of Data Breach annual reports. This data includes information on cyber incidents, financial costs, and industry-specific variables.
2. **Incident Rate Calculation:** The incident rate (IR) was calculated as a measure of the frequency of cyber incidents relative to the number of players in each industry. This metric was used to measure the exposure of different sectors to cyber threats.
3. **Logarithmic Regression Analysis:** A logarithmic regression model was employed to analyze the relationship between financial costs and various industry-specific factors, including revenue, incident rate, and employee numbers. This model allows for the examination of exponential relationships that may not be captured by linear regression.

4. **Systemic Risk Analysis:** Systemic risk was assessed by examining the debt-to-revenue ratio of key industries, incorporating cyber incidents as a factor influencing this risk. This analysis helps to understand the broader economic implications of cyber risk.
5. **Bivariate Analysis:** Correlation tests, including Pearson and Kendall's tau, were used to explore the relationships between different variables, such as incident rates, financial costs, and systemic risk.

Object of the Study

The object of the study encompasses the financial impact of cyber risk on key industries within Greece's private and public sectors. Specifically, the research focuses on seven main industries: energy, communications, healthcare, retail, banking and finance, digital infrastructure, and government services. These industries were chosen due to their critical role in Greece's economy and their varying levels of exposure to cyber threats. The study also considers the broader European context, using data from similar industries in countries like Germany, Italy, France, and the UK to draw comparisons and enhance the robustness of the findings.

Structure of the Study

The dissertation is structured into several key chapters, each addressing different aspects of the research:

1. **Introduction:** Provides an overview of the research topic, its relevance, and the primary objectives of the study.
2. **Literature Review:** Reviews existing literature on cyber risk, financial costs, and systemic risk, highlighting gaps that the current research aims to fill.
3. **Data Selection and Methodology:** Details the data sources, the process of data collection, and the empirical methods used in the analysis, including the calculation of incident rates and the setup of the regression models.
4. **Empirical Analysis:** Presents the results of the logarithmic regression analysis, bivariate tests, and systemic risk assessment, discussing the implications of these findings.
5. **Discussion and Conclusion:** Summarizes the key findings, discusses their relevance to both the academic community and industry decision makers, and provides policy recommendations.
6. **Appendices:** Includes detailed tables, graphs, and additional data that support the empirical analysis.

Chapter 1: The cyber risk concept and general characteristics

In recent years the increasing development of new technologies and use of information systems that are mainly attributed to Internet have inundated our lives. The use of the Internet is considered as a necessity and its value for any business in private and public sector regardless of its type, size or geographical placement is unquestionable.

The Internet has its roots in ARPANET (Advanced Research Projects Agency Network) and constitutes its evolution of ARPA network that began to grow experimentally in the late 1960s in the United States. The pioneers of internet Larry Roberts and J.C.R. Licklider in an effort of further researching on development of the Pentagon programs ARPA (Advanced Research Project Agency), started experimenting with remote computers interconnection with each other and initially created the ARPANET network. At its first phase the program aimed to experiment with a new technology known as packet switching which would allow many users transmit and share data separated into packets through the same line. In 1973, scientists conducted a new experimental research which concluded in a new technique known as Internet Protocol (IP) according to which different networks that use and share the same IP protocol can be connected and communicate form one and only network. In

1983, ARPANET is conclusively implemented for academically and research use being adopted by universities and organizations. In 1990, is renamed into INTERNET.

In modern reality, the co-occurrence of the Internet, information systems and human factor is commonly known as Cyberspace that constitutes a virtual environment with global impact. Cyber space and ICTs facilitates communication, collaboration, exchange of ideas, instant access to a great amount of information and by extension the fundamental transformation and development of the global economy. Social networking, e-commerce, cloud computing, automated processes, new technologies and e-services are illustrative examples that prevail in every day life of an individual and the achievement of business goals of a company. Additionally, cyberspace and the aforementioned technologies provide not only improvements in sectors such as healthcare, education but also to financial sectors productivity and profitability.

Information technology (IT) has become a critical component of well-functioning economies, underpinning economic growth over the past decades. Organizations in both the public and private sector are becoming more and more interconnected and reliant on IT products and services since concerns about cyber risk have intensified as the economy and financial system is getting

digitalized. In recent years, the rise of targeted cyber-attacks against governments and businesses underscores the need to improve defense. Organizations need to address cyber incidents, since attackers diligently investigate their targets, analyze their weaknesses, and use this information to tailor their attacks. In the wake of recent high-profile cyber-attacks such as the WannaCry incident in May 2017, public awareness of these threats is on the rise.

In Greece, in accordance with a recent research conducted by Check Point Software Technologies[1] an organization is attacked an average of 479 times a week only the first half of the year. Compared to May 2020, there has been a 52% increase in the number of cyber-attacks in the country. It goes without saying that there are many factors that contribute to appearance of cyber risk at financial institutions, including the incorporation and use of quickly evolving technology, the increasing interdependence relation between the financial system and information technology infrastructure the growing sophistication of cyber criminals, and the intrinsic nature of financial institutions' business and services. Having taken into account the increase of sophistication of cyber risk incidents, supervisors and regulators have started taking steps

[1] "Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally".

against cyber risk at financial institutions, including enhancing resiliency capabilities and implementing plans for effective response to and recovery from cyber-attacks.

Recent years have seen the financial sector embrace blockchain technology and cryptocurrencies. These innovations offer novel, decentralized, transparent, and secure transaction methods. Blockchain's application in financial services could further democratize financial system access, particularly for cross-border transactions and remittances (www.searchmyexpert.com, 2024). Moreover, the innovative use of artificial intelligence (AI) and machine learning (ML) in financial services is transforming the industry. AI and ML aid in creating personalized financial products, enhancing risk assessment, detecting fraud, and improving customer service, making financial services more accessible, efficient, and secure, thereby contributing significantly to financial inclusion (World Bank, 2022).

In recent years, in the field of finance we can mention that the definition of risk is not clear but can be formulated as the probability that the final returns (profit & loss) will differ from the expected.

