Kauno technologijos universitetas

Ekonomikos ir verslo fakultetas

Pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams

Baigiamasis magistro studijų projektas

Gintarė Litvinavičienė

Projekto autorė

doc. dr. Alfreda Šapkauskienė

Vadovė

Kaunas, 2020

Kauno technologijos universitetas

Ekonomikos ir verslo fakultetas

Pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams

Baigiamasis magistro studijų projektas

Apskaita ir auditas (kodas 6211LX037)

Gintarė Litvinavičienė

Projekto autorė

doc. dr. Alfreda Šapkauskienė

Vadovė

doc. dr. Šviesa Leitonienė

Recenzentė

Kaunas, 2020

Kauno technologijos universitetas

Ekonomikos ir verslo fakultetas

Gintarė Litvinavičienė

Pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Gintarės Litvinavičienės, baigiamasis projektas tema „Pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____	_____
(vardą ir pavardę įrašyti ranka)	(parašas)

Autorius Litvinavičienė Gintarė. Pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams. Magistro studijų baigiamasis projektas / vadovė doc. dr. Alfreda Šapkauskienė; Kauno technologijos universitetas, Ekonomikos ir verslo fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė) : Verslas ir viešoji vadyba (Apskaita)

Reikšminiai žodžiai: kibernetiniai incidentai, akcijų kaina, įvykio analizės metodas.

Kaunas, 2020. 64 p.

Santrauka

Augantis informacinių technologijų naudojimas tampa neatsiejama įmonės veiklos dalimi. Atsiradusios naujos galimybės leido pasauliniu mastu išplėsti verslus. Tačiau šie pokyčiai atvėrė kelią informacijos saugumo problemai. Kibernetiniai incidentai tapo didžiule grėsme įmonėms, kurių akcijomis prekiaujama biržoje. 2016-2017 m. beveik dvigubai išaugo kibernetinių incidentų skaičius. Žalos kaina įmonėms, nukentėjusioms nuo kibernetinių incidentų, vertinama milijardais dolerių. Įmonės vis daugiau skiria lėšų kibernetinių incidentų prevencijai, tačiau kibernetiniai incidentai nesibaigia.

Vertinant kibernetinių incidentų žalą yra įvardijami ne tik ekonominiai nuostoliai, bet ir žala dėl reputacijos sumenkėjimo, socialiniai ir psichologiniai aspektai. Kibernetiniai incidentai tampa potencialiai žalingi įmonėms, kurių akcijomis prekiaujama biržoje. Investuotojai, įvertinę kibernetinio incidento poveikio mastą įmonei, priima investavimo sprendimus.

Mokslininkai ieško atsakymo kaip veikia akcijų kainų pokyčius atskleisti pranešimai apie kibernetinius incidentus. Tačiau tyrimų apie šiuos pokyčius nėra labai daug, todėl augant kibernetinių incidentų skaičiui, atsiranda poreikis tolimesniems tyrimams.
Šio darbo tyrimo objektas yra pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonės akcijų kainų pokyčiams.

Šio darbo tikslas – vertinti atskleistų pranešimų apie kibernetinius incidentus įtaką įmonių akcijų kainų pokyčiui. Siekiant įgyvendinti darbo tikslą, buvo užsibrėžti šie tyrimo uždaviniai:

1. atskleisti informacijos, susijusios su kibernetiniais incidentais, poveikį akcijų kainoms problematiką;
2. išanalizuoti akcijų rinkų ir informacijos atskleidimo tarpusavio įtakos teorinius aspektus;
3. parengti pranešimų apie kibernetinių incidentų įtakos akcijų kainų pokyčiams tyrimo metodologiją;
4. įvertinti atskleidžiamų pranešimų apie kibernetinius incidentus įtaką akcijų kainų pokyčiams.

Tyrimui pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų pokyčiui atlikti pasirinktas įvykio analizės metodas. Imtis sudaryta iš atrinktų 52 kibernetinių incidentų, įvykusių per 2015-2019 m. Šie kibernetiniai incidentai priskiriami įmonėms, kurių akcijos listinguojamos NASDAQ ir NYSE akcijų biržose bei priklausančios S&P500 indeksui.
Rezultatai parodė, kad dažniausiai suminė vidutinė perteklinė akcijų grąža susidarė vidutinio dydžio finansinių ir paslaugų įmonių įvykių languose. Taip pat didžiausia neigiama perteklinė grąža susidarė įmonėms kurių kibernetinio incidento tipas HACK (neautorizuotas įsilaužimas į kitas sistemas). Atskleisti pranešimai apie kibernetinius incidentus turi poveikį įmonių akcijų kainų pokyčiui.

Author’s Litvinavičiene Gintarė. Influence of Cyber Incident Reports on Changes in Corporate Stock Prices. Master's Final Degree Project / supervisor assoc.prof. Alfreda Šapkauskienė; School of Economics and Business, Kaunas University of Technology.

Study field and area (study field group): Business and Public Management (Accounting).

Keywords: cyber incident, event study, stock price.

Kaunas, 2020. 64.

Summary

The Growing use of information technologies has made it an essential part of doing business. The emerging opportunities allow for businesses to globalize, yet at the same time new security issues come to light. These issues are called cyber incidents have been a major problem for publicly traded companies in 2016 and 2017. In this short period of time, the number of incidents has almost doubled, causing billions of dollars in losses, as well as - calling for billions of dollars of investments to prevent these issues. But even though the money is being spent to prevent them, it is still not enough.

When evaluating cyber incident consequences, it is important to address not only the financial aspects, but also the social, psychological aspects – mainly the loss of good reputation. These incidents are a big issue for publicly traded companies as the investors must a tremendous amount of trust to invest in each company.

Scientists have been looking for an answer, as to how these incidents affect the stock prices. While there is a high demand for such research, there is not yet too much data available or too much research conducted on this issue.

The objective of this research is to evaluate the relationship between cyber incidents and stock price movement of the affected companies.

The goal here – is to evaluate the affects the reports about cyber incident reports are having to the stock prices. In order to achieve that, the research must conduct the following exercises:

1. Expose the problems of information related to cyber incident reports affect on stock prices.
2. Analyze theoretical aspects of information reporting and stock market relationship.
3. Prepare the methodology for the cyber incidents reports affects on stock prices analysis.
4. Evaluate the weight that reports have on stock prices.

The event study method was chosen to conduct this research. 52 cyber incident reports record were taken from a period 2015 through 2019. These incidents are associated with S&P500 companies, listed in NASDAQ and NYSE exchanges.

The results had shown that the most common average excess return was generated in medium-size financial and services companies. And the highest negative excess return was generated when HACK (Unauthorized access issues) type incidents occurred. The cyber incident reports do have an impact on stock price movement.

Turinys

Lentelių sąrašas **6**
Paveikslų sąrašas **7**
Įvadas **8**
1. Atskleidžiamos informacijos apie kibernetinius incidentus įtakos akcijų kainų pokyčiams problematika **10**
1.1. Kibernetinių incidentų paplitimas ir žalos įmonei mastas 10
1.2. Įmonių išlaidų tipai, patyrus kibernetinį incidentą 12
1.3. Įvykio analizės metodo panaudojimo galimybės, tiriant pranešimų apie kibernetinius incidentus atskleidimo įtaką akcijų kainų pokyčiui 13
1.4. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai tyrimų rezultatų problemiškumas ir interpretacija 14
2. Pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainai literatūros analizė **16**
2.1. Kibernetinio incidento sąvoka ir tyrimų, susijusių su kibernetinių incidentų atskleidimo įtaka akcijų kainai raida 16
2.2. Kibernetinių incidentų tipai bei susiformavimo prielaidos 19
2.3. Kibernetinių incidentų poveikis verslo subjektams ir investuotojų sprendimams 23
2.4. Informacijos saugumo sistemos svarba investuotojų požiūriu 27
2.5. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai tyrimų metodologijos ankstesniuose tyrimuose apžvalga 29
3. Pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams tyrimo metodologija **36**
3.1. Tyrimo problema ir nuoseklumas bei iškeltų hipotezių pagrindimas 36
3.2. Pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiui įvertinimo metodologija 38
4. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimas **42**
4.1. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimo imtis 42
4.2. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimo rezultatai 46
4.2.1. Bendras imties vidutinių perteklinių akcijų grąžų vertinimas 47
4.2.2. CAAR vertinimas pagal rinkos segmentą 48
4.2.3. CAAR vertinimas pagal įmonės kapitalizaciją 50
4.2.4. CAAR vertinimas pagal kibernetinio incidento tipą 51
4.2.5. CAAR vertinimas pagal kibernetinio incidento apimtį 52
4.3. Gautų tyrimų rezultatų palyginimas ankstesnių mokslinių publikacijų kontekste 54
Išvados **57**
Informacijos šaltinių sąrašas **59**
Priedai **65**

Lentelių sąrašas

1 lentelė. Išlaidų grupavimas, patyrus kibernetinį incidentą. 12
2 lentelė. Didžiausios duomenų vagystės įvykdytos 2013-2019 m. pagal įmonių rinkos segmentą. 18
3 lentelė. Kibernetinių incidentų tipai. 20
4 lentelė. Įvykio lango intervalai, nustatyti pranešimų apie kibernetinius incidentus įtakos akcijų kainų tyrimuose 31
5 lentelė. Tyrimo metodai ir taikyti modeliai tyrimuose pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiui 32
6 lentelė. Literatūros analizėje aptartų tyrimų išvados ir rezultatai 33
7 lentelė. Pranešimų apie kibernetinių incidentus imties atrankos detalizacija 42
8 lentelė. Imčių grupės pagal veiksnius 43
9 lentelė. Vidutinės perteklinės grąžos (AAR) 47
10 lentelė. Visos imties Suminės vidutinės perteklinės akcijų grąžos 48
11 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal rinkos segmentą 49
12 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal įmonės kapitalizaciją 51
13 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal kibernetinio incidento tipą 52
14 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal kibernetinio incidento apimtį 53

Paveikslų sąrašas

1 pav. Kibernetinių incidentų ir pavogtų įrašų duomenys JAV mln. vnt. statista.com duomenimis*. 11
2 pav. Kibernetinius incidentus lemiantys veiksniai 21
3 pav. Kibernetinių incidentų poveikio įmonės veiklai schema 25
4 pav. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai schema 34
5 pav. Loginė tyrimo seka 36
6 pav. Laiko eilutė, naudojama įvykio analizės metode laiko langams pažymėti 39
7 pav. Tyrimo imtis pagal rinkos segmentus 44
8 pav. Tyrimo metu surinktų pranešimų pagal incidento tipą imtis procentais 45
9 pav. Kibernetinių incidentų skaičius pagal apimtį 2015-2019 m. 46

Įvadas

Įmonės veiklos sėkmė per pastaruosius kelis dešimtmečius tapo labai priklausoma nuo informacinių technologijų vystymosi. Informacinių technologijų naudojimas tampa neatsiejama verslo dalimi ir įmonėms leidžia įgyti konkurencinį pranašumą prieš tradicines įmones. Dinamiška verslo aplinka – bendravimas su klientais iš bet kurios pasaulio vietos, operatyvūs pinigų pervedimai, elektroninė komercija, atsivėrusios rinkodaros galimybės ir pan. sukūrė papildomų galimybių verslui plėstis ir augti pasauliniu mastu. Tačiau šie pokyčiai versle atvėrė kelią labai aktualiai problemai – kibernetinių incidentų plitimui, kai pasinaudojus saugumo spragomis nutekinami konfidencialūs duomenys. Kibernetiniai incidentai yra auganti ir sparčiai plintanti grėsmė verslui, kadangi prarastas, pavogtas intelektinis turtas, pakenkta reputacija gali būti rimtas signalas investuojant į šių įmonių akcijas (Layton ir Waters, 2014).

Kibernetiniai incidentai tampa vis didesne grėsme įmonėms, kurių akcijomis prekiaujama biržoje. Žalos kaina su kiekvienais metais auga ir yra vertinama milijardais dolerių (Ponemon Institute, 2018). Lėšos, skiriamos prevencijai auga milžiniškais tempais, todėl kibernetiniai incidentai tampa viena iš didžiausių problemų įmonės valdymo srityje (Lending ir kt., 2018). Šio amžiaus pradžioje buvusi aktuali, tik kaip technologinė problema ir įdomi tik įmonės informacinių technologijų specialistams, pastaruoju laikotarpiu kibernetiniai incidentai tampa nauja ir aktualia strateginio lygmens problema.

Elektroninėje erdvėje žinios plinta labai greitai, todėl pranešimai apie kibernetinius incidentus, žinant jų poveikio reikšmę, kelia susirūpinimą akcininkams. Investuotojai įvertina tokius pranešimus ir priima investavimo sprendimus. Viešas pranešimas apie kibernetinį incidentą įtakingose žiniasklaidos priemonėse rodo, kad šie incidentai yra reikšmingi įmonei, galintys turėti neigiamam akcijų kainų pokyčiui (Spanos ir Angelis, 2016). Padidėjus rizikai dėl nuolat intensyvėjančių bei nuolat technologiškai tobulėjančių kibernetinių incidentų, svarbu suprasti, kokio tipo kibernetiniai incidentai lemia įmonės pažeidžiamumą, ar turi įtakos kibernetinių incidentų apimtis akcijų kainų svyravimui, kokios įmonės dažniausiai paveikiamos, kuriam laikotarpiui paveikiama akcijų kaina. Tai yra svarbios žinios akcininkams ir investuotojams. Akcininkai, žinodami silpnąsias grandis kibernetinių incidentų saugumo srityje, gali sutelkti resursus šioms grandims apsaugoti. Investuotojai, vertindami informacijos saugumo sistemą įmonėje, priima pozityvius sprendimus investuojant į tokių įmonių akcijas (Yang ir kt., 2020).
Atlikta nemažai mokslinių tyrimų, kuriuose konstatuota sumažėjusi reputacija, prarast klientai, sumažėjęs augimas ar net verslo praradimas dėl pranešimų apie kibernetinius incidentus poveikio, tačiau tyrimų, kuriuose analizuojama tiesioginiai kaštai akcininkams, t.y. kibernetinių incidentų poveikis akcijų kainų pokyčiams yra pakankamai nedaug. Naujausi tyrimai kibernetinių incidentų poveikio akcijų kainoms tyrimų srityje rodo ypač išaugusį dėmesį šiai mokslinei problemai (Colivicci ir Vignaroli,, 2019; Yang ir kt., 2020; Juma ir Alnsour, 2020, Evans ir kt., 2019).

Tyrimuose mokslininkai ieško atsakymų mokslinei problemai – kokio tipo kibernetiniai incidentai veikia įmonių vertę stipriausiai (Spanos ir Angelis., 2016), kuri pramonės šaka labiausiai yra atakuojama įsilaužėlių (Rosati ir kt., 2017). Kaip pabrėžia Vernon ir kt. (2019), tokie tyrimai yra svarbūs įmonėms, kad galėtų apskaičiuoti rizikas pinigine verte, investuotojams ir analitikams leistų geriau suprasti pranešimų apie kibernetinius incidentus įtaką investavimo sprendimams.

Tyrimai, kuriuose stebima pranešimų apie kibernetinius incidentus atskleidimo įtaka akcijų kainų pokyčiams, dažniausiai atlikti užsienio akcijų rinkų kontekste, tačiau Lietuvos akcijų rinkos kontekste

tokių tyrimų nėra atlikta. Tyrimus Lietuvoje apriboja apsunkintas duomenų apie įvykusius kibernetinius incidentus prieinamumas, pakankamo kiekio nebuvimas, o dėl mažos duomenų imties išvados gali būti netikslios ir neinformatyvios, todėl, dėl išvardintų priežasčių, šiame projekte tyrimas atliekamas JAV akcijų rinkos kontekste.

Šiame magistro baigiamajame projekte siekiama išsiaiškinti, ar paskelbta informacija apie kibernetinį incidentą daro įtaką įmonės akcijų kainų pokyčiui. Kaip minėta anksčiau apie klausimus, kylančius akcininkams ir investuotojams, tyrime bus ieškoma atsakymų: kurio rinkos segmento įmonės yra pažeidžiamiausios, kokio tipo ir apimties kibernetiniai incidentai labiausiai atsakingi už neigiamą investuotojų reakciją.

Šio darbo tyrimo objektas yra pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonės akcijų kainų pokyčiui.

Šio darbo tikslas – vertinti atskleistų pranešimų apie kibernetinius incidentus įtaką įmonių akcijų kainų pokyčiui.

Siekiant įgyvendinti darbo tikslą, buvo užsibrėžti šie **tyrimo uždaviniai**:

1. atskleisti informacijos, susijusios su kibernetiniais incidentais, poveikį akcijų kainoms problematiką;
2. išanalizuoti kibernetinių incidentų poveikio įmonių veiklai bei akcijų kainų pokyčiui ankstesnių mokslinių tyrimų aspekte;
3. sudaryti pranešimų apie kibernetinių incidentų įtakos akcijų kainų pokyčiams tyrimo metodologiją;
4. įvertinti atskleidžiamų pranešimų apie kibernetinius incidentus įtaką akcijų kainų pokyčiams.

Tyrimo metodai ir šaltiniai. Tyrime bus remiamasi įvykio analizės metodas, kurią sudaro regresinė analizė, rinkos modelis. Naudota mokslinės literatūros analizė, kurios visi šaltiniai yra užsienio autoriai. Darbe naudojama vokiečiu mokslininkų sukurta elektroninė programa „event study tools“ akcijų grąžų skaičiavimui (Shimmer ir kt., 2014) bei SSPS programa.

Baigiamojo magistro studijų projekto struktūra sudaryta iš keturių pagrindinių dalių. Pirmojoje dalyje aptariama pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams problematika. Pateikiama statistinių duomenų bei pavyzdžių, kurie susiję su neigiama kibernetinių incidentų įtaka. Antrajame skyriuje apžvelgiamos pagrindinės mokslinės literatūros tendencijos bei aptariami metodai. Trečiojoje dalyje pateikiamas ir pagrindžiamas tyrimo metodas, pateikiamas tyrimo sekos algoritmas, kuriuo vadovaujantis atliekamas tyrimas. Paskutiniame tyrimo, pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams, skyriuje pristatomi gauti rezultatai bei lyginami su mokslinėje literatūroje pateiktais rezultatais. Galiausiai pateikiamos išvados, pristatomi tyrimo ribotumai bei siūlymai, kaip ateityje būtų galima plėtoti šią tematiką.

1. Atskleidžiamos informacijos apie kibernetinius incidentus įtakos akcijų kainų pokyčiams problematika

Pirmojoje dalyje, kuri padalinta į keturis poskyrius, aprašoma kibernetinių incidentų paplitimas ir žalos mastas. Pateikiami sugrupuoti išlaidų tipai. Taip pat pristatomas įvykio analizės metodas bei pateikiama diskusija rezultatų problemiškumo ir interpretacijos klausimais.

Kasmet verslo, perkeliančio procesus į elektroninę erdvę, kreivė kyla milžiniškais tempais, vis daugiau duomenų yra saugoma elektroninėje erdvėje, vis daugiau finansinių transakcijų atliekama elektroniniu būdu, tačiau ne visada įmonės sugeba užtikrinti duomenų saugumą. Surastos spragos programiniuose koduose, leidžia hakerių organizacijoms įvykdyti kibernetinius incidentus. Susiformavusi problema prieš kelis gerus dešimtmečius – atskleistų pranešimų apie kibernetinius incidentus įtaka akcijų kainai, tampa ypatingai aktuali dabartiniu laikotarpiu.

1.1. Kibernetinių incidentų paplitimas ir žalos įmonei mastas

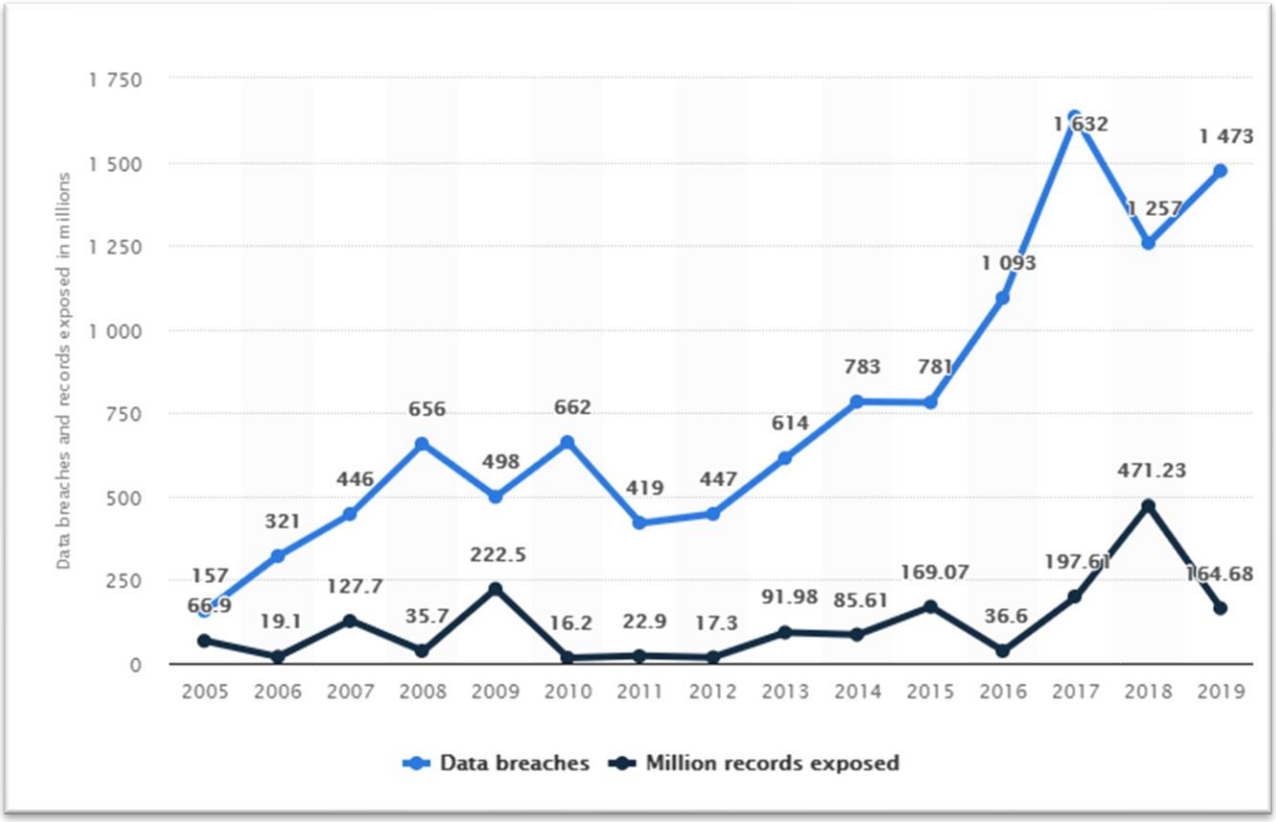
Verslas vis labiau priklauso nuo skaitmeninių duomenų, debesų kompiuterijos, darbo jėgos mobilumo, todėl privatūs įmonių duomenys, saugomi vietiniuose kompiuteriuose, įmonių duomenų bazėse, debesų serveriuose, tampa vis dažniau pažeidžiami, o tokių, mažai apsaugotų, duomenų pasisavinimas tampa vis lengviau prieinamas įsilaužėliams. Sparti komunikacijų ir technologijų pažanga formuojama pasaulinio verslo ir ateityje keis verslo struktūras. Informacinių sistemų valdymas ir apsauga vis dažniau patraukia akcininkų dėmesį dėl nuolat vykstančių kibernetinių incidentų. Duomenų kibernetinėje veikloje saugumas ir privatumas tampa opi problema kasdieninėje įmonės veikloje. Net ir įvedus įmonėje tam tikras procedūras, galinčias sumažinti kibernetinių incidentų riziką – duomenų šifravimas, ugniasienės, vartotojo prieigos kontrolė, darbuotojų mokymas, kibernetinio incidento grėsmės vis dar išlieka. Nepaisant įvairių saugumo priemonių, programišiai tampa labiau organizuoti bei technologiškai pasiruošę.

Paminėtini plačiai pasaulyje žinomi kibernetinių atakų pavyzdžiai, dėl kurių nukentėjo ne tik įmonių prestižas, bet finansiniai ištekliai. Bendrovės „Yahoo“, buvusios tarp populiariausių paieškos sistemų, po 3 mlrd. duomenų vagystės 2013 m., apie kurią prabilta tik 2016 m., kaina smuko iki 350 mln. dolerių. Tačiau tik praėjus trejiems metams, po prijungimo prie „Verzion“ buvo pranešti tikrieji nuostolio mastai, susidarę dėl įvykusio kibernetinio incidento. Tik viena kenksminga žinutė kompanijos darbuotojo elektroniniame pašte ir kompanijos vertė rinkoje sumažėjo kelis kartus. „Uber“ 2016 m. nutekinta informacija apie 56 milijonus vartotojų dėl žmogiškojo faktoriaus – informacinių technologijų specialisto laikyti slaptažodžiai viešai prieinamoje saugykloje tapo programišių taikiniu. 2018 m. Viešbučių tinklas „Meriot International“, kurio akcijos parduodamos biržoje taip pat pranešė, kad patyrė kibernetinį įsilaužimą ir pavogta buvo apie 500 milijonų klientų asmeninių duomenų. „British Airways“ sulaukė 183 mln. svarų sterlingų baudos už tai, kad įsilaužėliai 2018 m. pavogė kelių šimtų tūkstančių keleivių duomenis. 2017 m. „Equifax“ išplatino pranešimą, kuriame sakoma, kad 146 milijonai asmens duomenų buvo nutekinti, pasinaudojus programėlės saugumo spraga. (Yahoo finance.com). Tai įmonės, kurių kapitalizacija yra labai didelė, tačiau duomenis programišiai nutekina pasinaudoję labai primityviomis darbuotojų klaidomis.

Šie pakankamai stambūs kibernetiniai incidentai yra tik keli pavyzdžiai iš daugelio nutikusių per pastarąjį dešimtmetį. Kaip matyti iš pateiktų skaičių 1 paveiksle, metams einant didėja nutekintų duomenų skaičius, t.y. auga nukentėjusiu nuo kibernetinių atakų dėl trečiųjų asmenų kaltės, privačių asmenų skaičius.

Įmonės taip pat nelieka be pasekmių – 2019 m. kibernetinės atakos JAV verslui kainavo 8,19 mln. JAV dolerių. Per 14 metų nuo 2006 m. net 130 proc. išaugo kibernetinių incidentų skaičius JAV. Pasauliniu mastu 2019 m. vidutinė kibernetinių atakų kaina siekia 3,92 mln. (Ponemon Institute, 2019)

Tenka pastebėti, kad duomenų nutekėjimas neprasidėjo, kai įmonės pradėjo saugoti savo duomenis skaitmeniniu būdu. Ištakos, kaip jau anksčiau buvo minėta, siekia tuos laikus, kai tik asmenys ar įmonės pradėjo tvarkyti duomenis rašytine informacija. Kaip pavyzdžiai galėtų būti asmeninių medicininių bylų peržiūra neturint leidimo ar rastų dokumentų peržiūra po netinkamo jų sunaikinimo.



1 pav. Kibernetinių incidentų ir pavogtų įrašų duomenys JAV mln. vnt. statista.com duomenimis*.

*Pastaba. Paveikslas paimtas iš statista.com

Tačiau, atsiradus laisvai prieinamam internetui, duomenų nutekinimas persikėlė į elektroninę erdvę Taigi 1 paveiksle grafiškai pavaizduotas kibernetinių atakų ir pavogtų įrašų skaičiaus kitimas nuo 2005 m iki 2019 „statista“ duomenimis. Šio paveikslo duomenys rodo, kad viešai skelbiamų duomenų nutekinimas – kibernetiniai incidentai JAV per 2016- 2017 metus išaugo beveik dvigubai.

Dažnu reiškiniu tampantys kibernetiniai incidentai, kurių metu vykdomi įsilaužimai į bendrovių interneto tinklalapius, duomenų saugojimo bazes ar kitus objektus, turint tikslą užvaldyti konfidencialius duomenis, kelią klausimą akcininkams, kaip paveiks įmonę šie incidentai. ir su tuo susijusias veiklas kaip, duomenų pasisavinimą, sunaikinimą ar išpirkos prašymus, užduoda klausimą, ar tokie atskleisti faktai daro įtaką įmonių akcijų kainų pokyčiams. Pažeidimų skaičius auga ir skaičiumi, ir padaryta žala. Kalbama apie galimą tiek tiesioginį, tiek netiesioginį poveikį pažeistoms įmonėms (Layton ir Waters, 2014; Morgan, 2017).

1.2. Įmonių išlaidų tipai, patyrus kibernetinį incidentą

Pranešimus apie kibernetinius incidentus reikėtų priskirti prie pranešimų, kurie turi tiesioginę įtaką organizacijai. 2019 m. Ponemon Instituto tyrime nurodyta, kad vidutinė duomenų pažeidimo kaina vienam sugadintam įrašui siekė 148 JAV dolerius, o pažeidimai aptikti vidutiniškai per 196 dienas. Tyrime konstatuota, kad išlaidos ir pavogtų duomenų apimtys auga metams bėgant. Išlaidos gali susidaryti mokant kompensacijas klientams už jų pavogtus asmeninius duomenis, valstybei baudas už duomenų pažeidimus, už teisininkų paslaugas, už duomenų atkūrimą, saugumo spragų tvarkymą. Taip pat gali būti patiriamos išlaidos dėl reputacijos sužlugdymo, intelektualios nuosavybės, produktyvumo praradimo (Morgan, 2018). Išlaidas, atsiradusias dėl kibernetinių incidentų galima suskirstytos į dvi išlaidų grupes (1 lentelė).

1 lentelė. Išlaidų grupavimas, patyrus kibernetinį incidentą.

Išlaidų grupė	Praradimai	Aprašymas
Tiesioginės	Pelno praradimas. Produktyvumo praradimas. Programinės ir kompiuterinės įrangos kaina.	Dėl trečiųjų šalių atakos sulėtėja serverių darbas, užsakymų sistema sulėtėja ir nebegali priimti užsakymų. Dėl viruso atakų elektroninio pašto sistemos ar tinklo sistemos sulėtėja ar visiškai išsijungia; darbuotojai sprendžia susidariusias problemas, bandydami pašalinti virusus. Infekuoti pašto ar failų serveriai turi būti pataisyti ar pakeisti naujais; sugedusi kompiuterinė įranga keičiama nauja.
Netiesioginės	Klientų pasitikėjimo ir lojalumo praradimas. Konkurencinio pranašumo praradimas. Investuotojų pasitikėjimo praradimas.	Klientai bijo dėl duomenų saugumo ir nebepasitiki įmone, kuri nesugeba apsaugoti jų privačių duomenų. Klientai išeina pas konkurentus; pavogtos prekybos paslaptys mažina konkurencinį pranašumą. Investuotojai parduoda akcijas arba nustoję jas pirkę. Išauga kapitalo kaina.

Pastaba. Lentelė sudaryta autorės pagal Juma'h, (2020), Amir ir kt. (2018), Lending ir kt. (2018), Spanos ir Angelis, (2016).

Pirmoje lentelėje išlaidos po kibernetinių atakų suskirstytos į dvi grupes. Kaip matyti, atsiradus tiesioginėms išlaidoms neišvengiamai įmonė patirs netiesioginių išlaidų, jei nebus operatyviai atnaujintas serverių darbas, pašalinti virusai. Taip pat daug priklausys kokio masto įsilaužimas įvykdytas ir kaip pakenkti duomenys, kiek jų pavogta. Tiesioginės išlaidos siejamos su sugadintos programinės įrangos atstatymo kaina, produktyvumo praradimu dėl sulėtėjusių serverių darbo, kai nebegali įmonė vykdyti veiklos, pvz. elektroninės komercijos įmonės. Netiesioginės išlaidos gali stipriai pakenti konkurencinėje kovoje dėl klientų nebepasitikėjimo ir perėjimo pas kitus tiekėjus. Toks scenarijus įmonei ypač skausmingas, nes atstatyti prarastus ryšius su klientais gali užtrukti.

Akcijų rinkų rezultatai gaunami įvertinus daugybę duomenų šaltinių, kurie tiesiogiai ar netiesiogiai reaguoja į įvairius įvykius. Tiriant kibernetinių incidentų žalą, nėra pakankamai paprasta įvardinti visas pasekmes (Amir ir kt.) Kaip jau minėta, kad įtaką akcijų kainai sudaro nemažai dedamųjų, todėl tyrimai, kuriais stebima kibernetinių išpuolių poveikis įmonės akcijų vertei, dar tik įsibėgėja.

1.3. Įvykio analizės metodo panaudojimo galimybės, tiriant pranešimų apie kibernetinius incidentus atskleidimo įtaką akcijų kainų pokyčiui

Remiantis efektyviosios rinkos hipoteze – visa prieinama informacija jau atsispindi akcijų kainoje. Tačiau nepaisant šios teorijos įtakos finansų mokslui, gali būti ir kitokių atvejų, kai informacija sulaikoma ar nepranešama tam tikrą laiką arba reaguojama į panašią informaciją labai skirtingai. Atlikus, dar daugiau tyrimų, galima tiksliau vertinti duomenų pažeidimo įtaką organizacijų akcijų kainų pokyčiams bei kitiems ekonominiams rodikliams. Vadovai gali būti linkę bent laikinai slėpti tokio tipo pranešimus investuotojams, nenorėdami sulaukti neigiamos reakcijos rinkoje (Amir ir kt., 2018). Pranešimai apie kibernetinius incidentus į žiniasklaidos akiratį patenka ne iškarto po incidento išaiškinimo. Gali praeiti nemažai laiko nuo kibernetinio incidento fiksavimo kaip įvykio įmonės veikloje iki pranešimo spaudai. Tam gali būti kelios priežastys – įmonė gali nežinoti, kad yra įsilaužta į jos tinklus kaip, kad atsitiko „Equifax“ atvejis arba informacija apie įvykusį incidentą gali būti tendencingai slepiama iki tam tikro momento– „Yahoo“ atvejis.

Tyrimuose, kuriuose analizuojama pranešimų apie kibernetinius incidentus atskleidimo įtaka akcijų rinkų pokyčiams, ieškoma veiksnių, kurie galėtų veikti rinkos kainų svyravimus. Šiame amžiuje svarbiu akcijos kainos rodikliu tampa viešai paskelbta, prieinama informacija. Ji plinta greitu tempu, investuotojai turi būti pasiruošę interpretuoti informacijos turinį.

Informacijos ir akcijos kainos priežastinio ryšio problema egzistuoja nuo tada, kai buvo pradėta prekiauti įmonių akcijomis viešai. Įmonių pranešimai apie esminius įvykius ar kita nefinansinė informacija, kaip pranešimai apie kibernetinius incidentus mažina informacijos asimetriją, t.y. leidžia investuotojams turėti visą prieinamą informaciją apie įmonę. Investuotojai, turėdami patikimos informacijos apie įmonę, reaguoja apsispręsdami – pirkti ar parduoti akcijas. Tokios reakcijos yra kaip prielaidos įsitikinti, kokias naujienas vertina investuotojai ir kaip po to reaguoja rinka. Investuotojai vertina ne visas informacinio srauto naujienas, susijusias su organizacijų veikla – yra atsirenkama tai, kas turi potencialiai didžiausią įtaką akcijų kainoms kisti tam tikru laiku. Reikėtų pabrėžti, kad jei kalbama apie informacijos srautą, tai dažniausiai kalbama apie informacijos sklaidą interneto kanaluose.

Tyrimai, kuriuose analizuojama pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams yra dar pakankamai nauja sritis (Spanos ir Angelis, 2016). Įvykio analizės metodas pritaikytas šiuose tyrimuose leidžia nustatyti akcijų kainų pokytį (Campbel, 2003). Įvykio analizės metodas yra statistinis metodas, kuris remiasi efektyviosios rinkos prielaida, nustatantis perteklines akcijų grąžas, atsirandančias dėl tam tikro įvykio. Dėl rinkos racionalumo įvykis iškart atsispindės akcijų kainoje (MacKinlay, 1997). Įvykio analizės metodas, kuriuo tiriama pranešimų apie kibernetinius incidentus įtaka akcijų kainų pokyčiams, remiasi efektyvios rinkos prielaida, kuri teigia, kad rinka racionali tada, kai investuotojai žino visą prieinamą informaciją apie akcijos kainą ir tai yra panaudojama priimant investavimo sprendimus. Tačiau efektyviosios rinkos teorija ne visada yra palaikoma iracionalių investuotojų, kurių kiekis yra išaugęs dėl lengvai prieinamo investavimo galimybių. Šiuos investuotoju dažnai lydi sentimentai.