In general risk expresses uncertainty about future situations, developments, whose results could affect their achievement of short-term and long-term goals of the company. We can identify risk

as a measure of uncertainty which indicates uncertainty about the outcome of the results which may be divergent than the expected in a positive or a negative way. Quantification of uncertainty is measured using statistical quantities such as standard deviation. In other words, we try to create a measurement of it probability that the realized performance will differ from the expected one.

Greece has an updated National Cyber Security Strategy, basen on 5 general axes, 15 specific targets and more than 50 actions.

It is crucial for organizations to take measures to better protect themselves from cyber attacks. In particular, organizations need to establish enterprise wide risk management programs and cyber security under the supervision of IT executives department, chief executive officer or a chief risk officer reporting to the CEO.

Regardless of the role of public and private sector take on in governance against cyber security threats there are other factors that can advocate this important endeavour.Every single individual as a unit has the responsibility to protect his own system and data and by extension the whole community. Is not enough for Governments to provide awareness to citizens if they are not willing to apply the knowledge they have received. In other words, in accordance with the correct instructions individuals have to take technical security measures, behavioral security measures and report cyber incidents.

Table1: Private and Public Sector and their cyber governance performances

Private sector	1. Technical Security 2. Security policies 3. Awareness raising (e-mails, websites) 4. Audits and assessments 5. Cyber crisis plans 6. Support law enforcement agencies 7. Promote international norms 8. Confrontation of terrorism acts and misinformation
Government	1. Laws 2. Performing periodic cyber security status reports 3. Cyber security compliance exercises and audits 4. Research and development 5. Working groups 6. Support employees, citizens and SME's 7. Technical security 8. Awareness raising (trainings)

Source: Author's work (2023)

First of all there are simple technical and behavioral prevention measures that we can take such as locking the screen when the computer is inactivate, encrypt sensitive information before mailing it to external recipients, share sensitive information only with authorized entities and verify recipient e-mail addresses before sending e-mails. (Reveron D.S. & Savage J.E. 2020).

Moreover the are many qualified educational institutions that can provide public and private sector's employees and every willing individual with digital knowledge and skills on everything concerning the protection of their digital world and especially how to prevent cyber threats.

Chapter 2: Exploring digital financial services in cybersecurity strategies in Greece

Cybersecurity in Greece encompasses a broad range of activities and agencies aimed at protecting both the private and public sectors from cyber threats. One year following the EU's introduction of its initial Cybersecurity Strategy, the Cyber Crime Division was established within the Hellenic Police (P.D. 178/2014). This division aims to prevent, investigate, and halt crimes and antisocial behaviour occurring online or via other electronic platforms. Concurrently, following the original NIS Directive, the National Cyber Security Authority (NCSA) was formed (P.D. 82/2017) and designated as the country's National Competent Authority for cybersecurity (N. 4577/2018). Additionally, in 2019, Greece replaced its 2016 Ministry of Digital Policy, Communication and Media with the updated Ministry of Digital Governance (P.D. 81/2019), which focuses on accelerating the digital transformation of the public sector, reducing bureaucratic hurdles, aligning digital policies with e-governance and public services, and enhancing interoperability across all levels. This shift, combined with the Covid-19 pandemic, led to an increased reliance on the internet for various activities, promoting digital literacy and the modernization of services in Greek society. Moreover, Greece actively participates in international cyber defence collaborations,

including NATO's cyber defence initiatives and the European Union's cybersecurity programs.

The National Intelligence Service (EYP) also plays a pivotal role, focusing on protecting national security from espionage, terrorism, and cybercrimes, operating as the national CERT (NCERT-GR, RFC2350). Despite not being accredited by the TI, GRNET-CERT, established in 2003 and hosted by the National Infrastructures for Research and Technology, is the only accredited CERT. Recently, EYP gained notoriety due to its alleged use of Predator spyware to monitor mobile phones of politicians, journalists, and business leaders (politico.eu). Although this incident has cyber elements, it remains a domestic issue under ongoing investigation and is thus not the focus of this thesis. Nevertheless, this situation influenced the recent addition to the Greek constitution with Law N. 5002/2022, which addresses the declassification of communications, enhancement of EYP's operations, protection of communication privacy against surveillance software, strengthening national cyber security, and safeguarding citizens' data privacy (Sotiropoulou, 2023).

On a practical level, Athens was the venue for one of the initial five preparatory workshops for the inaugural Pan-European Cyber Security Exercise on Critical Information Infrastructure Protection (CIIP) named "Cyber Europe 2010" in September 2010.

This event, supported by ENISA and the Joint Research Centre, was designed to foster collaboration among European nations to address expansive cyber threats. Beyond this, Greece also leads two PESCO Projects related to cybersecurity: the Cyber Threats and Incident Response Information Sharing Platform, and the Deployable Special Operations Forces (SOF) Tactical Command and Control (C2) Command Post (CP) for Small Joint Operations (SJO) – known as SOCC for SJO. In 2022, the increase in cyber-attacks on critical infrastructure and those associated with the conflict in Ukraine introduced new strategies for managing cyber risks. These include the development of an independent operational system named Thorax, which will integrate into the Third Division of the Hellenic National Defence General Staff. Thorax aims to leverage big data, artificial intelligence, and various algorithms to manage the vast daily information influx to detect threats and automate responses. Additionally, the Technical Assistance and Information Exchange Instrument of the European Commission, in collaboration with the Greek Ministries of Foreign Affairs and Digital Governance, held a workshop in Thessaloniki in June 2022 on "The role of the EU's Cyber Ecosystem in the global cyber security stability" (ENISA, 2022a). Initiated by the European Security and Defence College and ENISA, with participation from Western Balkans partners, this conference facilitated valuable exchanges among regional experts

and policymakers, enhancing trust and resilience. This aligns with two strategic EU and Greek goals: cybersecurity and the integration of the Western Balkans into these frameworks. Furthermore, the International Fair of Thessaloniki in 2022 welcomed ENISA for the first time to support the European Year of Youth 2022 activities, aiming to foster a more inclusive digital future and heighten awareness of cybersecurity skills. These efforts included the establishment of an incident notification platform, developed in partnership with a prominent international entity known as CSIRT (Computer Security Incident Response Team). CSIRT is actually a sub-branch of military intelligence and thus responsible for developing regulations, certification systems and contribute to the prevention and response to cyberattacks across the country.