Psichologų susidomėjimas asmenų finansiniais sprendimais išaugo praėjusio šimtmečio septintajame dešimtmetyje. Analizuota investuotojų elgesys, priimat sprendimus, nagrinėtos kognityvinės klaidos, o rezultatuose rasta abejonių dėl efektyviosios rinkos. Kaip jau žinoma iš Tversky ir Kahneman (1973) darbų, šie mokslininkai konstatavo, kad sprendimų priėmėjai (investavimo atveju –

investuotojai) linkę susikoncentruoti ties kraštutinumais, o ne faktais. Taip atsitinka, kai gaunama informacija akivaizdžiai neatitinka turimos informacijos, t. y. atmetami prieštaringi elementai, o priimamas šališkumas. Pranešimų apie kibernetinius incidentus tyrimu atveju dažnai nurodoma, kad negatyvi investuotojų reakcija išsilaikė tik kelias dienas po pranešimo.

Elgsenos finansų šalininkai kritikuoja efektyvios rinkos hipotezę, tačiau kol nesukurta alternatyvių modelių, kuriais būtų tiriama akcijų rinkų kitimo prognozės, vertinimui pasitelkiama investuotojų iracionalumą, psichologinius veiksnius, įskaitant informacijos patikimumą ir prieinamumą. Atsiradus lengvam prieinamumui turėti galimybę pirkti akcijas, efektyviosios rinkos hipotezė ne visada veikia, kai atsiranda emocijos ir jos perkamos akcijų pavidalu – Strauss ir Smith (2019). Tiriant institucinių investuotojų emocijas elgsenos finansų kontekste, galima tikėtis kitokių išvadų. Ahmad'o ir kt. (2017) tyrimas patvirtino šias išvadas. Jų elgsenos finansų tyrimo metu atmestas teorinis institucinių investuotojų neracionalaus elgesio modelis. Analizė parodė, kad elgsenos euristika ir šališkumas yra dinamiški ir sudėtingi, o norint suprasti elgesio šališkumo kilmę, priežastis ir padarinius reikia kompleksiško vertinimo psichologijos, sociologijos ir biologijos kontekste. Sujungus kognityvinę psichologiją ir finansus į vieną objektą mokslininkų darbuose atsirado elgsenos finansų tyrimų, kuriuose stebima emocinių veiksnių įtaką investuotojų finansiniams sprendimams. Jain ir kt. (2019) išskyrė penkis investuotojus veikiančius kriterijus – „parduodu akcijas, nes jos jau pakankamai pabrango", „žinios ir naujienos žiniasklaidoje labai veikia mano investavimo sprendimus", „investuoju į kiekvieną akciją atskirai ", „aš išlaikau nuvertėjusias akcijas, tikintis, kad jų kaina ateityje kils". Tyrėjai pažymi psichologinio nusiteikimo svarbą sprendimų priėmimui investavimo procese. Individualios savybės tampa svarbiomis šiame procese. Sprendimams turi įtakos vidiniai ir išoriniai elgesio veiksniai.

1.4. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai tyrimų rezultatų problemiškumas ir interpretacija

Kaip pažymi Strauss ir Smith (2019) tyrimo išvadose – investuotojų elgesys gali prieštarauti racionaliajam rinkos modeliui, kai kalbama apie staiga atsiradusią naują ir netikėtą informaciją. Galima sutikti, kad investuotojams prieštaraujant racionaliajam rinkos modeliui, atsiranda temos problemiškumas – atsiradus naujiems pranešimams apie kibernetinius incidentus rinkos reakcija gali būti netikėta. Investuotojų sprendimas gali būti netikėtas net ir kalbant apie panašaus pobūdžio informaciją, tačiau atsiradusi skirtingu laiku, iš įmonių, priklausančių skirtingam rinkos segmentui ar pranešime nurodant kibernetinio incidento tipą bei apimtį, gali būti vertinama labai prieštaringai. Laikui einant kinta probleminės sritys įmonių valdyme – įdiegus naujas ir efektyvias saugumo sistemas, investavus lėšų, įdiegus saugumo standartus, vėlgi, leidžia investuotojams peržiūrėti investavimo sprendimus, o tyrėjams kyla naujų uždavinių tyrimams bei metodikoms (Spanos ir Angelis., 2016).

Atotrūkis tarp informacinių technologijų ir verslo nyksta. Technologiniai pokyčiai pakeitė informacijos saugumo problemą nuo pavienio klausimo iki strateginio verslo iššūkio ir reikalauja atitinkamo valdymo. Dėl visapusiško technologijų įtraukimo į verslą, pranešimai apie kibernetiniai incidentai daro tiesioginį poveikį verslui ir gali rimtai paveikti organizaciją (Berkman ir kt., 2018; Horne ir kt., 2017; Soomro ir kt., 2016)

Daugumoje atliktų tyrimų šiuo metodu gauti rezultatai rodo, kad atsiranda negatyvi investuotojų reakcija į pranešimus apie kibernetinius incidentus, t.y. stebimos suminės vidutinės perteklinės akcijų

grąžos. Tačiau tie patys tyrimai atskleidžia, kad labai prieštaringus rezultatus siejamus su reikšmingumo lygiu.

Nustatyta, kad įmonės, kurios nėra stiprios informacinių technologijų srityje yra dažniau pažeidžiamesnės kibernetinių incidentų. Taigi kibernetiniai incidentai gali identifikuoti trūkumus įmonių vidaus kontrolėje, atsainų požiūrį į apsauginių sistemų diegimą, ir neatsakingą elgesį su klientų asmeniniais duomenimis. Tokias išvadas padarę investuotojai savo investavimo sprendimais sukelia neigiamas akcijų grąžas.

Tačiau anksčiau, šiame skyriuje minėti kibernetiniai incidentai, kuriuos patyrė didžiosios bendrovės „Equifax“, „Walmart“, „Apple“ rodo, kad kibernetiniai incidentai yra grėsmė net ir toms įmonėms, kurios investuoja į informacines technologijas. Dažnas autorius nurodo, kad žalos efektas ar tai būtų finansinio pobūdžio ar ne nėra gerai žinomas (Brody ir kt., 2018), tačiau stebint perteklines akcijų grąžas įvykio analizės metodu matomi neigiami rodiklių rodmenys. Pirmuosiuose tyrimuose atliktuose dar apie 2000 m. buvo atskleista, neigiama statistiškai reikšminga rinkos reakcija konfidencialių duomenų imties daliai (Campbel, 2003). Vėlesniais metais atlikti tyrimai, naudojant įvykio analizės metodą ir parenkant imčiai skirtingus veiksnius pateikė labai skirtingų rezultatų (Abhishta ir kt., 2017; Colivicci ir Vignaroli, 2019; Rosati ir kt., 2017). Kibernetiniai incidentai sulaukia prieštaringo dėmesio bei kelia klausimus – kaip apsaugoti įmonės duomenis nuo įsilaužėlių ir kokios pasekmės gali laukti įmonės (Juma'h, 2020). Kaip savo darbe taikliai pastebėjo Lending‘as ir kt. (2018), kad nusikalstami kibernetiniai incidentai, o vėliau ir pranešimai apie juos neigiamai veikia įmonės veiklos rezultatus – sumažėjusius pardavimus, padidėjusius prekių grąžinimus, galimai apyvartos sumažėjimus, akcijų kainas bei kitus rodiklius.

Kibernetiniai incidentai gali būti vadinami kaip mažos rizikos nusikalstamumas, galintis atnešti milžiniškų pajamų nusikaltėliams ir padaryti nepataisomą žalą milijonams žmonių per metus (McAfee, 2020). Įmonių išlaidos progresuoja ir sudaro platu spektrą: nuo pažeistos intelektinės nuosavybės, asmeninės ir verslo informacijos iki sugadintos reputacijos, prarasto verslo bei finansinių, susijusių su baudomis, kompensacijų mokėjimais.

Apibendrinant galima teigti, kad nuo kibernetinių incidentų neapsaugotas niekas, kas aktyviai naudojasi internetu, ar tai būtų pavienis vartotojas, ar didžiulė korporacija. Pastebėta, kad tik analizuojant pranešimų apie kibernetinius incidentus atskleidimo įtaką įmonių akcijų kainų pokyčiams, galima suprasti kokios įmonės gali būti veikiamos šių incidentų. Žinant kibernetinių incidentų tipus, kokias vietas pažeidžia ar net dažniausiai nutekinamų duomenų pobūdi, galima parengti prevencinius planus įmonės saugumo atžvilgiu, klientams parodant socialiai atsakingo verslo poziciją. Akivaizdu, kad kibernetiniai incidentai ir jų poveikis įmonių akcijų kainoms išlieka aktualia problema akcininkams ir investuotojams. Toliau darbe bus analizuojama mokslinė literatūra pranešimų apie kibernetinius incidentus įtakos akcijų kainų pokyčiui tematika, siekiant įgauti žinių, kurios bus naudingos tolimesniame tyrimo etape.

2. Pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainai literatūros analizė

Šiame skyriuje bus apžvelgtos pagrindines mokslinės literatūros tendencijos, susijusios su kibernetinių pranešimų įtaka įmonės akcijų kainai. Aptartos sąvokos, veiksniai, suvaldymo strategijos. Taip pat bus pateikta įžvalgų, kokiais metodais vadovaujasi mokslininkai, tiriantys kibernetinių incidentų poveikį įmonių akcijų kainoms.

2.1. Kibernetinio incidento sąvoka ir tyrimų, susijusių su kibernetinių incidentų atskleidimo įtaka akcijų kainai raida

Technologinė pažanga skatina verslus keistis – vis daugiau verslo operacijų perkeliama į elektroninę erdvę, duomenys ir kita konfidenciali informacija saugoma, naudojantis debesų kompiuterijos paslaugomis. Pasaulio ekonomika tampa priklausoma nuo elektroninių sandorių, elektroninės komunikacijos, kur vartotojai irgi keičia savo įpročius – keliasi į kibernetinę erdvę.

> *Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija. (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018).*

Su informacinių technologijų pažanga atsiranda asmenų, kurie siekia piktavališkai pakenti. Pavienių asmenų ir grupuočių vykdomi kibernetiniai incidentai tapo opi problema, kadangi ketinimai susiję su siekimu užvaldyti asmeninę ir įmonių konfidencialią informaciją. Skaitmeninių duomenų apsaugai tampant vis didėjančiu rūpesčiu, su kibernetiniu saugumu susijusių išpuolių ne tik daugėja, bet keičiasi ir auga jų įvairovė (Spanos ir Angelis, 2016). Taip pat rūpestį kelia kibernetinių incidentų sukeliama žala. Nepaisant vis didėjančių pastangų užkirsti kelią kibernetiniams pažeidimams, kaskart galima stebėti pranešimus apie organizacijas, kenčiančias nuo kibernetinių incidentų.

Kibernetinio incidento sąvoka įvairių valstybių teisėje apibrėžiama nepakankamai išsamiai. Pavyzdžiui, JAV teisėje nurodoma, kad kibernetinis incidentas tai ne tik įvykis, bet ir suplanuoti veiksmai, kurie kelia pavojų informacinėse sistemose esančiai informacijai.

> „*Kibernetinis incidentas – įvykis ar veikla kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018).*

Kibernetinės atakos gali būti įvardijamos kaip duomenų vagystės, kurios nusakomos netgi tokiomis veiklomis, kaip įsilaužimas į įmonės duomenų bazę, žinomų asmenų nuotraukų publikavimas, įsilaužimas siekiant pavogti kredito kortelių duomenis ar netgi netinkamai išmestų fizinių dokumentų radimas (Lending ir kt., 2018).

Autoriai nepateikia vienareikšmiškos ir griežtos sąvokos. Literatūroje naudojami įvairūs terminai, apibrėžiantys kibernetinius incidentus: „Kibernetinės atakos“ (Amir ir kt. 2018), „duomenų

pažeidimai“, „duomenų vagystės“ (Vernon ir kt. 2019), “kibernetinis nusikaltimas“ (Smith, 2018), „Informacijos saugumo įvykiai“ (Spanos ir kt., 2016).
Dar kelios sąvokos, susijusios su kibernetiniais incidentais, kurias būtina apibrėžti, yra „kibernetinis saugumas“ ir „informacijos sauga“.

> „*Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą*.“ *(Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018).*

Kibernetinis saugumas tai yra procesų, valdymo, vadovavimo ir kontrolės priemonių, naudojamų skaitmeninei aplinkai apsaugoti, visuma, apimanti informacinį ir elektroninį turtą, galutinius vartotojus, organizacijas, vyriausybes. Šiuo procesu pašalinami, sumažinami arba sušvelninami neteisėti veiksmai, kuriais siekiama padaryti žalą (Azmi ir kt., 2018)

Terminų Kibernetinė sauga ir informacinė sauga reikšmė yra panaši. Tačiau kibernetinis saugumas apima platesnį objektų kiekį – ne tik kibernetinės erdvės, bet ir asmenų turto, kurį galima pasiekti elektroninėje erdvėje apsaugą.

Pasauliui skaitmenizuojantis, programinė įranga tampa svarbia kasdieninės veiklos dalimi, tačiau lygiagrečiai atsiradę kibernetiniai incidentai stiprėja technologiškai, o jų mastas auga. Atsiradus pirmajam kompiuteriui, o vėliau ir internetui, supaprastinus jų valdymą iki eilinio vartotojo lygio, interneto vartotojų skaičius sparčiai augo. Pirmasis kibernetinis incidentas minimas 1973 m. data, kai vieno Niujorko banko kasininkas, kompiuterio pagalba, išeikvojo apie 2 mln. JAV dolerių (Wavefrontcg, 2016). Po devynerių metų buvo išsiųstas pirmasis nepageidaujamas elektroninis laiškas. Vėliau kas metai kibernetinių incidentų kiekis augo, o nusikaltimai sunkėja kartu su technologine pažanga. Išleidžiama didelis kiekis įvairios programinės įrangos, kuriose kūrimo ar priežiūros stadijose jau yra padarytos klaidos. Tokiomis klaidomis naudojasi kenkėjiškų programų kūrėjai. Kūrėjai nuolat tobulina programas, tačiau kenkėjiškos veiklos elektroninėje erdvėje nuolatos tobulėja taip pat. Gali būti situacijų, kai išleidžiama programa su pakankamai saugiu kodu, tačiau vartotojų prašoma atskleisti perteklinį skaičių asmeninių duomenų ar gauti prieigą prie kitų įrenginyje saugomų duomenų. Vėliau tokie duomenys gali būti perduoti trečiosioms šalims (Nacionalinio kibernetinio saugumo būklės ataskaita, 2018). Įmonės išleidžia vidutiniškai daugiau nei tūkstantį milijardų JAV dolerių, investuojant į informacines technologijas (Pirounias ir Patsakis, 2014)., todėl nukentėję tampa įvairūs suinteresuoti asmenys: akcininkai, klientai, mokesčių mokėtojai.

Pirmieji tyrimai, susiję su kibernetinių incidentų pranešimų poveikiu akcijų kainai atlikti prieš beveik 20 metų (Campbell ir kt. 2003; Cavusoglu ir kt., 2004; Garg ir kt., 2003). Vis daugiau tyrinėtojų atlieka tyrimus kibernetinių incidentų pranešimų įtaka įmonės akcijų kainai tema, paliesdami įvairius šios temos aspektus.

Roztocki ir Wistroffer (2008) apžvelgia literatūrą kibernetinų incidentų tematika, kuri apima ankstesnius tyrimus nuo 1993 m. iki 2008 m. Straipsnyje aptariami jau egzistuojantys 46 tyrimai,

kuriuose įvykio analizės metodu stebima akcijų kainų viršpelniai, atsirandantys po reakcijos į kibernetinius incidentus. Atlikę analizę, autoriai teigia, kad įvykio analizės metodas yra pakankamai naujas, tačiau greitai populiarėjantis, todėl yra siūloma ateityje atlikti daugiau panašių tyrimų.

Spanos'as ir Angelis (2016) pratęsė sisteminę literatūros, susijusią su pranešimų apie kibernetinius incidentus poveikiu akcijų kainai analize. Analizuojamu laikotarpiu nuo 2003-2015 m. atrinko 37 straipsnius. Autoriai teigia, kad tyrimų apie kibernetinio saugumo užtikrinimą yra pakankamai daug, tačiau kibernetinių incidentų poveikis nėra pakankamai ištirtas. Jie atskleidžia 37 akademinius darbus, kuriuose nagrinėjamos ekonominės kibernetinių incidentų pasekmės. Didžioji dauguma šiame tyrime nagrinėtų darbų (71 proc.) parodė, jog akcijų vertė sumažėjo dėl neigiamų įvykių, kurie buvo susiję su kibernetiniais incidentais.

Smith (2019) atliko tyrimą kibernetinių incidentų tematika, kurioje mokslininkė atsako į du klausimus – pirmasis, kaip veikia listinguojamų įmonių akcijas naujienos apie kibernetinius incidentus, o antrasis, kaip paveikia klientus. Tyrime analizuota dešimties įmonių akcijų vertės pokyčiai įvykio analizės metodu, autoriai gautus rezultatus lygino su „Down Jones" indeksu. Nustatyta, kad akcijų kainos buvo neigiamai paveiktos visais nagrinėtais laikotarpiais, ypač trečią dieną po pranešimo. Didžiausios reakcijos akcijos kainai sulaukta sveikatos paslaugų sektoriuje. Atsakant į antrąjį klausimą autoriai konstatuoja, kad milijonai asmeninių klientų duomenų, įskaitant kreditinių kortelių duomenis buvo nutekinti dėl žmogiškosios klaidos. Reziumuojant, tyrėjai siūlo įdiegti informacinio saugumo valdymo sistemą, kad pastoviai būtų kontroliuojama informacinė sauga. Taip pat siūlo kruopščiai atrinkti darbuotojus, neturi būti įgoruojami net menkiausi įtarimai apie įsilaužimus. Galima sutikti su autoriais, kad prevencija yra pigesnė už pasekmių išlaidas.

Kibernetiniai incidentai siejami su neautorizuotais prisijungimais prie svetimų tinklų, tinklalapių ir momentiniu paslaugų nebeveikimu, konfidencialumo spragų įtakotais duomenų pažeidimais bei kitais panašiais nusikalstamais veiksmais. Duomenų pažeidimų ataskaitose tokios veiklos įvardijamos kaip „kenkėjiškos programos", „įsilaužimas", „duomenų vagystės" ir „žmogiškosios klaidos" (Spanos ir Angelis, 2016). Tarp duomenų vagysčių dažniausiai minima socialinių draudimo numerių, banko sąskaitos numerių ir medicininės informacijos užvaldymas.