This enhanced cybersecurity framework played a key role in Greece achieving the 7th rank on the National Cyber Security Index (NCSI), comparing its cyber security measures with other nations globally from 2016 to 2023. NCSI Index. By adhering to a systematic development strategy, Greece advanced significantly to secure the top position among 160 countries in 2019. This index evaluates the measures implemented by various relevant Greek authorities, such as the Cyber Defence Unit, the Cybercrime Unit, the National CERT, the Hellenic Authority for Communication Security, and the Hellenic Data Protection Authority, among others.

The Greek government's approach to cybersecurity also includes educational initiatives for citizens, and the banking sector's policies on cybersecurity education, along with the role of Artificial Intelligence (AI) in enhancing cybersecurity. The Greek government has recognized the importance of cybersecurity and has been actively working to enhance the nation's cyber defence capabilities. This includes the establishment of a national cybersecurity strategy that outlines the government's vision and action plan to improve cybersecurity across all sectors. The strategy emphasizes the protection of critical national infrastructure, the enhancement of public and private sector collaboration, and the alignment with international cybersecurity standards and best practices. To educate citizens on cybersecurity, the Greek government, often in collaboration with the European Union, has launched various awareness campaigns. These initiatives aim to increase public understanding of cyber risks and promote safe online behaviors. Educational programs and resources, such as online safety tips, workshops, and seminars, are made available to the public to help individuals protect themselves against cyber threats (Boiko, Vasylenko and Kukharenko, 2019).

The business landscape in Greece has been responsive to the growing cyber threats. With increasing cyber-attacks targeting businesses—ranging from SMEs to large enterprises—Greek

companies are investing more in cybersecurity solutions. This investment goes beyond mere compliance with the EU's General Data Protection Regulation (GDPR) and moves towards a more holistic approach to cyber resilience. This includes adopting advanced cybersecurity technologies, training employees, and implementing robust incident response strategies. Since its inception, the Greek NCSA has implemented various laws and regulations that have shaped the Greek cybersecurity landscape on a business level. These initiatives serve as exemplary models for other nations, providing a solid foundation for the challenging subsequent phases of execution and enforcement. Among the outcomes is a maturity assessment framework that enables organizations to progressively enhance their cybersecurity maturity. This process involves stabilizing at the current level before advancing to higher levels through ongoing organizational improvements. This is achieved by utilizing both quantitative and qualitative data for decision-making. For example, at maturity level 2, organizations transition from an "ad hoc" approach to a "managed" level by establishing robust security controls and processes. Additionally, this framework could be adopted at a European level to guide the prioritization of mitigation plans and cybersecurity funding. In scenarios where a full security review is not feasible, conducting effective cybersecurity risk assessments

and implementing mitigations in large, critical infrastructures could serve as a provisional approach (Maglaras et al., 2020)

Since the mid-1990s, Greek banks have been working to fortify their market position and enhance their operational efficiency. This effort has been largely motivated by shifts within the European banking sector and investment prospects in Southeastern Europe. Nevertheless, Greece's banking sector is currently experiencing extraordinary challenges, including issues related to liquidity and profitability. These challenges are primarily due to the fiscal and macroeconomic decline in Greece, as well as the numerous downgrades of the country's sovereign credit rating. However, in recent years, cyber-attacks have become a significant and growing concern. The frequency of cyber-attacks on financial institutions in Greece remains uncertain, as the four major systemic banks do not publish official reports or records. It is believed that tens of thousands of incidents occur annually, with e-banking services being the primary focus of these cyber attackers due to the fact that phishing and data breaches can result in significant financial losses for the institutions while generating substantial profits for the attackers.

Since Greece’s banking system in completely incorporated to the European Central Bank’s regulatory framework, Greek institutions adhere to the so-called Payment Service Directives

(PSD) that are issued by the ECB on an annual basis. The objective of these directives is to build a protective shield over payments services and financial transactions across the European Economic Area. Recently, the revised PSD2 legislation has adopted API (Application Programming Interface) technology, allowing banks to mitigate security risks in payment transactions through an API architectural model. This model incorporates additional fraud protection and authentication layers because it enables the integration of security features such as access control and threat detection directly into data-sharing services. This proactive approach allows for enhanced security measures. Furthermore, with a consensus on a unified technical specification, all systems across the EU could potentially converge on a single or a limited number of API technical standards (Gounari et al., 2024). Last but not least, banks in Greece also play a significant role in educating citizens about cybersecurity. Recognizing that financial services are prime targets for cyberattacks, Greek banking institutions have implemented measures to raise awareness among their customers (Boiko, Vasylenko and Kukharenko, 2019). For instance, the National Bank of Greece, one of the country's leading banking institutions, regularly distributes cybersecurity awareness flyers to educate both its corporate and retail clients. These include providing information on how to recognize phishing emails, secure online

banking practices, and the importance of protecting personal and financial information. Many banks offer resources on their websites and conduct awareness campaigns to inform customers about the latest cyber threats and how to avoid them (nbg.gr).

Following a recent similar mandate from the Association of Business and Industry (BSE), each company is required to appoint a Chief Information Security Officer (CISO) and establish a team responsible for developing and overseeing the cybersecurity strategy. If the scale of a business does not warrant such roles, it would be beneficial to coordinate efforts to ensure safe digital operations and provide training for those involved. According to the same educational directive, cybersecurity responsibilities extend beyond the IT department; all employees must be vigilant, as the majority of breaches occur through phishing emails or spam that any staff member might inadvertently open. Therefore, it's vital to consistently conduct training programs and informational campaigns (covering best practices, case studies, etc.) to prepare staff to effectively respond to digital threats.

Artificial Intelligence (AI) has emerged as a powerful tool in the fight against cyber threats, offering new possibilities for enhancing cybersecurity in Greece and beyond. AI can analyse vast amounts of data to identify patterns and detect anomalies that may indicate a cyberattack. This allows for the early detection of threats

and swift response to potential security breaches. AI-driven security systems can automate the monitoring of network traffic, identify vulnerabilities, and even predict future attack vectors based on current trends. Furthermore, AI can help address the cybersecurity skills gap by automating routine tasks, allowing human experts to focus on more complex challenges. However, it is also important to note that as AI technology advances, cybercriminals may also utilize AI for malicious purposes, necessitating continuous innovation and adaptation in cybersecurity strategies (Citictel-cpc.com, 2023).

Based on the European Defense Agency (EDA) Greece is actively investing in artificial intelligence (AI) technologies for military purposes and is a participant in several European defense initiatives. Greek defense industries, including the Hellenic Aerospace Industry, Intracom Defense Electronics, and EFASSYS, are key players in developing AI-driven systems, specializing in electronics, communications, and unmanned systems. Greece is involved in multiple European-funded AI programs aimed at enhancing military capabilities and operations. These include the LOTUS program for developing low observable tactical unmanned air systems, the SMOTANET program focusing on tactical network devices, and the INDY project which studies energy storage and distribution for military units. Additional projects include COMMANDS for manned-unmanned systems operations, the

European Patrol Corvette initiative, and ACHILLES, which aims to advance unmanned vehicle swarms for defense. Other notable initiatives include AVICOM for improving communications in disaster scenarios and Agile 4.0, a project enhancing digital innovation and agile manufacturing in the industry sector (eda.europa.eu). Amid geopolitical challenges posed by regional dynamics and Turkey, Greece aims to bolster its defense capabilities through AI, which can provide strategic advantages over numerical superiority. For Greece to fully leverage AI in defense, it must overcome internal limitations and embrace a broader vision that includes cultural heritage, educational reform, biodiversity conservation, and strengthened alliances within the Mediterranean and beyond. This comprehensive approach is essential for improving Greece's geopolitical stance and fostering a productive and innovative national ethos.

Chapter 3: Analysis of the financial costs of cyber risk in the business and public sector in Greece

In general, it is difficult to quantify the exact financial costs of cyber risk, as these costs can vary widely depending on the size and type of business or organization, as well as the specific nature and impact of the cyber incident. Nevertheless, we can still estimate the average costs per cyber incident by using external reliable financial reports and utilize them for the purposes of this dissertation. Those monetary direct or indirect average costs will allow us to test the correlation effect as well as the impact magnitude of them on the systemic risk component of the respective business industry on the one side and the generic relationship between costs and cyber incident types on the other. Therefore, our research was conducted based on the hypothesis that: Cyber risks, in general, in the Greek economy pose a real measurable financial danger, but are not a factor in increasing systemic risk. The likelihood of individual high-damage cyber risk events is significant and is associated not only with the occurrence of greater financial damage and costs to companies, but also the likelihood of impacting systemic risk as a whole.

At the end, we will make a stab at answering a vital question that literally interests policy makers regardless operating in the private or public sector; how much of a problem are cyber incidents?

In other words, we will try to measure the losses driven by cyber risk as a percentage of the revenue of the industry we focus on and hence provide useful insights to decision makers regarding the cyber risk investments they should undertake in order to increase organization's cyber security and mitigate the consequences of cyber-attacks.

Summary of the empirical results

Descriptive analysis of cyber incidents

1. The classification of cyber risks based on the frequency of their occurrence as a percentage of the total number of cyber incidents shows that Data breach reports represent the majority (32%) among the 171 observations throughout the years 2014-2021 in all industries, followed by malware attacks (25%), phishing (23%) and finally privacy breaches (20%).

2. Data breach reports have seen a three-fold increase from just over 15000 in 2017 to over 45000 in 2021, analogously, similar to data breach notion, privacy violations have sharply increased in this time space from just few thousand cases in 2014 to over 40000 incidents in 2021.

3. On the contrary, malware and phishing attacks during 2014-2021 period show relativly constant dynamic when it comes to absolute number of incident records.

4. When it comes to the absolute number of observations related to all types of cyber incidents by sector and by the percentage of incidents, we can point out that the retail sector stands out from the rest in terms of size (more participants and higher revenues), which is why most of our observations and subsequently incident records come from this particular sector - 32% of all observations.

5. Government services, in terms of the absolute number of observations related to all types of cyber events experience relatively a lot of cyber incidents - 27% of all observations.

6. In terms of absolute number of incidents related to all types of cyber events, incidents in energy, healthcare, and digital infrastructure are the lowest in number.

7. Regarding the indicator "Incident rate by sector" - the sectors of communications, energy and digital infrastructure absorb a larger cyber risk impact due to a higher incident rate.

8. When it comes to cyber risks of data breaches and malicious software attacks the banking and digital infrastructure sectors exhibit high volatility in the period 2014-2021concerning the average cost per incident. On the other hand, both government services and retail market sector undergo no significant volatile changes in the studied period regarding cyber event average costs

per incident; a data breach in the government sector can yield an average cost of 3 Mio. €, while a malware attack in the retail sector can yield less than 1 Mio. € in financial and corporate losses.

Descriptive statistics

1. A data breach is considered to be the most serious incident among all types, regardless the scope of business the mean value of the average financial costs caused by a data breach is €2.43 million. The data breaches yield similar financial and corporate costs across all industries of interest.

2. Based on the average cost per incident indicator (ACC), the ranking of cyber risk types is as follows: data breach with €2.43 million per incident; privacy breaches with €2.34 million per incident; phishing events with €2 million per incident; malicious software attack with €1.80 million per incident.