2 lentelė. Didžiausios duomenų vagystės įvykdytos 2013-2019 m. pagal įmonių rinkos segmentą.

Metai	Verslo įmonės	Medicinos įstaigos	Mokymo įstaigos	Banko, kredito ir finansų institucijos	Valstybinės, karinės
2013	194	271	54	35	60
2014	263	332	57	38	91
2015	312	275	58	71	63
2016	497	373	97	51	72
2017	907	384	128	134	79
2018	575	369	78	135	100
2019	644	525	113	108	83

Pastaba. Sudaryta pagal statista.com

Verslui sparčiai persiorientuojant į darbą su šiuolaikinėmis technologijomis, visada bus silpnų vietų, dėl kurių pažeidžiamumo, kibernetiniai incidentai neišvengiami. Pakankamai daug pavyzdžių galima pateikti apie nukentėjusias įmonės nuo kibernetinių incidentų –„Target“, „Depot“, Yahoo“, „JPMorgan“, „Equifax“ ir daugelis kitų, gerai žinomų, organizacijų.

Kalbant apie įmones, kurių akcijomis prekiaujama biržoje, pažeidžiamiausi pramonės sektoriai – mažmeninė prekyba, finansai, sveikatos priežiūra ir smulkusis verslas – konstatuojama Kalifornijos valstijos kibernetinių incidentų ataskaitoje, kuri apima 2012-2015 m.(Harris 2016). Tiek mažmeninės prekybos parduotuvių operacijose, tiek sveikatos priežiūros įrašuose pateikiama daugybė asmeninės informacijos. Technologijomis grįsta mažmeninė prekyba bei sveikatos apsaugos organizacijos yra puikus programišių taikinys (Smith ir kt., 2019).

Finansinio sektoriaus įmonės, kurių akcijomis prekiaujama biržoje patiria stipresnes kibernetines atakas nei kitų sektorių įmonės (Colivicci ir Vignaroli, 2019). Šie mokslininkai analizavo 277 pranešimų apie kibernetinius incidentus įtaką įmonės akcijų kainoms. Tyrime sukurtas akcijų portfelis, kurį sudarė panašios finansinio sektoriaus įmonės kaip ir tos, kurios buvo patyrusios kibernetinius incidentus. Šiame modelyje stebėta skirtingą grąžos koreliacija ir prieita išvados, kad finansinių įmonių akcijos turi didesnes neigiamas perteklines akcijų grąžas.

Statistika rodo, kad atvejų kiekis JAV verslo įmonėse nuo 2013 m. išaugo šešis kartus. Pagal šiuos statistinius duomenis dažniausiai atakuojamos verslo įmonės bei medicinos įstaigos.

2.2. Kibernetinių incidentų tipai bei susiformavimo prielaidos

Egzistuoja daugybė elektroninių nusikaltimų rūšių, kurios nuolat kinta, jų kiekis auga kartu su besivystančiomis technologijomis. Įmonės privalo saugoti duomenis ir nuolat tobulinti kibernetinių incidentų prevencijos būdus. Informacinių technologijų eros pradžioje nebuvo įstatymų, kurie baustų programišius. Tik po stambių kibernetinių incidentų buvo pripažinta, kibernetiniai incidentai būtų pripažinti nusikalstama veikla. Skirtingi autoriai grupuoja kibernetinių incidentų tipus labai įvairiai, tačiau visi vardina tuos pačius veiksmus. 3 lentelėje išvardinti susisteminti keli pagrindinai kibernetinių incidentų tipai.

Galima vardinti daugybę apgaulių, susijusių su kibernetiniu nusikalstamumu, kurios paliečia ir verslo subjektus, ir privačius asmenis. Prieš kelis dešimtmečius kibernetinius incidentus vykdė pavieniai asmenys ar mažos grupuotės, tačiau dabar kibernetiniai nusikaltimai vysta stambiais, anksčiau, nevykusiais mastais.

Pasaulio ekonomikos forume (2019) teigiama, kad rizikos, susijusios su kibernetiniu saugumu, duomenų pažeidimais tampa visuomenės krize. Atsiradusi pažangesnė technologija, debesų kompiuterija keičia informacinių technologijų naudojimą.

Organizacijos keičia tradicinius verslo modelius į skaitmeninį verslą, kuriame diegiamos aukšto lygio technologijos – debesų kompiuterijos, dirbtinio intelekto, didžiųjų duomenų, internetinių daiktų, mobiliųjų ir socialinės žiniasklaidos panaudojimo. Toks verslo modelis tampa visiškai priklausomas nuo informacinių technologijų – nebelieka ribos tarp fizinio ir skaitmeninio pasaulio kaip ir tarp saugumo ir verslo. Technologinis pokytis pakeitė pavienius saugumo klausimus į strateginius verslo

saugos sprendimus, kurie turi būti valdomi, antraip, atsiranda didžiulė tikimybė kibernetiniais išpuoliais rimtai paveikti organizaciją (Horne ir kt. 2017).

3 lentelė. Kibernetinių incidentų tipai.

Kibernetinis incidentas	Aprašymas
Kompiuterių virusai	Kenkėjiškos kompiuterių programos, kurios plinta savaime ir įgauna epidemijos mastus. Sunaikina ar sugadina kompiuteriuose esančią informaciją, gali atlikti atakas prieš kitus kompiuterius, nulemti tinklų perkrovas ar net perimti kompiuterio valdymą.
Botnet tinklai	Kenkėjiškos programinės įrangos sudaryti tinklai, kurie susidaro užkrėtus kitus kompiuterius, vėliau panaudojant atakoms vykdyti
Kibernetinis terorizmas	Atsitinka, kai teroristai pakenkia ar sugadina elektronines sistemas.
Elektroninės vagystės ir sukčiavimas	Sukčiavimo forma prieš organizacijas ir privačius asmenis, kuria siekiama užvaldyti klientų sąskaitas banke, prieš tai apgaulės būdu išviliojus prisijungimus. Viso to siekiama pasitelkiant elektroninius laiškus ar netikrus tinklapius
Kenkėjiška programinė įranga „Malware“	Įdiegtos pačios surenka ir persiunčia reikalingus duomenis –fiksuoja klaviatūros mygtukų paspaudimus. Platinamos su nemokama programine įranga, el. laiškais ir pan.
Įsilaužimas	Įvyksta kai nusikaltėliai, apeidami sistemos slaptažodžius, saugumo priemones, neteisėtai prisijungia prie kitų kompiuterių duomenų. Dažniausiai pasinaudojama saugumo spragomis – neapsaugotais interneto tinklais ar sistemomis.
Šnipinėjimo programos „Hacking“	Programinė įranga, kuri gali būti įdiegta į kompiuterį, išmaniuosius įrenginius, siekiant rinkti informaciją apie įrenginių naudotojus be jų žinios.
Elektroninė banko kortelių apgaulė	Nelegalus veiksmas elektroninėje erdvėje, kai pasinaudojus kito asmens banko kortelės numeriu perkamos prekės elektroninėse parduotuvėse.

Debesų kompiuterija – paslaugos, kurioms patekti reikalingas tik interneto ryšys (Vikipedija). Įmonių atžvilgiu tai paslaugos už kurias mokama pagal reikalavimą, nebereikia investuoti informacinių technologijų personalą, nes už paslaugų priežiūrą atsakingi debesų kompiuterijos paslaugų tiekėjai, gali gauti prieigą prie naujausių modelių. Įprastai debesų saugyklose laikomi duomenys yra pakankamai saugūs. Tačiau ir šios technologijos gali turėti saugumo spragų. Debesų aplinka nėra visiškai apsaugota nuo įvairių trikdžių, gedimų ar įsilaužėlių.

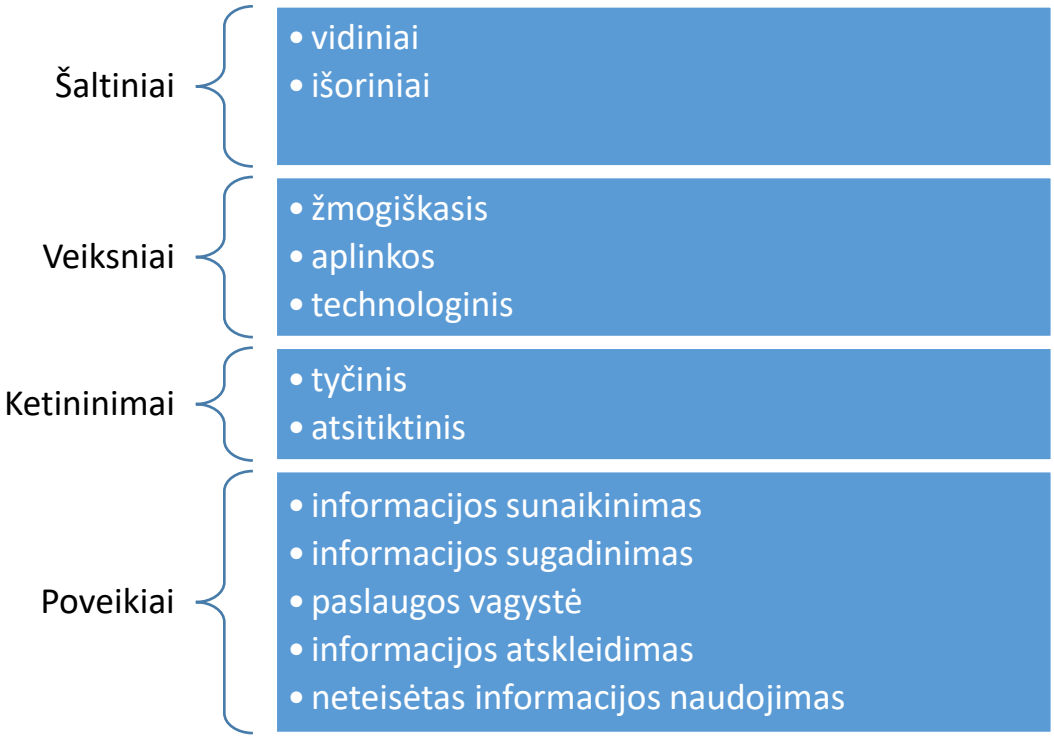
Dauguma įmonių, organizacijų, valstybinių institucijų senas informacines sistemas keičia į debesų kompiuteriją. „Microsoft“, „Google“, „Amazon“, „Oracle“, „Alibaba“ – lyderiaujančios organizacijos keičia tradicines informacinių technologijas į debesų kompiuteriją. Nors debesų kompiuterija teikia pakankamai privalumų – verslo mobilumas, sąnaudų mažinimas, greitesnė verslo pradžia (Chang ir kt. 2019), tačiau tai reiškia, kad paslaugos tiekėjas savo infrastruktūroje laiko kitų įmonių duomenų turtą. Ši priežastis gali vartotojams sukelti riziką, kurios jie nebegali kontroliuoti. Dėl šios rizikos galimai atsiradę duomenų pažeidimai gali sukelti intelektinės nuosavybės vagystes, fizinio saugumo grėsmes, duomenų praradimus Hasbini ir kt. (2018), Higgs ir kt (2016), Horne ir kt. (2017), Kaušpadienė ir kt. (2017).

Naujausios technologijų galimybės, kai mobiliųjų programėlių pinigų pervedimams naudojimas leido įsigalėti naujiems kibernetiniams nusikaltimams. Debesies naudojimas atvėrė ne tik naują duomenų saugojimo būdą, bet ir suteikė programišiams naują erdvę informacijos vagystėms. Kenkėjiška programinė įranga išlieka pagrindine grėsme, tačiau įsitvirtina naujos kibernetinės grėsmės, kurios vykdomos nutolusiuose kompiuteriuose, perimant visišką sistemos valdymą, leidžiančią įdiegti

kenksmingus kodus. Galima konstatuoti, kad besikeičianti elektroninio verslo aplinka, senų technologijų atnaujinamas, verslo perėjimas į skaitmeninę erdvę, greitas informacijos srautas, leidžiantis žaibiškai paskleisti virusus, nesustabdoma ir prisitaikanti programišių veikla – rizikos, kurioms esant vis labiau įsigali kibernetiniai incidentai. Kibernetiniai incidentai, kaip jau buvo minėta anksčiau literatūros analizėje, sukelia rimtus finansinius nuostolius. Kovoje su kibernetiniais incidentais ir jų pasekmėmis, labai svarbu žinoti programišių taktiką, metodus ir suprasti panaudotų technologijų veikimą. Žinant šiuos atsakymus, atsiranda aiškesnis suvokimas kas slepiasi už šių atakų ir kaip jų išvengti. Visa tai reikalauja ypatingo informacinių technologijų išmanymo ir nuolatinio tobulėjimo.

Informacinių technologijų ekspertams svarbu suprasti kaip duomenis pažeidžia kibernetiniai incidentai, kurie duomenys tampa dažnu taikiniu ir kokius saugos sprendimus pritaikyti, kad apsisaugoti ateityje nuo panašių atakų Kaip (Jouini ir kt., 2014).

Norint apsaugoti turtą, reikia išsiaiškinti kokio tipo kibernetinis incidentas įvykdytas, suprasti kaip veikia ir iš kokių šaltinių patenka, todėl kibernetiniai incidentai grupuojami. Grupavimas padeda suprasti kiekvieno incidento poveikį įmonės turtui bei atakos vietą, t.y. į kuriuos duomenis dažniausiai taikomasi. Visa tai leidžia informacinių technologijų ekspertams kurti ir pritaikyti saugos sprendimus (Hasbinin ir kt., 2018). Žinojimas kaip veikia kibernetiniai incidentai, kas ir kodėl sukelia, leidžia kurti sistemas, kurios užkirstų kelią galimoms atakoms ateityje. Vis tai leistų investuotojams palankiai vertinti įmonės perspektyvas. 2 paveiksle parodyta kibernetinių incidentų susiformavimo prielaidos.



2 pav. Kibernetinius incidentus lemiantys veiksniai

Sparčiai plintant kenkėjiškai programinei įrangai, įvairūs virusai, „trojanai“, išpirkos reikalaujantys virusai („Ransomware“) yra platinami el. paštu, socialinius tinklus, mobilias programėles. Tokių

poelgių ketinimai ir motyvai irgi labai įvairūs – siekimas neteisėtos finansinės naudos, nesąžiningo pranašumo prieš konkurentus, siekimas paveikti politinius, ekonominius įvykius.

Kibernetinės grėsmės dažnai kyla iš organizacijos vidaus – dažniausiai žmogiškasis veiksnys (Hwang ir kt., 2017) ir iš išorės – įvairios kenkėjiškos programos. Vidiniai ir išoriniai įsilaužimai turi skirtingus motyvus ir metodus kaip pasiekti įmonės duomenis. Išoriniai – aukštos kvalifikacijos, veikia organizuotai, pakankamai novatoriški ir turi tyčinį ketinimą.

Vidiniams šaltiniams priskiriami darbuotojai, kai dėl jų kaltės, turint prieigą prie serverių, tinklų, pažeidžiamas saugumas. Dažniausiai manipuliuojama patiklumu, baime, neapdairumu ar žinių trūkumu. Neatsakingi ar neapmokyti darbuotojai yra viena iš dažnesnių kibernetinių incidentų priežasčių (Evans ir kt., 2019). Žmogiškasis faktorius gali kelti didesnį pavojų nei nuolat besikeičiančios, stiprėjančios kenkėjiškos programos. Kibernetiniai įsilaužėliai nors ir kuria kenkėjiškas programas, taiko aukščiausias technologijas, tačiau lengviausias įsilaužimo būdas – žmogaus prigimtis, vis dar išlieka. (Hwang ir kt., 2017)

Atidarytas laiškas, paspausta nuoroda, silpni raktažodžiai, apgaulingi ir klaidinantys elektroniniai laiškai, žinutės socialiniuose tinkluose su kenkėjišku kodu, netgi netikri techninės pagalbos skambučiai ar palikta atminties kortelė, kenkia įmonės kibernetiniam saugumui ir gali būti kibernetinio incidento priežastimi (Evans ir kt. 2019).

Žmogiškasis faktorius – 2018 m. Lietuvos nacionalinio kibernetinio saugumo ataskaitoje įvardijamas socialinės inžinerijos terminu. Šioje ataskaitoje teigiama, kad didžiausia socialinės inžinerijos grėsmė kyla naudotojams, kurių kibernetinio saugumo ir informacinių technologijų raštingumas yra žemo lygio, o įmonėms dėl šių incidentų praradusios konfidencialią informaciją, patiria tiesioginius finansinius nuostolius.

Mokslininkai tyrimuose ieško atsakymo, kiek žmogaus klaidos gali lemti duomenų saugumo pažeidimus. Evans‘as ir kt. (2019) atliko tyrimą siekdami nustatyti kokią apimtį sudaro socialinė inžinerija kibernetinių atakų plotmėje. Kadangi vienas iš pagrindinių kibernetinių incidentų veiksnių – žmogiškasis faktorius atskleidžia technologijų raštingumo spragas, atsiranda siekis susisteminti kibernetinių įsilaužimų informaciją, nustatant dažniausius pažeidimus padaromus žmogaus. Atlikus empirinį tyrimą, kurį sudarė 7202 kibernetinių incidentų imtis, paaiškėjo, kad 64 proc. visų įvykių tikrai priklausė nuo žmogaus veiklos ir 36 proc. – galimai buvo priklausomi nuo žmogiškojo faktoriaus. Autoriai, palyginę tyrimą su kitų mokslininkų tyrimais konstatuoja, kad net 99 proc. kibernetinių atakų yra galimai paremtos žmogiškojo faktoriaus grėsme.

Organizuoti ir sudėtingi išpuoliai prieš organizacijas nesikartoja kasdien, tačiau kasmet jų atsitinka dažniau. Net ir kenkėjiškų programų patekimo į organizacijos informacines sistemas atveju dalyvauja neatsargūs darbuotojai. Pripažįstama, kad kibernetiniai incidentai, susiję su vidiniais šaltiniais yra sunkiausiai užkertami (Hwang ir kt., 2017; McLeod ir Dolezel, 2018).

Aplinkos veiksniams priskiriama ne žmogaus sukelti pavojai – stichinės nelaimės, gaisrai, žaibai, žemės drebėjimai ar kitokios gamtos sukeltos stichijos, kurios daro didelę žalą informacinėms sistemoms. Prie aplinkos veiksnių priskiriama karai, teroristų atakos, riaušės.

Technologinius veiksnius gali sukelti fiziniai procesai, kurių metu gali būti įsibraunama į apsaugotus pastatus, patalpas, ar kitą aplinką. Įsibrovus pavagiama ar sugadinama kompiuterinė įranga, programos, atjungiami maitinimo šaltiniai ir pan.

Atakos turi ketinimus ir tikslus, kurie tampa kenkėjiškais (angl. malicious) arba nekenkėjiškais (angl. Non-malicious) rezultatais.

Kenkėjiškas grėsmės – virusai, kirminai, „Trojos arkliai“ kyla ir iš vidaus, ir iš išorės. Tai dažnu atveju lemia žmogiškasis faktorius – mažai apmokytų, neatsakingų darbuotojai ar savininkų klaidos (Evans ir kt., 2019).

Dėl prastos apsaugos strategijos ir silpnos kontrolės atsiranda saugos spragos, dėl kurių kyla nekenkėjiškos atakos. Darbuotojai, nenorėdami gali tapti tarpine grandimi, kuri padeda įvykdyti atakas prieš įmonės informacines sistemas.

Sėkmingas“ kibernetinis incidentas gali sukelti įvairius neigiamus tiesioginius ir netiesioginius padarinius. Tiesioginiai poveikiai dažniausiai susiję su informacijos praradimu, sunaikinimu, atskleidimų ir pan.

Informacijos sunaikinimas siejamas su tyčiniu sistemos komponentų sunaikinimu, norint nutraukti sistemos darbą.

Informacijos sugadinimas siejamas su informacijos perrašymu, pakeitimu ar kenkėjiškos programos įkėlimu per spragas naršyklėse ar pateikiant kaip naudingą programą.

Informacijos atskleidimas siejamas su informacijos perdavimu asmenims, kurie neturi teisės šia informacija disponuoti.

Paslaugos vagystė siejama su neteisėtu kompiuterio ar tinklo naudojimu, kai prisijungia pašaliniai naudotojai. Šie naudotojai gauna padidintas administravimo privilegijas ir tuomet gali įvykti tyčinis kompiuterio ar tinklo blokavimas, išteklių sunaikinimas. Neteisėtas naudojamas vyksta tuomet, kai kibernetiniam incidentui inicijuoti naudojamos įprastos sistemos, kurios turi saugos spragų. Pasinaudojus jų galimybe yra atliekami neteisėti veiksmai.

2.3. Kibernetinių incidentų poveikis verslo subjektams ir investuotojų sprendimams

Besikeičiantis kibernetinis nusikalstamumas tapo realia ir pavojinga grėsme įmonėms, kurių akcijomis prekiaujama biržoje. Be verslo galimybių praradimo, suinteresuotų šalių pasitikėjimo praradimo ir akcijų vertės pokyčių, kyla ir ilgalaikiai, nenuspėjami iššūkiai, kurie reikalauja didesnių investicijų į kibernetinių incidentų prevenciją bei atkuriant investuotojų pasitikėjimą įmone (Evans ir kt., 2019) Dėl tokių netiesioginių padarinių, kaip klientų, partnerių finansiniai ir nuostoliai dėl reputacijos, gali tekti mokėti bylinėjimosi išlaidas, baudas valstybei, todėl kibernetiniai incidentai riboja įmonės produktyvumą, inovacijų galimybes, konkurencinį pranašumą (Hasbini ir kt., 2018; Higgs ir kt., 2016). Taip pat kibernetinės atakos gali sukelti staigią neigiamą rinkos reakciją ir turėti esminės įtakos įmonės finansinei būklei, pinigų srautams (Higgs ir kt., 2016).

Amir ir kt. (2018) tyrimui pasitelkę alternatyvų kibernetinių atakų padarytos žalos vertinimą, pastebėjo, kad informacija apie sunkesnes atakas yra sulaikoma, t.y. stengiamasi, kad nebūtų prieinama iki tam tikro laiko. Mokslininkų grupė pasitelkę nukentėjusių įmonių paskelbtus žalos įvertinimus bei objektyvų indeksą, kuriuo matuojamas kibernetinių išpuolių „stiprumas“ palygino

laiko tarpą nuo įvykio atsitikimo iki paskelbimo viešai. Tyrimas parodė, kad įmonės užlaiko pranešimus apie stipresnio poveikio kibernetines atakas palyginus su švelnesnio poveikio. Kibernetinės atakos dažnai nepastebimos visuomenei, todėl atsakingi asmenys, dėl savanaudiškų tikslų, gali neskubėti pranešti informacijos viešai. Mokslininkai suskirstė kibernetinius išpuolius pagal pranešimo pobūdį į dvi grupes:

- kibernetines atakas, kurias atskleidė pati įmonė;
- kibernetines atakas, kurios buvo nuslėptos, o vėliau išaiškintos išorinio šaltinio.

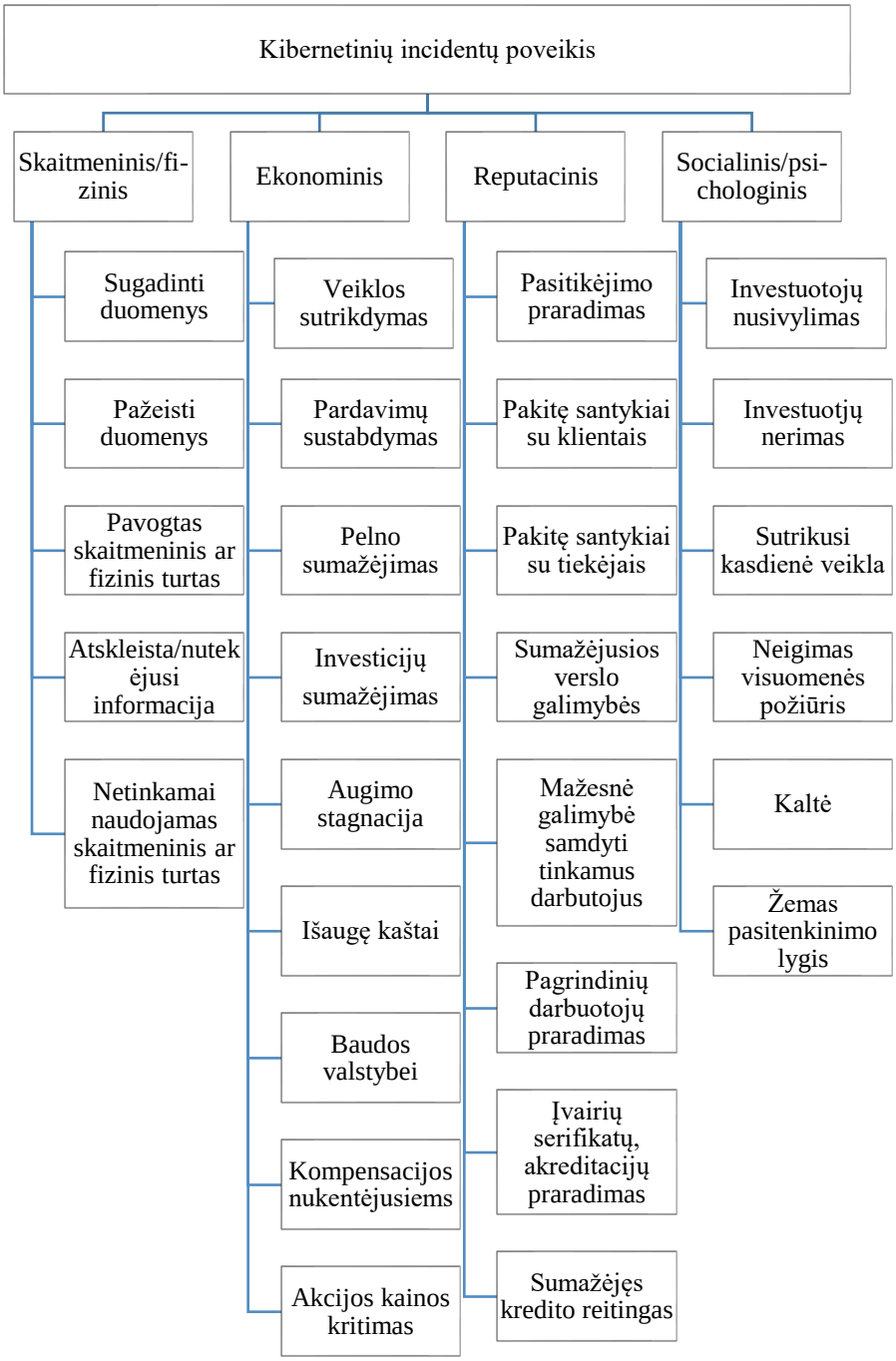
Nustatyta, kad rinkos reakcija į atskleistus išpuolius nebuvo labai reikšminga, tačiau rinkos reakcija į nuslėptus, bet vėliau atskleistas atakas yra neigiama ir reikšminga. Tokios išvados rodo, kad vadovai linkę atskleisti lengvesnio pobūdžio, o uždelsti pranešti apie sunkesnes kibernetines atakas. Taip pat šie mokslininkai konstatuoja, kad tik esant 40 proc. tikimybei, jog investuotojai atskleis įvykusį išpuolį, įmonės priima sprendimą paviešinti kibernetinio incidento faktą. Jei tikimasi, kad apie kibernetinius incidentus išoriniai vartotojai nesužinos, tuomet yra tikimybė, kad informacija bus užlaikyta. Šis tyrimas parodė, kad viešas informacijos atskleidimas apie smulkius kibernetinius įsilaužimus yra retas reiškinys.

Kibernetinių incidentų poveikis aprašomas mokslininkų darbuose yra plataus spektro – nuo skaitmeninio-fizinio iki socialinio-psichologinio (3 pav.). Susisteminta informacija apie kibernetinių incidentų poveikį leidžia aiškiau suvokti kokiu mastu paveikiama įmonės veikla ir yra pirminė informacija prevencinių saugumo sistemų kūrimui. Dažnai nesureikšminami poveikio elementai kaip psichologiniai-socialiniai yra svarbūs, norint tinkamai įvertinti kibernetinio incidento poveikį.

Kiekvienas kibernetinio incidento poveikio elementas pavaizduotas 4 paveiksle turi ryšį su kitu elementu ir galima pavadinti kibernetinio incidento poveikio verslo subjektams grandine. Nutekinti duomenys yra pradinė visos žalos grandinės dalis ir tai yra pirminis programišių tikslas. Šioje grandinės dalyje sugadinami, pasisavinami, duomenys, sutrikdoma informacinių sistemų veikla ir atliekama panaši veikla aprašyta šio skyriaus 2 poskyryje.

Toliau seka antroji poveikio įmonei grandinės dalis – ekonominė žala. Po vienaip ar kitaip nutekintų duomenų, sutrikdytų serverių darbo, sutrinka procesų veikla, t.y. procesai nebeveikia normaliu darbo režimu. Šiuo atveju pagrindinis tikslas yra kuo greičiau atkurti normalų procesų veikimą, užtikrinant kuo mažesnį žalos poveikį įmonei. Užsitęsus ar nepavykus teisingai atkurti darbo režimo, sutrinka pardavimai (jei tai elektroninės komercijos įmonė), kurie generuoja apyvartas ir pinigų srautus. Klientai, nebegalėdami prisijungti prie įmonės pardavimo sistemų ar sistemoms dirbant apsunkintu režimu, ieško reikalingų prekių ar paslaugų pas konkurentus. Tai reiškia, kad įmonė gali netekti klientų, kuriuos susigrąžinti ir neprarasti konkurencingoje verslo aplinkoje gali ir būti didelis iššūkis. Nuo kliento lygmens kibernetinių incidentų žalos grandinėje perėjus prie įmonės lygmens kibernetinių incidentų poveikio mastas tik plečiasi. Netekus apyvartų įmonės pelnas gali sumažėti drastiškai, o įmonėje prasidėti recesija, t.y. augimo sulėtėjimas nebegaunat investicijų iš išorinių šaltinių. Galiausiai šios ekonominės žalos grandinės dalyje investuotojai, matydami aukščiau išvardintus drastiškus pasikeitimus įmonės veiklos grandinėje, gali priimti ypač nepalankius sprendimus investuojant, kas iššauktų staigų akcijų kainų sumažėjimą.

Kibernetinių incidentų tyrimas gali užtrukti ne vienerius metus, todėl papildomi kaštai atsiranda tyrimo metu specialistams, nukentėjusių klientų kompensacijoms, galbūt, išpirkos mokestis, kad galėtų tęsti veiklą, o galiausiai baudų mokėjimams.



3 pav. Kibernetinių incidentų poveikio įmonės veiklai schema

Pastaba. Parengta pagal Hasbini ir kt., 2018; Higgs ir kt., 2016; Hwang ir kt., 2017; McLeod ir Dolezel, 2018; Rebollo ir kt., 2015.

Svarbi poveikio po kibernetinio incidento grandinės dalis yra reputacija. Reputacijos praradimas gali būti stiprus smūgis įmonei, kadangi reputacija kuriama ilgą laiką, skiriamos didelės pinigų lėšos įvaizdžiui gerinti, tačiau ir taisyti reputacijai gali prireikti išleisti pakankamai nemažai lėšų. Konkurencija rinkoje didžiulė, todėl klientai visada perka prekes ar paslaugas tik iš tų įmonių, kuriomis yra pasitikima labiausiai. Atsitikus kibernetiniam incidentui, dėl kurio buvo nutekinti konfidencialūs klientų ar partnerių duomenys, neišvengiamai nukenčia įmonės reputacija. Dėl neigiamo visuomenės požiūrio sumažėja įmonės prestižas. Savaime aišku, pašlyja santykiai su

klientais ir tiekėjais. Susidariusios šioms neigiamos verslo galimybės veda į sulėtėjusią plėtrą ir augimą (ekonominis poveiki).

Svarbus faktas yra praradimas svarbių darbuotojų, kurie paliko įmonę ar buvo atleisti. Taip pat darbo rinkoje esančių aukštos kvalifikacijos profesionalų nepasitikėjimas įmone, kurių įmonė negali samdyti dėl šių aplinkybių, t.y. sunku pritraukti ir įdarbinti tinkamus darbuotojus, kurie galėtų užtikrinti nenutrūkstamą organizacijos veiklą ateityje.

Reputacijos veiksniams galima priskirti ir padidintą žiniasklaidos dėmesį, kai nuolat pateikiami nauji faktai, kurie ne visada gali būti teisingi ir taip atkreipiamas dėmesys į įvykusį kibernetinį incidentą, kas vėl galėtų skatinti iracionalus investuotojus elgtis neadekvačiai akcijų biržoje perkant ar parduodant įmonės akcijas. Taigi reputacijos veiksnių grandinė, susidaranti iš įvairių prielaidų, sukuria galutinį ryšį su galimu akcijos kainų pokyčiu.

Galiausiai socialiniai-psichologiniai veiksniai tokie kaip investuotojų nusivylimas, nerimas veda prie ekonominių žalos elementų. Sutrikusi kasdieninė veikla kelia susirūpiną ne tik klientams, bet ir darbuotojams, atsiradusi įtampa nepalengvina sprendimų priėmimo.

Svarbu suprasti kibernetinio incidento žalos plitimo tendencijas. Išvardinti žalos grandinės elementai leidžia susidaryti aiškų kibernetinio incidento poveikio schemą, iš kurios galima formuluoti išvadas, kokia reikšminga žala gali susiformuoti vėlesniuose incidentuose.

Labai svarbus investuotojo požiūris į poveikio grandinės elementus, priimant investavimo sprendimus. Pastebėta, kad dažnai tiriamas ryšys ne tik tarp akcijų viršpelnių, kurie susiformuoja paveikti įvairių veiksnių, bet tyrimuose stebima kaip reaguoja į pranešimus skirtingos investuotojų grupės Westerholm ir kt. (2016), Barron ir kt. (2018), Jin ir kt. (2019). Rinkos dalyviai, investuojantys akcijų rinkoje siekia naudos su jiems priimtinu rizikos lygiu. Investuotojai geba prognozuoti ir priimti sprendimus, tačiau jie yra subjektyvūs.

Investuotojus, pagal kilmę, galima suskirstyti į dvi stambias grupes: individualūs investuotojai – neprofesionalai ir instituciniai investuotojai – profesionalai.

Individualūs investuotojai tai asmenys, kurie neturi profesionalaus pasiruošimo, tačiau valdo patys ar padedant finansų makleriams savo investicijų portfelį. Investuoja privačias laisvas lėšas, norėdamas uždirbti pelno iš akcijų prekybos.

Instituciniai investuotojai – tai investuojančios įmonės, valstybiniai, juridiniai vienetai ir įvairios institucijos. Šių investuotojų investicijos valdomos aukšto lygio profesionalių investuotojų. Jų veikla apribota taisyklėmis ir procedūromis, investuoja didesnes sumas nei individualūs investuotojai, ir dažniausiai investuoja į likvidžias vertybinių popierių emisijas. Šie investuotojai gali turėti turi didelę įtaką administruojant įmonę dėl stambaus akcijų paketo įsigijimo.
Instituciniai investuotojai:

- fondai,
- draudimo kompanijos,
- komerciniai ir investiciniai bankai,
- finansų maklerio bei valdymo įmonės,
- kitos įmonės ar valstybinės institucijos.

Westerholm‘as ir kt. (2016) Australijos akcijų rinkoje yrė institucinių ir individualių investuotojų prekybos apimtis, kurios galėjo būti paveiktos įmonių pranešimų. Duomenis stebėjo dienos prekybos bėgyje kas penkias minutes. Pranešimų laikas irgi buvo fiksuojamas. Gauti rezultatai praplėtė suvokimą apie individulių ir institucinių investuotojų prekybos apimtis prieš pat ir iškarto po pranešimų paskelbimų. Tyrimo rezultatai rodo reguliuojamos informacijos atskleidimo poveikį individulių ir institucinių investuotojų prekybos apimtims. Šiame tyrime nustatyta, kad individualūs investuotojai vykdo intensyvesnę prekybą akcijomis po pranešimų, o instituciniai investuotojai intensyviai prekiauja ir prieš, ir po pranešimų. Galiausiai tyrimo autoriai pabrėžia, kad tiek individualių, tiek institucinių investuotojų pirkimo apimtys būna didesnės nei pardavimo, rinkoje esant optimistinėms nuotaikoms, sklindančiu tikėjimu augimu ateityje.