3. Based on the descriptive statistics for the different types of cyber incidents and the division of the observed cases into separate quartiles according to the amount of damage suffered, we can point out that the average values of the top 25% of observations (Quartile 4) show twice as large an average cost per incident compared to those for the whole group of observations: data breaches € 5.26m for Q4 vs € 2.43m for the whole population; privacy breaches € 5.01 million for Q4 vs. €2.34 million for the whole population; software attacks € 4.93 million for Q4 vs. € 1.80

million for the aggregate; phishing events € 4.90 million for Q4 vs € 2.00 million for the aggregate;

This data shows that while the average cost per incident for all industries is relatively low, in 25% of cases (Q4) losses from cyber incidents can be many times greater than the average expectation overall. This raises not only the question of the importance of cyber security in general, but also the question of the significant possibility that in 25% of incidents the amount of damage from the realisation of different types of cyber risks could be double the industry average expectation. This issue is particularly significant for large corporations where, due to the larger scale, we can expect to realise greater damage from the occurrence of any of the cyber risks. The issue takes on added significance given the fact the highest average values in Q4 are recorded specifically for cyber events with the highest record of recorded occurrences - data breaches (32%) (Q4 - €5.26 mil.) malware attacks (25%) (Q4 - €4.93 mil.), phishing (23%)(Q4 - €4.90 mil.) and finally privacy breaches (20%) (Q4 - €5.01 mil.).

If in 25% of cases (quartile Q4) the average cost per incident exceeds approximately twice this benchmark typical in the remaining 75% of cases, the question arises as to which sectors companies are most at risk of these higher losses. Considering the data presented for the "Incident rate by industry" indicator (Figure

14), we could assume that it is potentially companies mainly in the Digital Infrastructure, Communications, Energy and Banking sectors. Considering the other indicator "Average cost by industry" we could assume that the main threat comes from the Banking and Government sectors. While their incident rate is lower compared to the IR of the Digital Infrastructure, Communications, Energy sectors, the average cost by industry for the Government and Banking sectors is roughly twice as high: a) banking 44.93(million euros) and government (public) sector 39.58(million euros), vs. b) energy 22.34(million euros) and digital 19.84(million euros).

The communications sector can be seen as similar to the government and banking sectors - there is a very similar Incident rate (approximately 0.22 vs. 0.21 for the banking and public sectors) and a relatively high average cost of €29.29 million.

The retail sector although having the highest average cost has approximately five times lower "Incident rate by industry".

4. Regarding the indicator “Average cost by industry” (ACI), the data show the following classification: Retail trade sectors EUR 16 985,46 million; health 114,18 million euro; banking 44,93 million euro; government (public) sector EUR 39.58 million; communications EUR 29.29 million; energy EUR 22.34 million; digital technologies EUR 19.84 million;

The retail sector, due to its nature and scale, encompasses the activities of many companies, both large multinationals and small family-owned businesses, so it is understandable that this sector records the highest average costs associated with cyber-attacks. The large scale of the sector determined by the large number of operating companies predetermines also the highest total incident volumes and thus the highest total financial costs due to its size. It should be noted that although due to its size the retail sector shows the highest value of the indicator 'Average cost by industry', this sector is also characterised by the lowest value of the indicator 'Incident rate by industry'. On the other hand, the public sector and the banking sector register a balance of the indicators "Average cost by industry" and „Incident rate by industry" (IR) showing average levels for both indicators leading to the conclusion of the presence of risk exposure implying a relatively high IR accompanied by significant Average costs associated with the implementation of cyber risks. The remaining industries show either high IR accompanied by low Average cost by industry and vice versa.

Digital infrastructure companies in Greece experience the lowest financial costs overall compared to the rest industries. Perhaps, this happens because those companies do not engage with sensitive consumer data, rather applying new tech in order to

maintain and improve existing digital networks for the sake of the economy as a whole.

5. When it comes to considering the impact of cyber risks in the context of the impact they can have on large Too Big to Fail (TBTF) companies and hence on systemic risk in general, it should be noted that over the period 2014-2021 TBTF private sector companies, and in particular those in the banking sector, show a steady reduction in risk exposure. On the contrary, the public sector not only maintains a constant risk exposure for the overall study period, but also registers the high values of the indicator "Average cost per incident" marking a high possibility for successful and large-scale cyber-attacks to have their damage in terms of size fall into the upper quartile (Q4) of damaging incidents characterized by a large average cost per incident with the result that single cyber incidents have a significant impact on systemic risk as a whole.

6. The presence of a distinct possibility of cyber risk events leading to the formation of more significant damages is indicated by the descriptive statistics of indicators Incident rates and Industrial revenues across all industries (Table 11). The observed distributions of these two indicators register the presence of "fat tails" marking the possibility of occurrence of cyber risk events with large magnitude of realized damages. While the mean and median values indicate that at least 15% of the industrial players experiences

one or multiple incidents per year. The above facts add to the risk characterization of the Greek public sector insofar as they not only indicate the statistical possibility of cyber risk events occurring, in general, but also, more proportionally, the possibility of damages larger in value than single such events. This, relative to the fact that the public sector also demonstrates higher values of the "Average cost by industry" indicator for a single cyber risk incident, again highlights the issue of increased cyber risk exposure of the Greek public sector.

Bivariate analysis results

1. There is a the positive statistically significant correlation between “Average costs per incident - ACI” (scale variable) and “Incident rates per industry per year of interest – IR” (ordinal variable). The correlation coefficient indicates a low to moderate positive relationship between the two variables (0.23).

2. The measuring of the relationship between “Incident rates per industry – IR” and the “Systemic risk – SR” shown the presence of a negative correlation between the two variables of -0.20, which is statistically significant at the 0.01 level (0.007).

3. A negative correlation is also observed between the indicators for "Incident rates" and "Industrial revenue" - the correlation coefficient is found to be negative (-0.48) at a critical significance level of 0.01. The results show that whenever the

volume of cyber incidents increases within an industry, the total industry revenue decreases. This inverse relationship is very pronounced, as for every unit increase in cyber incidents there is a 0.5 unit decrease in revenue.

4. The correlation testing of the relationship between "Incident type" and "Average costs" from one side and "Systemic risk" on the other, shows: that when "Average costs per incident" is considered as a dependent variable, there's a very weak but positive correlation with the "Incident type" - (0.165); a weak but statistically significant positive correlation between "Systemic risk" and "Incident type"(0,176).