Jin ir kt. (2019) atliko panašų tyrimą, kuriuo stebėjo ryšį tarp akcijų kainų pasikeitimų ir vietinių bei užsienio investuotojų elgesio, kai buvo skelbiami pranešimai apie įsigijimus ir susijungimus Korėjos rinkoje. Rezultatai parodė, kad vietiniai investuotojai linkę parduoti akcijas dėl didesnės grąžos, o užsienio investuotojai, atvirkščiai, perka dėl to paties poreikio.

Galima teigti, kad atliktų tyrimų analizė rodo, kad individualūs investuotojai yra mažiau informuoti nei instituciniai. Tačiau Korėjos tyrime Jin ir kt. (2019) liko neaišku koks yra santykinis užsienio ir vietinių institucinių investuotojų informuotumas šios šalies akcijų rinkoje.

Skirtingi investuotojai renkasi vis kitokią investavimo strategiją, prisiimant numatytą riziką. Kylančios akcijų kainos rodo investuotojų tikėjimą rinka, krintančios – atvirkščiai. Kaip jau minėta anksčiau, akcijų kainas lemia ne tik makroekonominiai veiksniai. Dažnai labai specifiniai įvykiai įmonės veikloje, tokie kaip kibernetiniai incidentai, gali nulemti investuotojų tikėjimą arba pesimizmą akcijų ateitimi. Keičiantis verslo aplinkai, labiau prisitaikant prie rinkos poreikių, pranešimai apie kibernetiniu incidentus, kurie anksčiau kėlė nedaug susirūpinimo, tampa stipriu išbandymu organizacijų veikloje.

Per pastarąjį dešimtmetį eksponentine kreive išaugo surinktų, apdorotų ir saugomų įvairiausių įmonių duomenų. Tokia tendencija tęsis ir artimiausius metus (Rossati, 2017). Duomenų analitika keičia daugelį pramonės šakų – sveikatos apsaugą, bankininkystę, finansus, žiniasklaidą. Duomenys dažnai yra konfidencialūs ir vertingi, todėl traukia kibernetinių nusikaltėlių dėmesį. Todėl auga kibernetinių incidentų skaičius ir tuo pačiu išlaidos jų padariniams kompensuoti.

2.4. Informacijos saugumo sistemos svarba investuotojų požiūriu

Technologijoms sparčiai augant, investuotojai teigiamai vertina įmones, kurios turi aiškų, ateities perspektyvomis parengtą informacinių technologijų naudojimo planą. Tačiau tokios įmonės, bekaupdamos įvairiausius duomenis elektroniniuose serveriuose, susiduria su problema kaip apsaugoti turimus duomenis ir neprarasti įgyto konkurencingumo, įvykus nenumatytam įvykiui – kibernetiniam incidentui. Naudojantis internetu ne visada patiriamos mažiausios išlaidos, kadangi tenka nemažai investuoti į saugumo sistemas. Klientų asmeninių duomenų apsaugojimas yra etinė ir teisinė atsakomybė akcininkų atsakomybė. Investuotojai gali susirūpinti, matydami, kad įmonė mažai ar nepakankamai dėmesio skiria informacinių technologijų ir duomenų saugumui. (Schmith ir kt., 2016).

Įmonės taiko keletą informacijos apsaugos būdų – sistemų autentifikavimas, duomenų šifravimas, vartotojo prieigos kontrolė, ugniasienės. Taip pat, atliekami vidiniai darbuotojų mokymai, kuriuose

mokoma atsakingo elgesio kibernetinėje erdvėje ir veiksmų orientuotų į įmonės informacijos saugumą. Tokia veikla turėtų būti vykdoma visos įmonės mastu, nes pavienės iniciatyvos atskiruose padaliniuose nebeduoda teigiamo efekto, sprendžiant saugos nuo kibernetinių incidentų problemas (Rebollo ir kt. 2015).

Didėjantis kibernetinių incidentų poveikis verčia įmonių valdybas atrasti naujų būdų kaip užtikrinti saugumą ir sumažinti išpuolių skaičių. Vadovų įsitraukimas į įmonės informacijos saugumo strategijos kūrimą yra labai svarbus žingsnis veiksmingos apsaugos sistemos sukūrimo procese. Suprantant kaip veikia grėsmės, koks poveikis laukia įmonės, galima iš anksto sukurti informacijos saugos strategiją, kuri padėtų išvengti plintančių kibernetinių atakų (šio skyriaus 3 skyrelyje kalbėta plačiau apie kibernetinių atakų poveikį).

Strateginis požiūris į informacijos saugumo reiškinį vadinamas informacijos saugumo valdymu (Nicho, 2018). Netolimoje praeityje informacijos saugumui buvo skiriama nepakankamai dėmesio, tačiau didėjant kibernetinių incidentų skaičiui ir augant pasekmėms, įmonės siekia įsidiegti informacijos saugumo valdymo sistemas ir standartus. Tai yra tinkamiausias metodas ne tik kontroliuoti saugumo procesus, bet ir turėti suderinamumą su verslo strategijomis (Rebollo ir kt. 2015). Įmonėje turi būti užtikrinta, kad rizikos būtų tinkamai valdomos, tikslai pasiketi, organizacijos ištekliai atsakingai naudojami. Todėl informacijos saugumo valdymas tampa įmonių strategijos dalimi kovojant su kibernetiniais incidentais.

Informacijos saugumo valdymas susideda iš kontrolės aplinkos sukūrimo ir palaikymo, siekiant valdyti riziką, susijusią su informacijos konfidencialumu, vientisumu ir prieinamumu (Nicho, 2018). Informacinių technologijų valdymas, įmonės valdymas ir informacijos saugumas yra tiesiogiai susiję. Į šį procesą turėtų įsitraukti aukščiausio lygio vadovai ir personalo valdymo komanda. Informacijos saugumo valdymas atliekamas vykdomuoju lygmeniu, kuris susideda iš vadovybės, organizacinių struktūrų ir procesų, susijusių su informacijos išteklių apsauga. Valdybos nariai, turėdami informacijos apie kibernetinių incidentų poveikį įmonės veiklai, gali veiksmingiau įgyvendinti informacijos saugumo valdymo strategijas, skirtas sumažinti vėlesnių incidentų riziką. Informacijos saugumo valdymas priklauso ne tik nuo technologijų, bet ir nuo darbuotojų švietimo, kultūros organizacijoje. Su šiuo teiginiu galima sutikti, kadangi informacijos saugumas organizacijoje apima ir techninius, ir strateginius, ir teisinius klausimus, todėl į informacijos saugumą reikia žvelgti kompleksiškai – kaip įmonės valdymą, kuris apima vadovybės atsakomybę prieš akcininkus.

Įvairios organizacijos kuria savo saugumo strategiją, o tai reiškia, kad vienodi objektai gali būti traktuojami visiškai skirtingai. Siekiant susisteminti kibernetinių ataskaitų pranešimus, JAV atestuotų buhalterių institutas (AICPA, 2017) sukūrė tokių ataskaitų standartizuotą struktūrą. Remiantis šia struktūra, įmonėms yra paprasčiau ir aiškiau atskleisti naudingos informacijos apie saugumo valdymą investuotojams. Sistema sudaryta iš trijų svarbiausių komponentų, kurie padeda investuotojams geriau suprasti įmonės informacijos rizikos valdymą: programos strategijos aprašymas, vadovybės tvirtinimas, kad strategija atitinka buhalterių instituto aprašytus kriterijus, efektyvumo matavimo kriterijus, siekiant kibernetinio saugumo tikslų ir nuomonės apie įdiegto saugumo valdymo veiksmingumą.

Tokia bendra visiems struktūra leidžia suinteresuotoms šalims – įmonei ir investuotojams „susikalbėti“. Tačiau nėra pakankamai aišku kokią įtaką investavimo sprendimams gali turėti žinojimas apie informacijos saugumo valdymo strategiją (Yang ir kt., 2020). Šių mokslininkų grupė

apklausė grupę neprofesionalių investuotojų ir nustatė, kad šių investuotojų sprendimai yra tiesiogiai susiję su pranešimais apie įmonių informacijos saugos strategiją, kuri parengta standartizuotu metodu. Neprofesionalūs investuotojai suvokia tokios standartizuotos sistemos reikšmę ir tyrime atskleista, kad šios prielaidos paveikia palankiai investavimo ketinimus. Reikėtų pabrėžti, kad tokių ataskaitų teikimas ir informacijos saugumo strategijų atskleidimas yra savanoriškas. Investuotojams visada darė gerą įspūdį savanoriškas informacijos atskleidimas, ypač tokiose srityse, kur galėtų turėti poveikį investavimo sprendimams priimti (Chen ir kt., 2016).

Galima daryti išvadą, kad tobulinant veiklos ir administravimo procesus duomenų saugumo atžvilgiu, siunčiamas optimistinis signalas investuotojams. Tačiau investicijų į duomenų saugumą grąža pakankamai sunkiai išmatuojama dėl riboto duomenų prieinamumo ir priklausomybės nuo vadybinių sprendimų. Saugumo sistemų kūrimas ir valdymas yra ne tik metodas, leidžiantis kontroliuoti saugumo procesus, bet yra ir sudėtinė verslo strategijos dalis, esanti greta kitų įmonės tikslų Rebollo ir kt. (2015). Taip pat šie autoriai, kad organizacijos vis dažniau susidurdamos su kibernetiniais incidentais, eina sistemos ir standartų kūrimo keliu.

Informacijos, kaip vertingo turto apsauga neturėtų būti palikta vienam atsakingam asmeniui, o turėtų būti traktuojama kaip valdymo klausimas (Rebollo ir kt. 2015). Su šiuo teiginiu galima sutikti, kadangi informacijos saugumas organizacijoje apima ir techninius, ir strateginius, ir teisinius klausimus, todėl į informacijos saugumą reikia žvelgti kompleksiškai – kaip įmonės valdymą, kuris apima vadovybės atsakomybę prieš akcininkus.

Duomenys yra svarbi intelektinė nuosavybė, todėl įmonės kuria planus ir strategijas, diegia informacijos saugumo valdymo sistemas, kad sumažintų duomenų nutekinimo rizikas, tačiau visada išlieka įsilaužimo ir sukčiavimo grėsmė. Informacijos saugumas, privatumas, neliečiamumas yra lemiantis veiksnys, kuris patvirtina įmonės tęstinumą ir tvarumą (Ahmad, 2019).

2.5. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai tyrimų metodologijos ankstesniuose tyrimuose apžvalga

Mokslinėje literatūroje tyrimams, vertinantiems naujų, netikėtų pranešimų apie įmonę, įtakos akcijų kainų pokyčiams tirti, dažniausiai pasirenkamas įvykio analizės metodas (angl. event study). (Ozo, 2019; Felimban, 2018; Mutuku, 2015; Strauss, 2019). Šiuo metodu paremtų tyrimų istorija siekia 20 a. pradžią, kai 1933 m. James Dalley ištyrė pranešimo apie akcijų padalijimą įtaką akcijų kainai (Dolley, 1993). Vėliau sekė ilga įvykio analizės tyrimų grandinė įvairių mokslininkų darbuose (Myers and Bakay, 1948; Ashley 1962; Ball ir Brown, 1968). Metodas gali būti naudojamas tiek trumpalaikius (Brown ir Warner, 1980; 1985), tiek ilgalaikius poveikius su tam tikrais patobulinimais (Lyon, ir kt., 1999) tirti.

Tyrimams, vertinantiems pranešimų apie kibernetinius incidentus įtaka akcijų kainai, taip pat pasirenkamas įvykio analizės metodas. Kibernetinis incidentas yra įvykis, kuris labai glaudžiai siejasi su įmonės veikla esamuoju momentu ir gali turėti reikšmingos įtakos ateityje. Apie kibernetinių incidentų poveikį įmonei aptarta 2. 3 poskyryje. Šio tyrimo atveju pranešimas apie kibernetinį incidentą yra įvykis, kuris atitinka naujumo, netikėtumo, prieš tai niekam nežinomo įvykio požymius, todėl atitinka įvykio analizės metodo reikalavimus įvykiui.

Įvykio analizės metodo teorinis pagrindas yra efektyviosios rinkos teorija, kurią pristatė, o vėliau ir ištobulino 2013 m. Nobelio premijos laureatas Eugene Fama. Jau XX amžiuje E. Fama (1977) pristatė

efektyviosios rinkos hipotezę (ERH) – rinka yra efektyvi, jei kainos atspindi turimą informaciją. Pagal šią teoriją investuotojai racionaliai vertina akcijų kainas. Racionalumas pasireiškia tuo, kad investuotojai gauna visą naujausią informaciją, kurią panaudoja vertindami akcijų kainas. Veikiant racionaliems rinkos žaidėjams, akcijų kainos išlaiko pusiausvyrą, o rinka yra efektyvi. Tačiau biržoje veikia ir iracionalūs rinkos veikėjai, kurių veiksmų įtaka kainoms yra atsitiktinė. Darant teorines prielaidas, kad nebūtinai visi rinkos žaidėjai tūri būti racionalūs, o jei iracionaliųjų yra pakankamai ir jie veikia nepriklausomai, tai iracionaliųjų veiksmai rinkoje pasiskirsto, o akcijų kainos tampa artimos pusiausvyros kainoms, kas rodo rinkos efektyvumą.

Empirinė analizė tikrina tam tikras išvadas. Dažniausiai nagrinėjama šios išvados:

1. informacijos įtaka akcijų kainai, t. y. atsiradus naujai informacijai, akcijos kaina turi reaguoti ir atspindėti naują informaciją teisingai ir greita reakcija;
2. akcijos kaina negali svyruoti, nes kaina turi sutapti su fundamentaliąja verte iki kol nėra naujos informacijos susijusios su akcijos verte.

Galima būtų paneigti šias išvadas, parodant, kad įmanoma gauti didesnį nei vidutinį pelną, negaunant naujos informacijos. Tačiau reikėtų įvertinti pelną, kuris būna susijęs su rizika. Rizikai vertinti reikėtų rasti papildomų prielaidų, o gautas pelnas galėtų būti įvertintas kaip rizikos kaina. E. Fama (1970) savo kertiniame darbe įvardijo ir išskyrė tris informacijos šaltinius ir iškėlė efektyviosios rinkos hipotezės formas:

1. silpna forma – dabartinės kainos parodo informaciją apie praeities kainas;
2. pusiau stipri forma – dabarties kainos parodo visą šiuo momentu viešai prieinamą informaciją;
3. stipri forma – dabarties kainos parodo visą dabarties visiems prieinamą informaciją kartu su neatskleista vidine informacija.

Racionalios rinkos požiūriu susiformuoja investuotojų elgesio principai – sprendimai priimami nuosekliai ir taip, kad neatsirastų priešprieša su kitais priimtais sprendimais, savanaudiškumo principas – investuotojai ir įmonės siekia gauti didžiausios naudos, investuotojai remiasi visiems vienodai prieinama informacija.

Kaip Fama (1991) teigia, kad viskas kas žinoma apie finansus buvo ištirta pasitelkiant įvykio analizės metodą bei nurodo, kad įvykio analizė geriausiai tinka analizuoti pusiau stiprios rinkos efektyvumą. Taip pat pabrėžia įvykio analizės tinkamumą moksliniuose finansų tyrimuose stebėti kaip veikia vieši pranešimai akcijų rinką (Fama, 1991).

Galima teigti, kad šis metodas sukurtas norint įvertinti nenumatyto įvykio efektą akcijų rinkų pokyčiams. Kaip minėta anksčiau šio tyrimo nenumatytas įvykis – kibernetinis incidentas. Pagal efektyviosios rinkos teoriją visa nauja informacija (pranešimas apie kibernetinį incidentą), kuri gali būti susijusi su įmonės akcijos kaina, tuojau pat yra įtraukiama į įmonės akcijos kainą. Priimant prielaidą, kad rinka yra efektyvi, būtina atsižvelgti į tai, kad joks kitas įvykis (pranešimas), galintis paveikti akcijos kainą, analizuojamojo (kibernetinio incidento) įvykio dienomis nebuvo įvykęs. Atitikus šioms prielaidoms galima interpretuoti akcijos kainos pasikeitimą kaip reakciją į naują pranešimą apie kibernetinį incidentą.

Perteklinė grąža taip pat turi seną tyrinėjimų istoriją siekiant išmatuoti įmonės pasiektus rezultatus, lygį ir kt. ne tik finansų valdymo srityje, bet ir vadyboje (McWilliams ir Siegel, 1997). Šie mokslininkai siūlo tris pagrindines prielaidas, kuriomis remiantis nustatoma perteklinė grąža:

- rinkos efektyvumas (akcijos kainoje atsispindi tik naujausia, finansiškai svarbi informacija),
- nenumatyti įvykiai (pranešimas atskleidžia netikėtus, anksčiau nežinomus atvejus),
- klaidinantis poveikis (tiriamo įvykio poveikį galima atskirti nuo kitų įvykių poveikio).

Įvykis (pranešimas) turi turėti naujos informacijos, galinčios reikšmingai paveikti įmonės akcijų kainą (MacKinlay 1997). Įvairios naujienos gali pakeisti investuotojų prognozes apie akcijų kainą, tačiau kaina gali likti ir nepakitusi. Tačiau stipriai išreikštos geros ar blogos naujienos (pranešimai) gali generuoti teigiamus arba neigiamus ypač reikšmingus pokyčius akcijos kainoje.

Literatūroje, analizuojančioje įvykio analizės metodą (MacKinlay, 1997), išskiriami pagrindiniai etapai, kurie turi būti įvykdyti: Įvykio lango identifikavimas, imties apibrėžimas, akcijų kainų pokyčių skaičiavimas. Po tikslios pranešimo datos nustatymo reikia nustatyti įvertinimo langą ir įvykio lango periodus. T

Įvykio langai – kelios dienos prieš pranešimą ir po pranešimo bei pranešimo diena įvairiuose tyrimuose apibrėžiama labai skirtingais laiko tarpais, kurie vadinami įvykio langu (ang. event window). Analizuojant mokslinius straipsnius pastebėta, kad dažniausiai, reikšmingi akcijų kainų pokyčiai identifikuojami trumpalaikiu periodu – stebima minučių (Westerholm ir kt., 2016; Straus ir Smith, 2019), valandų, dienų (French,_2018), savaitės ar mėnesio intervalų akcijų kainų grąžos. Tyrėjai, norėdami nustatyti pranešimų apie kibernetinius incidentus įtaką įmonės akcijų kainai analizuoti perteklinėms akcijų grąžoms intervalus nuo -20 iki +20 (4 lentelė), tačiau labai dažname tyrime intervalai tesudaro nuo -5 iki +6 dienų. Tyrimai parodė, kad statistiškai reikšminga suminė vidutinė perteklinė grąža stebima kelios dienos po įvykio (Tweneboah-Kodua, 2018). Vėlesnėmis dienomis nebegeneruojama perteklinė grąža, o ilguoju periodu gali atsirasti kitų įvykių, kurie turės įtakos akcijų pokyčiui ir rezultatai neatitiks realybės.