Logarithmic analysis – Equation (4)

The regression results of equation (4) using data from all industries studied show:

1. There's a weak negative relationship between Industrial revenue (IREV) and Average costs per cyber incident (ACC), i.e., an increase in revenue quotas could potentially decrease the financial impact (on average) of a cyber event: The logarithmic regression outcome suggests (coefficient of -0,0005, Figure 18) that a 10% increase in industrial revenues is estimated to result in a 0.005% decrease in the average costs per cyber-attack incident. On the other hand, when it comes to the expected value cost for one cyber incident (or IR=1) = 0,0032 (Figure 18), then the corporations

that belong to a 1 billion € industry, would experience 0.0032 Bn. € or 3.2 Mio. € in average costs per cyber event.

2. There's a weak positive relationship between Incident rate (IR) and Average costs per cyber event (ACC), i.e., an increase in the incident rates could potentially increase the financial impact (on average) of a cyber event:

- The logarithmic regression outcome suggests (coefficient of 0,0005, Figure 19) that a 10% increase in the incident rate is associated with a 0.0005% increase in costs. Once again, this impact might appear to be insignificant in industrial terms, however, from a firm's point of view this impact might be huge.

- When it comes to the expected value cost for one cyber incident (or IR=1) = 0,0033 (Figure 19), the result also indicates that even if all industrial players experienced at least one incident (IR = 1), they would have to tackle 0.0033 Bn. € or 3.3 Mio. € in average financial costs.

It is noteworthy that the directionality of the impact on ACC from IREV and IR has the expected direction and sign of influence - an increase in the average cost per cyber incident leads to a negative industry revenue adjustment (IREV), and the positive relationship with the number of cyber incidents (IR) determines that an increase in IR is accompanied by an increase in ACC. It should be noted that, even with opposite sign, the impact of IREV and IR

on ACC is of almost the same magnitude (coefficient in absolute value of 0.0005). We see a similar closeness of response rates when it comes to the expected value cost for one cyber incident. The response rate of AAC relative to IREV (0.0032) is approximately the same value as that associated with IR (0.0033). Since aggregated data for all industries and types of cyber incidents are used to calculate these coefficients, we can assume that the resulting coefficients are averaged over all incidents recorded and used in the study, regardless of size. This leads to the formation of an averaged estimate that can significantly differ from the same interaction metric between ACC, IREV and IR when it comes to more significant in terms of the size of damage from a single incident. The realization of the latter is directly related to both the overall level of national cyber risk exposure and the temporal dynamics of the probability of cyber incidents characteristic of individual industries.

3. There's a weak negative relationship between the Total number of industry's employees and ACC (Figure 20), i.e., an increase in employee quotas could potentially decrease the financial impact (on average) of a cyber event: The regression outcome indicates that a 10% increase in the industry's headcount is estimated to result in a 0.003% decrease in the average costs per cyber-attack incident. When it comes to the expected value cost for

one cyber incident (or IR=1) = 0,0036 (Figure 20), in monetary terms, industries and corporations that belong to a 100K headcount industry, would experience 0.0036 Bn. € or 3.6 Mio. € in average costs per cyber event.

Logarithmic analysis – Equation (5)

1. There's a strong positive relationship between Systemic risk (SR) and the size of the industry in revenue (IREV) (Figure 21), i.e., an increase in revenue quotas could potentially increase the level of the systemic risk: The logarithmic regression outcome suggests (coefficient of 1,8752, Figure 21) that a 1% increase of industrial revenues could potentially increase systemic risk by 1.875%. On the other hand, when it comes to the expected value cost for one cyber incident (or IR=1) = - 1,8088 (Figure 21) the results suggest that with the realization of each single cyber incident constituting the systemic risk a reduction of the expected value cost for one cyber incident by 1.80 will be achieved if the effect of revenue growth on the increase in systemic risk is removed as expressed by the averaged coefficient of 1.8752 (Figure 21), i.e. if industry revenues remain constant or decline. In this way, a mutually offsetting effect is achieved, if the studied industries realize economic and financial growth leading to an increase in their revenues and as a consequence in their systemic risk (1,8752), then at the same time this growth effect is offset by a decrease in the

expected value cost for one cyber incident (-1,8088)(Figure 21). Counteracting the effect of this offsetting effect implies that the increase in systemic risk at the macro level due to the increase in industry revenue is generally accompanied by an increase in the incident rate of cyber risk. If such an increase in IR is not present, then the impact of single manifestations of cyber risks may not lead to an increase in systemic risk for the industries studied as a whole.

2. There's a relatively weak negative relationship between Systemic risk (SR) and Incident rate (IR)(Figure 22), i.e., an increase in the incident rates could potentially decrease in the levels of systemic risk: The logarithmic regression outcome suggests (coefficient of -0,541, Figure 22) that a 1% increase in incident rates is related with a 0,54% decrease in the systemic risk rates. The expected value cost for one cyber incident (or IR=1) = 1.298 (Figure 22) suggests that a single occurrence of a cyber risk has the potential to increase the expected value cost of single cyber incidents that determine the level of systemic risk by approximately 1.30 points, i.e. if the averaged regression coefficient of -0.541 implies that an increase in IR rather leads to a decrease in SR for the industry as a whole, then on the basis of a single manifestation of a cyber risk included in the SR, the average expected value cost for one cyber incident increases the cyber losses determining the level of SR by 1.30 points. Thus, while at the macro level increased IR

does not directly increase SR, at the micro level the value of a single incident forming SR can lead to more significant expected losses. Or, at the micro level, the level of losses from a single cyber incident may be more significant than the overall macro estimate of SR for the industry would suggest.

This direction of impact of single manifestations of cyber risks from IR to an approximate 1.30 point increase in expected value cost for one cyber incident covered by SR can also be viewed in the context of a combined or chained manifestation. As discussed above with respect to the impact of revenue growth in the industries studied relative to SR growth, this increase in systemic risk on an industry-wide basis can only occur if accompanied by an increase in IR. Hence, on the one hand the increase in IR will directly provoke an increase in SR by increasing cyber damage from a single incident (regression coefficient of 1.298) (Figure 22), but on the other hand in the context of business growth and increased revenues will lead to a further increase in SR, as the logarithmic regression (Figure 21) coefficient of 1.8752 suggests.

3. There's a strong positive relationship between Systemic risk (SR) and the Total number of industry's employees (Figure 23), i.e., an increase in the total number of employees working in a specific industry could potentially increase the systemic risk:

- The logarithmic regression outcome suggests (coefficient of 1,3076, Figure 23) that a 1% increase in the total number of employees is related with a 1,30% incrise in the systemic risk rates.

- The expected value cost for one cyber incident (or IR=1) = -3.2006 (Figure 23) suggests that a single occurrence of a cyber risk has the potential to reduce the expected value cost of single cyber incidents determining the level of systemic risk by 3.20 points if the effect of the increase in the number of employees on the increase in systemic risk is removed as proxied by the averaged coefficient of 1.3076 (Figure 23). What is striking here is that the averaged coefficient of the impact of employees on systemic risk (1.3076) in approximately two and a half times lower than the coefficient of expected value cost for one cyber incident (-3.2006). This suggests that overall, if an increase in employees leads to an increase in systemic risk, then if the number of employees remains constant this would induce lower damage from the occurrence of one cyber incident than the averaged overall macro estimate of the employment impact for SR would predict.

4. The analysis of the relationship between industrial systemic risk (SR) and industrial incident rates (IR) in the context of the studied cyber risks (Data breaches, Privacy data breaches, Malware attacks and Phishing attacks) shows the following:

The results of the regression equation of Phishing attacks (Figure 27) shows the highest value of the coefficient reflecting the impact of the incident rate (IR) of this risk on the systemic risk SR of the industries studied (-1.261). The coefficients of the regression equation for the other cyber risks studied, subsequent in magnitude, show the following classification: Data breaches (-0.797) (Figure 24); Privacy breaches (-0.434) (Figure 25); Malware attacks (-0.115) (Figure 26);

but in terms of expected value cost per cyber incident, the highest cyber risk score demonstrates Malware attacks (2.0733) (Figure 26) followed by: Data breaches (1.0564) (Figure 24); Phishing attacks (0.683) (Figure 27); Privacy breaches (0.5591) (Figure 25);

5. The negative correlation between systemic risk (SR) and incident rate (IR) found from the regression equations of the individual cyber risks studied (Figures 22 and from 24 to 27) can be explained by the fact that cybercrime activity is directly related to economic growth. In an environment of rising GDP, systemic risk generally decreases, but economic growth provokes greater cybercriminal activity and stimulates an increase in cybercriminal risk. On the other hand, in an environment of economic growth, revenues in the economy are rising, and with a relatively constant level of debt, the coefficient of systemic risk decreases according to

Equation (2) applied in this study - % SRi,t = Debti,t / Revenuej,t . At the same time, under the same conditions of economic growth with a relatively constant number of participants in an industry, an increase in the incident rate due to increased cyber risk activity leads directly to an increase in the IR coefficient (Equation (1) - % IR = No. of incidents / No. of industry's players).

Therefore, since the negative sign of the coefficients of determination between SR and IR can be explained by the logical sequence: economic activity--> SR (Debt/Revenue) --> IR --> Cyber cost (ACC, ACI), they should be analyzed mainly as an absolute value.

6. The negative regression relationship between SR and IR may also be due to the fact that in the context of small in value single cyber risk losses, the increase in the number of incidents overall and in their aggregate value is outpaced by a general improvement in the environment leading to an improvement in SR which offsets the more frequent in number IR. This situation of "masking" the increased negative capacity of the increase in the IR of cyber risks consequent to the increase in economic growth and revenues of the studied industries may lead to an accumulation of disruptive potential that manifests itself in the occurrence of single cyber incidents with a larger volume of damage. For example, when incidents with damage volumes falling in the top 25% of

observations (Quartile 4) based on average values of ACC occur, it is possible that an increase in IR could cause an increase in SR - regression results for SR related to incident rates of an industry (Figure 22) show the expected value cost for one cyber incident (IR=1) = 1.298 with a -0.541 value of the averaged regression coefficient for the impact of IR on SR. Further support for the thesis that aggregated and averaged results (regression coefficients) based on the total number of incidents forming the IR, may lead to conclusions about the impact of individual determinants being weaker as an averaged coefficient based on all observations, but at the same time provoking a stronger impact based on a single manifestation of the individual factor, can also be found in the regression relationship between average cyber costs (ACC) related to the incident rate (IR) (Figure 19). The value of the coefficient showing the averaged impact of IR on ACC is 0.0005, but the value of the expected value cost for one cyber incident (IR=1) is approximately 6 times larger, or a coefficient of 0.0033.

7. Analyzing the above results in the context of the results of the application of the Granger Causality test, we can point out that when we consider the results of the relationship between SR, REV and IR measured only in the years when damaging cyber incidents of the respective type are recorded and only for the data

from the industries that record these incidents, we can draw the following conclusions:

- Regarding Phishing attacks - Granger Causality between SR4 REV 4 and IR4 respectively is only found at first lag, indicating a relatively short-lived interaction between the tested variables. In a direct comparison between the Granger Causality test results for these tested variables across the entire set of tested lags and cyber risk types, we can poin out that only for Phishing attacks such a short-lasting interaction between them is observed - it's only in one lag (lag 2). This gives us reason to assume the more significant impact of contingency in the manifestation of Phishing attacks and their impact on causality between SR, REV and IR. We can also see the impact of this short-term contingency when we analyze the direction of influence between the variables tested: for SR4 and REV 4, it is bidirectional, while between SR4 and IR4 the causality is from systemic risk to incident rate - that is, the intensity of cyber incidents related to Phishing attacks is directly determined by the state of systemic risk in a given industry.

- In terms of Malware attacks, recorded the highest regression coefficient of expected value cost for one cyber incident (IR=1) (Figure 26) - observed Granger Causality between SR3 REV3 and IR3 respectively, is with a higher degree of persistence over time compared to Phishing attacks. As the impact of the level

of systemic risk in the manifestation of Malware attacks cyber incidents on the revenue of the industry concerned, we should note the manifestation of this causality is in all lags studied (2, 4, 6 and 8), and the direction of causality is always from SR3 to REV3. When the causality between SR3 and IR3 is considered, the aforementioned categorical strength of the results weakens - Granger causality between systemic risk and incident rate is only recorded at lags 2 and 4, and the relationship is bidirectional.

- In contrast to the largest, in terms of statistical weight, impact of IR on SR (-1.261) recorded for Phishing attacks (Figure 27), we can examine the cyber risk Data breaches. Not only does it show the second highest impact in terms of impact strength, not only in terms of average weight (-0.797) (Figure 24), but also in terms of impact per incident (1.0564). The Granger causality between SR, REV and IR for this cyber incident shows the highest persistence in its manifestation, among all the cyber risks and lags studied, it is Data breaches that register the most Granger causalities - for SR1 and REV1 (lags 2,4,6 and 8), and between SR1 and IR1 (lags 2,4 and 6). As the lags of causality testing increased between SR1 and REV1, there was a directionality of impact at lag 2 from SR1 to REV1 that became bilateral at the remaining lags of testing. With respect to causality between SR1 and IR1, the opposite pattern of manifestation is observed: at lag 2 the relationship between the

two variables is bidirectional, but at lags 4 and 6 causality is in the direction from SR1 to IR1. This shows that in the relatively long term, the intensity of manifestation of this cyber risk expressed as the number of incidents (IR) is directly determined by the state of systemic risk.

- Combining the Granger causality results between SR and IR, as well as those from the regression dependencies (Figures 24 and 27), for the two cyber risks with the highest impact (Phishing attacks and Data breaches) we could determine their combined impact - in the short term (lag 2) for the systemic risk level (SR) the most significant impact is the impact of the intensity of manifestation (IR) of the cyber risk Phishing attacks, but the more persistent causality and determinacy over time between SR and IR is through the manifestation and impact of the cyber risk Data breaches. An additional argument in the financial significance of Data breaches as a cyber risk can be found in the fact that of all the risks studied it is Data breaches that show the highest average damage per incident (ACC) scores - €2.43m for the whole population of observations, and €5.26m for the top 25% of observations (Quartile 4).

Conclusion

We believe the analysis provided in this dissertation will be very useful in a number of different ways to future literature, corporations, policy makers, cyber security software providers and of course consumers in Greece and Europe. Despite the significant lack of data regarding cyber risk incidents and financial costs, we achieved to collect information not only from Greece but also from the European domestic economic area.

In conclusion, the future of financial digital inclusion is indeed bright, characterized by significant growth and innovation. The integration of emerging technologies, the strengthening of regulatory frameworks, the fostering of public-private partnerships, and a focus on building trust and inclusivity are key steps toward achieving this goal. While challenges like cybersecurity risks and the digital divide persist, the overall trend in Greece and the world is towards a more inclusive financial ecosystem. This evolution promises to bring about a financial landscape that is more accessible, efficient, and secure for everyone, especially underserved populations. As the digital landscape continues to evolve in Greece, ongoing collaboration, innovation, and a commitment to addressing these challenges will be crucial in shaping a more inclusive financial future.

Last but not least, we incorporated the loss rates per industry as a function of annual revenues. We concluded that the retail sector in Greece outpaces the rest of the industries in terms of financial losses and offered a plausible methodology, which describes all necessary steps defining a suitable annual cyber security budget, that can be used by corporate policy makers in Greece to mitigate financial costs related to modern cyber risk.

Ultimately, our empirical analysis confirms the hypothesis that increased cyber risk incidents in Greece correlate with higher financial costs for businesses and influence systemic industrial risk, highlighting the critical need for comprehensive cyber security strategies.

Scientific Contributions

1. An analysis and classification of the current cyber risk exposure in Greece in the period 2014 - 2021 is performed based on indicators of frequency of occurrence and extent of realized damage. The dynamics of the risk classification made is analyzed in the context of manifestation in the main economic sectors, thus producing an up-to-date assessment of the degree of cyber risk exposure specified by individual economic sectors. A classification of individual economic sectors is made, both in terms of the overall degree of cyber vulnerability and in terms of the impact of the individual types of cyber risks studied on them.

2. Using the metrics Average cost per incident, Average cost by industry and Incident rate by industry, a quantitative assessment of the impact of cyber risk exposure relative to systemic risk as a whole is made. Also, the impact of cyber risk exposure relative to large "Too Big to Fail (TBTF)" companies and hence on systemic risk in general is examined. An analysis of the dynamics of the impact of cyber risks on the systemic risk associated with these companies is made, clearly outlining both the current state and the temporal dynamics reflecting the measures taken by TBTF companies by sector to mitigate cyber risks.

3. The impact of cyber risks on systemic risk has been identified, and the methodology used has made it possible to outline both the overall impact of cyber risks on systemic risk and to identify a differentiation of the identified relationships determined by the size of single cyber incidents.

Publications

1. Koutsari, M. (2022). Internet financial risk managment. *Entrepreneurship*, 10 (2), 70-79 DOI: *10.37708/ep.swu.v10i2.7*

2. Koutsari, M. (2023). The financial impact of cyber risk: empirical evidence from Greece and the European economical zone. *Електронно научно списание – Финанси (Electronic scientific journal - Finance)*, 69-82. https://espisanie.financebg.com/wp-content/uploads/2024/02/finance-br-1-2023.pdf

3. Koutsari, M. (2024). Exploring bivariate correlations in cyber risk on an industrial level: empirical evidence from Greece and the European economic area. *Entrepreneurship*, 12 (1), 8 - 20 https://doi.org/10.37708/ep.swu.v12i1.2