4 lentelė. Įvykio lango intervalai, nustatyti pranešimų apie kibernetinius incidentus įtakos akcijų kainų tyrimuose

Autorius, metai	Įvykio lango periodas
Campbel, 2003	[-1,+1]
Abhishta ir kt., 2017	[-1,+1], [-2,+2], [-5,+5], [-10,+10], [-20,+20], [-15,+15], [-30,+30], [-3,+1], [-2,+1], [-1,+2]
Shinichi ir kt., 2018	[-1,+1],[-2,+2],[-5,+5]
Colivicci ir Vignaroli, 2019	[-20,+20], [-10,+10], [-5,+5], [-3,+3], [-20,-1], [-10,-1], [-5,11], [-3,11], [0,+20], [0,+10], [0,+5], [0,+3], [0,+1]
Tweneboah-Kodua, 2018	[-1,+1], [-2,+2], [-5,+5], [-10,+1], [-20,+20], [-15,+15], [-30,+30]
Smith, 2018	[-7,+7], [-3,+3] ,[-1,+1]
Rosati, 2017	[-5,+], [-4,+4] ,[-3,+3], [-2,+2], [-1,+1]
Bianchi ir Tosun, 2020	[-1,+1], [-2,+2], [-3,+3], [-3,+1], [-2,+1], [-1,+2], [-1,+3]

Atsiradus kitiems įvykiams įvykio lange nebeliktų prielaidos, kad tiriamas vienas reikšmingas įvykis. Suminė perteklinė grąža atspindi bendrą rinkos reakciją, nes sumuojami investuotojų veiksmai, kai jie keičia nuostatas (Abdel-Meguid ir kt., 2016).

4 lentelėje išvardinti įvykio lango intervalai, kuriuos tyrėjai naudojo paranešimų, susijusių su kibernetinių incidentų įtaka įmonės akcijų kainų pokyčiams tyrimuose. Galima teigti, kad dažniausiai pasirenkama trumpesnio intervalo įvykio langas. Taip atsitinka todėl, kad kibernetiniai incidentai dažniausiai turi trumpalaikį poveikį akcijų kainai. Ilguoju periodu labai sunku nustatyti ar tik analizuojamas įvykis turi įtakos akcijų kainai, nes ilgesniu periodu įmonės veikloje gali atsitikti daugiau iš anksto nenumatytų įvykių. Pasirenkami simetrinius arba nesimetrinius įvykio lango intervalai.

Atliekant tyrimą įvykio analizės metodu svarbi dar viena laiko atkarpa – įvertinimo langas, kurio datos intervalas yra kur kas ilgesnis nei įvykio langas, bet taip pat nėra griežtų standartų dėl ilgio pasirinkimo. Įvertinimo langas skirtas vertinti faktines akcijų ir rinkos grąžas, naudojant iki kibernetinio incidento paskelbimo datos duomenis. Dažnu atveju pasirenkamas vertinimo periodas siekia 120 – 365 prekybos sesijos dienų iki įvykio. Įvykio periodas negali būti įtraukiamas į vertinimo lango periodą. Įvykio analizės pradininkas MacKinlay (1997) siūlo 120 dienų intervalą. Tai yra beveik pusės metų prekybinės sesijos laikas ir tai yra pakankamas laiko tarpas, įvertinti vidutinę laukiamą akcijų grąžą. Tarp įvertinimo lango ir įvykio lango paliekamas dienų tarpas, kad nesusidengtų šie langai, t.y., kad nebūtų papildomų įvykių, kurie turėtų papildomą poveikį akcijų grąžai. Kiti autoriai pasirenka metų ilgumo įvykio vertinimo langą, t.y. 365 d. (Colivicci ir Vignaroli, 2019), 280 dienų (Smith ir kt., 2018).

5 lentelė. Tyrimo metodai ir taikyti modeliai tyrimuose pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiui

Autorius	**Tyrimo metodas ir taikyti modeliai perteklinių grąžų skaičiavimui**	**Veiksniai**
Schatz ir kt., 2016	Įvykio analizės metodas su rinkos modeliu	Dvi grupės pasikartojančių kibernetinių incidentų.
Abhishta ir kt., 2017	Įvykio analizės metodas su rinkos modeliu	DDos tipo kibernetiniai incidentai.
Rosati ir kt., 2017	Įvykio analizės metodas su 3 faktorių Fama french modeliu.	Kibernetinio incidento tipas, kapitalizacija.
Lending ir kt., 2018	Įvykio analizės metodas su rinkos modeliu.	Rinkos segmentas, kibernetinių incidentų apimtis, tipas.
Juma ir Alnsour, 2020	Įvykio analizės metodas su rinkos modeliu	Finansinis ROA.
Smith ir kt., 2018	Įvykio analizės metodas su rinkos modeliu	10 skirtingų įmonių atvejai.
Tweneboah-Kodua, 2018	Įvykio analizės metodas su rinkos modeliu	Rinkos segmentai.
Colivicci ir Vignaroli, 2019	Įvykio analizės metodas / rinkos modelis, turto ir kainos nustatymo modelis	Rinkos segmentas, finansinių įmonių portfelis.
Kammoun ir Bounfour, 2019	Įvykio analizės metodas su rinkos modeliu, Fama-French keturių faktorių modelis	Rinkos segmentai, rinkos.

Taigi įvykio analizės metodo pagrindas yra išmatuojamas turtas laiko vienete ir įvykis (kibernetinis incidentas), kuris kaip tikimasi, turės įtakos šio turto (akcijos) vertei. Paprastai naudojamos istorinės

akcijų kainos tam tikrą laiką prieš prognozę ir po įvykio datos. Įvykio analizės metodas, grindžiamas apskaičiuojant perteklinę grąžą, kuri ir atspindi reakciją į naujos, netikėtos informacijos gavimą. Perteklinei grąžai apskaičiuoti dažniausiai tyrėjų taikomas yra rinkos modelis (5 lentelė), kurio pagrindinė mintis, kad egzistuoja ryšys tarp akcijos kainos pokyčių ir bendrų rinkos tendencijų. Skaičiavime yra eliminuojama rinkos įtaka iš kainos pokyčio ir gautas rezultatas vadinamas pertekline akcijų grąža.

6 lentelė. Literatūros analizėje aptartų tyrimų išvados ir rezultatai

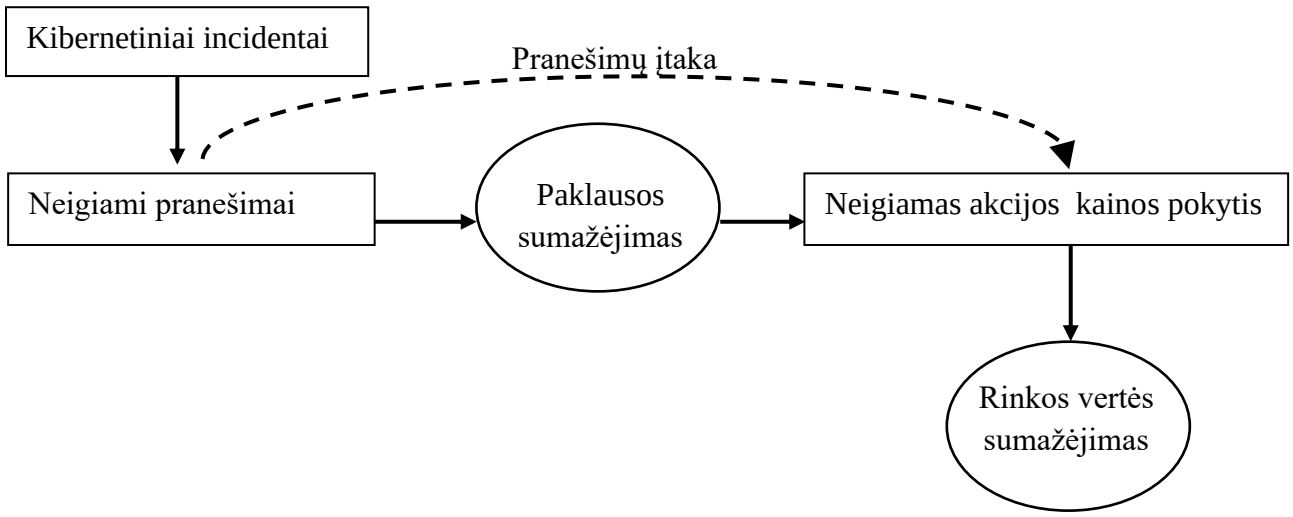
Autorius	**Tyrimo kryptis**	**Išvados ir rezultatai**
Layton ir kt., (2014)	Kibernetinių incidentų įtaka akcijų kainų pokyčiams	Suvaldytas kibernetinis incidentas turi nereikšmingą poveikį įmonės reputacijai, prekiniam ženklui.
Spanos ir Angelis., (2016)		Išanalizuoti 45 tyrimai ir nustatyta, kad 75,6 procento įvykio analizės metodu paremtuose tyrimuose yra gaunamas neigiama perteklinė akcijų grąža.
Higgs ir kt., (2016)		Tyrimas atskleidė, kad įmonės, turinčios valdybos lygio informacijos saugumo valdymo grupę, greičiausiai pranešė apie įsilaužimus. Taip pat tyrime nustatyta, kad neigiamą perteklinė akcijų grąža yra ženkliai mažesnė nei kitų įmonių.
Rosati ir kt., (2017)		Patvirtino, kad kibernetiniai incidentai turi įtakos trumpalaikiu periodu akcijų kainoms ir prekybos aktyvumui. Ypač stiprus poveikis buvo dėl didesnių duomenų vagysčių kiekio bei dėl įrangos vagysčių.
Amir ir kt., (2018)		Rinkos reakcija į atskleistus kibernetinius incidentus yra pakankamai maža, bet į užlaikytus – negatyviai reikšminga.
Juma ir Alnsour, (2020)		Tyrimas nepatvirtina ryšio tarp duomenų pažeidimų ir akcijos rinkos reakcijos, vertinant ketvirčio akcijų kainos pokyčio rezultatus, tačiau trumpuoju, kelių dienų, periodu stebėta neigiama perteklinė grąža.
Lending ir kt., (2018)		Įmonės, turinčios mažesnes valdybas, tačiau pakankamus finansinius išteklius yra mažiau atakuojamos. 30 dienų periodu pastebimas -3,5 proc. neigiamų suminių akcijų grąžų rodikliai.
Evans ir kt., (2019)	Kibernetiniai incidentai	Nustatyta 99 proc. žmogiškųjų klaidų mastas, turintis poveikį kibernetinių incidentų įvykiams.
Nicho, (2018)	saugumo sistema	Informacinių sistemų apsaugos valdymo inicijavimas, naudojant tam tikrą ciklą yra geriausia praktika, leidžianti investuotojams pozityviai vertinti įmonę.
Yang ir kt., (2020)	Saugumo sistema	Išvadoje atskleidžiama, kad investuotojai vertina kibernetinio saugumo sistemos naudą įmonei ir tai pozityviai atsiskleidžia su investavimo pasirinkimu.
Hwang ir kt., (2017)	Saugumo sistema	Nustatyta, kad darbuotojų švietimas saugumo klausimais padeda sumažinti netikėtų kibernetinių incidentų skaičių.

Rosati (2017) straipsnyje aprašo tyrimo pranešimų apie kibernetinius incidentu atskleidimo įtaką įmonių akcijų kainoms, rezultatus. Šiam tyrimui buvo pasirinktas įvykio analizės metodas su 3 faktorių Fama French modeliu, kuriame grąža yra laukiama rizikos premija ir paaiškinama trimis faktoriais – rinką atspindinčio portfelio rizikos premija, grąžos iš mažą kapitalizaciją turinčių įmonių akcijų portfelio ir grąžos iš didelę kapitalizaciją turinčių įmonių akcijų portfelio skirtumas ir grąžos skirtumas tarp aukštus B/P rodiklius turinčių akcijų portfelio ir žemus B/P rodiklius turinčių akcijų portfelio.

Apibendrinant galima teigti, kad itin paplitęs rinkos modelio naudojimas yra dėl paprastumo ir rezultatų tikslumo. Autoriai, naudoję kelis modelius, tyrimų pabaigoje konstatavo, kad sudėtingesnių modelių rezultatai palyginus su rinkos modelio rezultatais išsiskyrė visiškai nežymiai, todėl nėra pagrindo ir yra neefektyvu taikyti sudėtingus modelius (Colivicci ir Vignaroli, 2019; Kammoun ir Bounfour, 2019; Rosati ir kt., 2017).

Literatūros analizės metų pastebėta, kad autoriai, siekdami atskleisti pranešimų apie kibernetinius incidentus poveikį įmonių akcijų kainų pokyčiams, į tyrimus įtraukia papildomus veiksnius. Šiais veiksniais koreguojamos duomenų imtys, t.y. suskirstomi duomenys pagal tam tikrus pasirinktus veiksnius. Skaičiuojamos naujųjų smukiųjų imčių perteklinės grąžos ir lyginamos tarpusavyje. Dažniausiai autoriai skirsto pagal įmonės ir kibernetinio incidento charakteristiką taip pat taikomi finansiniai veiksniai, tačiau finansinių veiksnių duomenų gavimas yra sudėtingesnis ir rezultatai nepakankamai išsamūs. Pagal įmonės charakteristiką tyrėjai sudaro būdingas imtis: rinkos segmentas ir kapitalizacija (Rosati ir kt., 2017; Tweneboah-Kodua, 2018; Kammoun ir Bounfour, 2019), pagal kibernetinio incidento tipą skirstoma: kibernetinio incidento tipas, kibernetinio incidento apimtis (Lending ir kt., 2018; Rosati ir kt., 2017).

Atlikus literatūros pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams tematika matoma autorių nuomonė, kad pranešimai apie kibernetinius incidentus turi tam tikros įtakos įmonių akcijų kainai trumpuoju, kelių dienų periodu. Sudarius schemą (4 pav.), atsižvelgiant į literatūros analizės rezultatus, galima stebėti kibernetinių incidentų įtaka akcijų kainoms veikimo algoritmą. Visų pirma stebimas kibernetinio incidento atsiradimas ir pranešimo paskelbimas. Tuo metu rinkoje vyksta įvertinimas kiek svarbus įvykis įmonės akcijų kainai. Jei investuotojai sprendžia, kad gali stipriai paveikti įmonę toks incidentas, tai tokiu atveju įvyksta rinkoje akcijų išsipardavimas. Akcijos kaina rinkoje mažėja. Kiek laiko gali mažėti, kada atsistato, ar tikrai visais atvejais stebimos neigiamos perteklinės grąžos bus analizuojama tolimesnėje tyrimo eigoje.



4 pav. Pranešimų apie kibernetinius incidentus įtakos akcijų kainai schema

Pritaikius literatūros analizės įžvalgas tyrimo problemai pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams, spręsti išskiriami kertiniai tyrimo akcentai:

- skaičiuojamos ir vertinamos suminės perteklinės akcijų grąžos, pasirenkant plačiai tyrimuose pritaikomą įvykio analizės metodą bei rinkos modelį,
- akcijų grąžų pokyčiai skaičiuojami trumpalaikiu laikotarpiu, pasirenkant simetrinius ir nesimetrinius įvykio langus, norint plačiau atskleisti akcijų kainų pokyčius,
- parenkami veiksniai, susiję su įmonės ir kibernetinio incidento charakteristika: rinkos segmentas, kapitalizacija, kibernetinio incidento tipas ir apimtis.

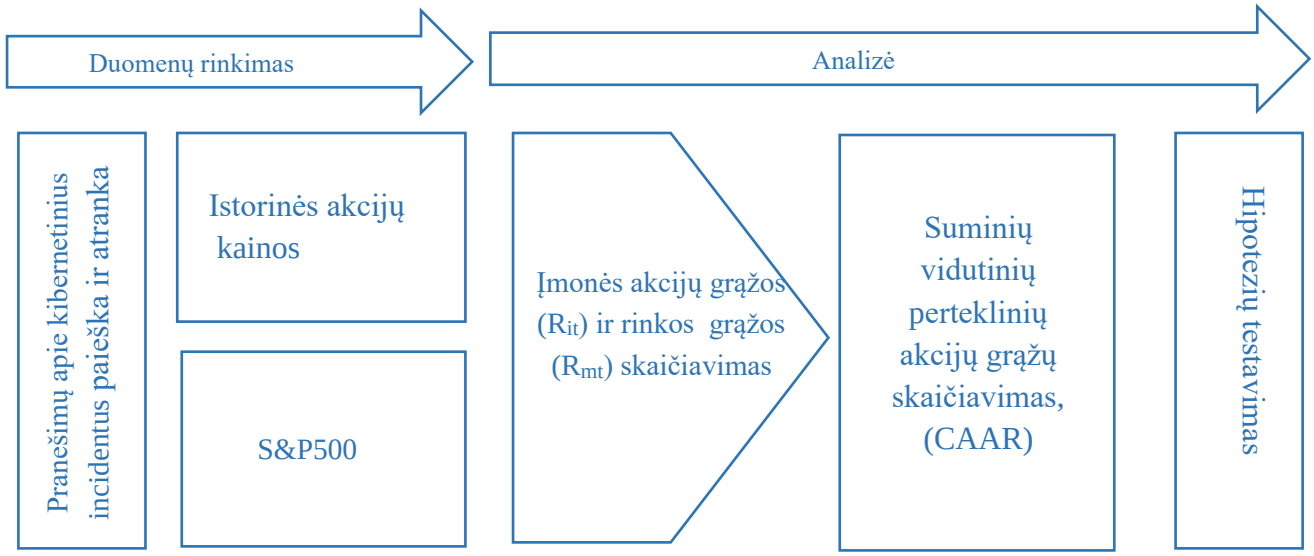
Remiantis teorinės analizės metu susistemintų tyrimų išvadomis ir rezultatais (6 lentelė) galima teigti, kad pranešimų apie kibernetinių incidentų poveikio akcijų kainai tyrimų vis dar nėra pakankamai atlikta dėl kasmet kintančių kibernetinių incidento pobūdžio, besikeičiančių technologinių sprendimų įmonėse. Rezultatai atspindi siauras tendencijas, todėl daugelis autorių siūlo pakartoti panašius tyrimus kitais laikotarpiais, skirstant įmones pagal rinkos segmentus bei įvykius pagal kibernetinių atakų tipus (Berkman ir kt., 2018; Chen ir kt., 2016; Spanos ir kt., 2016).

3. Pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams tyrimo metodologija

Šiame skyriuje apibūdinama pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų kainų pokyčiams tyrimo problema, pagrindžiamos keliamos hipotezės, pateikiamas ir pagrindžiamas tyrimo metodas, pateikiamas tyrimo sekos algoritmas.

3.1. Tyrimo problema ir nuoseklumas bei iškeltų hipotezių pagrindimas

Remiantis literatūros analize galima teigti, kad mokslininkai jau kelis dešimtmečius siekia išsiaiškint pranešimų apie kibernetinius incidentų atskleidimo įtaka akcijų kainoms. Literatūros analizėje nagrinėtų mokslinių tyrimų išvados, bendrąja prasme, teigia, kad akcijos patiria neigiamas grąžas po paviešintos informacijos apie kibernetinius incidentus, tačiau norint pateikti argumentuotą atsakymą šiuo klausimu turi būti atliekami išsamesni tyrimai, kuriuose parenkami veiksniai leistų giliau analizuoti akcijų kainų pokyčio pasekmes po kibernetinių incidentų atskleidimo. Ankstesniuose tyrimuose, kuriuose analizuojami akcijų kainų pokyčiai po kibernetinių incidentų pranešimų, parinkti įvairūs veiksniai, susiję su įmonės ar kibernetinių incidentų charakteristikomis leido pateikti platesnes įžvalgas šios problemos vertinimuose.



5 pav. Loginė tyrimo seka

Remiantis literatūros analizėje (2 skyrius) aptartais mokslininkų tyrimais, jų eiga, rezultatais bei teorinėje literatūroje aprašytais vertinimo modeliais, pateikiama pateikiama loginė tyrimo seka (5 pav.). Tyrimu siekiama nustatyti atskleistų pranešimų apie kibernetinius incidentus poveikį įmonių akcijų kainų pokyčiams.

Pirmajame etape analizuojama pranešimų apie kibernetinius incidentus turinys, kiekis, tikrinamos atskleidimo datos. Sisteminama informacija pagal veiksnių priklausymą įmonei bei incidentams. Kitame etape apskaičiuojamos akcijų perteklinės grąžos pasirinktuose įvykio lango intervaluose. Paskutiniame etape vertinamos suminės ir vidutinės perteklinės grąžos ir nustatoma ar atskleisti pranešimai apie kibernetinius incidentus turi poveikį esant skirtingiems veiksniams, susijusiems su įmonės ir incidentų charakteristika. Pagal šį modelį atliktas tyrimas, analizuojantis JAV akcijų biržoje

listinguojamų įmonių akcijų kainų priklausomybę nuo atskleistų pranešimų apie kibernetinius incidentus.

Pagrindinis šio tyrimo tikslas yra nustatyti ar pranešimai apie kibernetinius incidentus turi įtakos įmonių akcijų kainų pokyčiams. Kaip paminėta šio skyriaus 2.4 poskyryje, akcijų kainų pokyčių reikšmės bus vertinamos taikant įvykio analizės metodą. Remiantis ankstesnių tyrimų įtaka, kuriuose buvo naudojamas įvykio analizės metodas pranešimų apie kibernetinius incidentus įtakos akcijų kainoms tirti, keliamas klausimas, – ar po pranešimo apie įvykusį kibernetinį incidentą yra stebimas neigiamas poveikis įmonės akcijų vertei? Šio klausimo pagrindu iškeliama teorinėmis prielaidomis paremta nulinė hipotezė:

H_{10}: Atskleisti pranešimai apie kibernetinius incidentus nesukelia perteklinių akcijų grąžų (CAAR=0)

Šios srities tyrimų rezultatai apima labai platų diapazoną, todėl keičiant įvairius veiksnius, susijusius su įmonės ar kibernetinių incidentų ypatybėmis, atsiranda galimybė tyrimų rezultatuose atsakyti į akcininkų užduodamus klausimus – kurių įmonių neigiama grąža gali būti rizikinga investavimui, kurie kibernetiniai incidentai padaro daugiausiai žalos ir todėl akcijų kainos pokyčiai bus neigiami, ar rinka ilgai išlieka nestabili po kibernetinių incidentų?

Veiksniai susiję su įmone yra tokie veiksniai, kurių buvimas arbe nebuvimas lemia įmonės vertės pokyčius po pranešimų apie kibernetinius incidentus. Šiame tyrime analizuojami du su įmonės ypatybėmis susiję veiksniai: rinkos segmentas, kuriam priklauso įmonė ir kapitalizacija.

Tyrime tikimasi, kad rinkos reakcijos poveikis bus panašus kaip Colivichi ir Vignaroli (2019) tyrime. Šio tyrimo rezultatai rodo, kad statistiškai reikšmingą neigiamą poveikį pranešimo apie kibernetinius incidentus poveikį turėjo finansiniam rinkos segmentui priklausančios įmonės. Keliamos hipotezės:

H_{2F}: Atskleisti pranešimai apie kibernetinius incidentus sukelia finansinių įmonių neigiamą perteklinę grąžą.

H_{3K}: Kibernetinių incidentų sukelta perteklinė grąža yra neigiama ir priklauso nuo įmonės kapitalizacijos.

Pirmuosiuose tyrimuose, kurie susiję su pranešimų apie kibernetinius incidentus atskleidimo įtaka akcijų kainų pokyčiams, Campbell‘as ir kt. (2003) tyrimo išskirstė į smulkesnes imtis pagal kibernetinio incidento tipą ir konstatavo, kad didesnė neigiama grąža stebėta tų įmonių, kurių kibernetinio incidento metu. atskleisti duomenys buvo konfidencialūs.

Tyrime išskirti du apibrėžiantys veiksniai, susiję su kibernetinio incidento ypatybėmis – kibernetinio incidento tipas ir apimtis (duomenų kiekis, kuris buvo paveiktas incidento metu).

Nors kibernetinis incidentas pats savaime jau yra neigiamas įvykis akcininkams ir įmonėms, kurios patyrė šį incidentą, tačiau incidento apimtis ar tipas gali nulemti stipresnes ar lengvesnes pasekmes. Didesnės apimties incidentai gali būti siejami su didesniais netiesioginiais kaštais ir finansinėmis išlaidomis. Taip pat didesnės apimties incidentai sąlygoja platesnį pranešimų kiekį, didesnį dėmesį incidentui, todėl didelė dalis neracionaliųjų investuotojų apie kuriuos kalbėta literatūros analizėje gali sukelti rinkos „bangavimus“ ir padidinti perteklinių grąžų rodiklius. Todėl keliamos šios hipotezės:

H_{4KIT}: Kibernetinių incidentų sukelta neigiama perteklinė grąža priklauso nuo kibernetinio incidento tipo

H_{5KIA}: Kibernetinių incidentų sukelta perteklinė grąža neigiama ir yra didesnė tų įmonių, kurių kibernetinio incidento apimtis yra didesnė.

Moksliniuose darbuose, kuriuose analizuojamas pranešimų apie kibernetinius incidentus poveikis akcijų kainų pokyčiams, yra keliamos gana panašios hipotezės, tačiau rezultatai gaunami prieštaringi. Tokio nesutapimo priežastys atsiranda dėl skirtingų metodų naudojimo, į tyrimus įtraukiamos skirtingos rinkos ir indeksai, dažnai skirtumai atsiranda dėl labai skirtingų laikotarpių, dėl besikeičiančių incidentų tipų ir pan. Siekiant atlikti rezultatų palyginamumo analizę, įvertinti hipotezes tyrime naudojamas įvykio analizės metodas.

Taigi įvykio analizės metodo pagrindas yra išmatuojamas turtas laiko vienete ir įvykis, kuris kaip tikimasi, turės įtakos šio turto vertei.

3.2. Pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiui įvertinimo metodologija

Šiame poskyryje bus sudaroma pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiui įvertinimo metodika, remiantis 2 skyriuje nagrinėtų mokslininkių tyrimų praktika. Aptariami pagrindiniai įvykio analizės metodo elementai, pateikiama loginė tyrimo seka.

Remiantis literatūros analize tipinis metodas, naudojamas analizuoti rinkos reakciją į atskleistus įmonių pranešimus apie įvairius jų įvykius yra įvykio analizės metodas (angl. event-study). MacKinlay (1997) pristatė ir vėliau ištobulino įvykio analizės metodą. Šio metodo esmė yra įvertinti rinkos reakciją į viešai pateikiamą informaciją. Metodas labai plačiai naudojamas tiriant pranešimų apie kibernetinius incidentus atskleidimo įtaką įmonių akcijų kainų pokyčiams.

Pirmoji įvykio analizės tyrimo užduotis yra nustatyti įvykį, kuris domina tyrėjus ir apibrėžti laikotarpį per kurį informacija apie įvykį bus inkorporuota į įmonės akcijos kainą. Šio tyrimu atveju bus randami viešai paskelbti kibernetinių incidentų pranešimai. Žiniasklaidoje pranešimai pasirodo ne visada tą pačią dieną, todėl anksčiausio pranešimo data bus laikoma įvykio data.

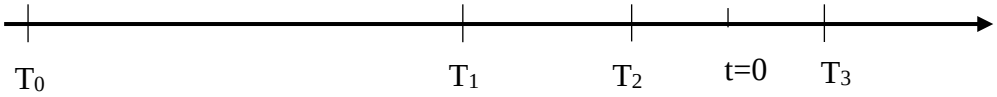
Po kibernetinių incidentų tikslios įvykio datos nustatymo, parenkami įvykio lango intervalai, kurie parodo kaip greitai paviešinta, nauja informacija apie kibernetinius incidentus atsispindi akcijos kainoje. Kiekvienam potencialiam įvykiui yra naudojami du įvertinimo laiko langai – įvykio langas (angl., estimated window) ir įvykio langas (angl., event window). Įvertinimo langų schema pavaizduota 6 paveiksle.

Įvertinimo langas pasirenkamas pakankamai ilgas laikotarpis – 120 dienų, kaip siūlo MacKinlay (1997) ir yra pakankamas, kad būtų įvertinta vidutinė reprezentatyvi akcijų grąža. Tarpas tarp įvertinimo lango ir įvykio lango – 11 prekybos sesijos dienų.

Kaip minėta literatūros analizėje, labai griežtos atrankos įvykio lango nustatyme nėra. Būtina parinkti keletą įvykio langų su skirtingais periodais, kad analizė būtų tikslesnė. Tyrėjai pasirenka simetriškus arba nesimetriškus įvykio langus su labai įvairiu dienų skaičiumi, tačiau dažniausiai varijuojama nuo vienos iki penkių dienų.

Šiame tyrime perteklinė akcijų grąža analizuojama tokias įvykio lango periodais:

- simetriniai [-1,1], [-2,2], [-3,3], [-4,4] [-5,5];
- nesimetriniai[0,1], [-1,0], [-1,2], [-2,1], [-1,3], [-1,4], [-1,5] [-5,+10].



6 pav. Laiko eilutė, naudojama įvykio analizės metode laiko langams pažymėti

čia

Intervalas T_0-T_1 – įvykio įvertinimo langas (angl. estimated window);

Intervalas T_2-T_3 – įvykio langas (angl. event window);

Laikas t=0 – įvykio data kalendoriuje.

Akcijų rinkoje dažna situacija, kada akcijų kainų svyravimas būna susijęs dėl bendro rinkos svyravimo veikiant makroekonominiams veiksniams. Norint pašalinti kainų svyravimus iš bendro rinkos judėjimo, iš akcijų kainų atimama pasirinkto akcijų indekso vertė. Turint šias reikšmes apskaičiuojamos kiekvienos įvykio dienos akcijų grąžos, kurios vėliau bus naudojamos perteklinei akcijų grąžai (angl. abnormal returns) apskaičiuoti.

Šiame tyrime skaičiuojama akcijos grąža, kuri susidaro atsiradus kainų pokyčiui po pranešimo atskleidimo apie kibernetinį incidentą. Vėliau vertinamos suminė ir vidutinė perteklinė akcijų grąžos Pasirinktas rinkos modelis remiasi prielaida, kad egzistuoja ryšys tarp akcijos grąžos ir rinkos pelningumo pokyčių. Eliminavus galimą rinkos poveikį akcijų grąžai, galima įvertinti kokia akcijos grąžos dalis yra paveikta investuotojų reakcijos į netikėtą pranešimą apie kibernetinį incidentą. Tam skirta regresinė analizė, o ryšys tarp akcijos ir vidutinio rinkos pelningumų randamas regresijos lygtimi:

$$\mathrm{R_{i,t}} = \alpha_i + \beta_i \mathrm{R}_{m,t} + e_{i,t}; \quad (1)$$

čia $R_{i,t}$ - įmonės akcijos *i* dienos grąža (angl. expected return);

α_i ir β_i - regresinės lygties parametrai įmonės akcijai *i*;

$R_{m,t}$ - rinkos indekso (tyrimo atveju S&P500) grąža laikotarpiu t;

$e_{i,t}$ - atsitiktinė paklaida (neutraliu periodu)

Įmonės akcijos dienos *i* grąža :

$$R_{i,t} = \frac{P_{i,t} - P_{i,t-1}}{P_{i,t-1}}; \quad (2)$$

čia $R_{i,t}$ – įmonės *i* akcijos faktinė grąža laikotarpiu *t*;

$P_{i,t}$ ir $P_{i,t-1}$ - įmonės *i* akcijos faktinės kainos (uždarymo) laikotarpiais *t* ir *t-1*;

Vidutinis rinkos indekso S&P500 pelningumas laikotarpiu *t*

$$R_{m,t} = \frac{Indeksas_{i,t1} - Indeksas_{i,t-1}}{Indeksas_{i,t-1}}; \quad (3)$$

čia Indeksas - $S\&P500_t$ indekso reikšmė *t* laikotarpio uždarymo kaina;

$S\&P500_{t-1}$ indekso reikšmė *t* laikotarpio uždarymo kaina;

Toliau apskaičiuojama:

Perteklinė grąža:

Prognozuojamą akcijos grąžą atėmus iš faktinės akcijos grąžos $R_{i,t}$, gaunama perteklinė grąža

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i \times R_{m,t}); \quad (4)$$

čia $AR_{i,t}$ – įmonės *i* akcijos perteklinė grąža (angl. abnormal return) gauta įvykio lango periodų, t.y. kai paskelbtas pranešimas apie kibernetinį incidentą.

Vidutinę perteklinę grąžą:

$$AAR_t = \frac{\sum_{i=1}^{N} AR_{i,t}}{N}; \quad (5)$$

čia AAR_t - visų įvykių (pranešimų apie kibernetinius incidentus) vidutinė perteklinė grąža dieną *t* (angl. average abnormal return);

N- pranešimų apie kibernetinius incidentus skaičius.

Suminę vidutinę perteklinę grąžą:

$$CAAR_{[t_1,t_2]} = \sum_{t=t_1}^{t_2} AAR_t \quad (6)$$

čia $CAAR_{[t_1,t_2]}$ – suminė vidutinė visų įvykių perteklinė grąža nuo dienos t_1 iki dienos t_2 (angl., cumulative average abnormal return);

AAR_t – visų įvykių vidutinė perteklinė grąža dieną *t.*

Toliau atliekamas iškeltų hipotezių vertinimas. Atliekamas gautų suminių vidutinių perteklinių akcijų grąžų (CAAR) reikšmingumo vertinimas atliekamas parametriniu testu t-statistika. Parametriniai testai remiasi prielaida, kad kiekvienos įmonės perteklinė akcijų grąža yra normaliai išsibarsčiusi. Šiame tyrime priimame prielaidą, kad akcijų grąžos yra normaliai išsibarsčiusios ir reikšmingumas tikrinamas naudojant parametrinį testą – t statistiką. Tyrime norima nustatyti, ar CAAR ir AAR nėra lygios nuliui. Jei šios reikšmės nelygios nuliui, tai nulinė hipotezė atmetama. T-statistika skaičiuojama pagal šias formules:

$$t_{AAR} = \frac{AAR_{m,t}}{\sigma\,(AAR)}; \quad (7)$$

$$t_{CAAR} = \frac{CAAR_{[t2,t3]}}{\sigma(AAR)^{\frac{1}{2}}}; \quad (8)$$

čia AAR_t – vidutinė perteklinė akcijų grąža konkrečiame įvykio laike t;

$CAAR_{[T2,T3]}$ – sukaupta vidutinė perteklinė akcijų grąža įvykio lange, $t = [T_2, T_3]$;

σ(AAR) – vidutinės perteklinės akcijų grąžos standartinis nuokrypis.

Apskaičiuotos t_{AAR}, t_{CAAR} reikšmės lyginamos su Stjudento skirstinio (n-1) laisvės laipsnių α/2 lygmens kritinėmis reikšmėmis ($t_{\alpha/2}(n-1)$). Jei reikšmės yra didesnės už Stjudento t kriterijų ($t_{0,005} t_{0,025,} t_{0,05}$), (3 priedas), gautas rezultatas yra statistiškai reikšmingas atitinkamai 99 proc., 95 proc., ir 90proc. patikimumu. Šiame tyrime pasirinktas statistiškai reikšmingas 90 proc. patikimumo lygis.

Šiame skyriuje sudaryta tyrimo, kuriame analizuojama pranešimų apie kibernetinių incidentus įtaka akcijų kainų pokyčiams metodologija. Ši metodologija sudaryta pasitelkiant ankstesnių tyrimų metodus ir modelius, kurie aptarti literatūros analizėje. Daugelis autorių tvirtina, kad šis metodas yra ganėtinai nesudėtingas, bet labai plačiai pritaikomas ir patikimas. Literatūros analizėje minėta, kad

įvairiuose tyrimuose mokslininkai taikydami kelis papildomus ir sudėtingesnius metodus stebėdavo pakankamai panašius rezultatus, todėl šiam tyrimui buvo pasirinktas dažniausiai sutinkamas moksliniuose tyrimuose, kuriuose analizuojama pranešimų apie kibernetinius incidentus atskleidimo įtaka akcijų kainų pokyčiui, įvykio analizės metodas. Tyrime taikomi papildomi veiksniai, kurių dėka gaunami informatyvesni rezultatai.

Pagal šiame skyriuje pateiktą metodologiją ir loginę tyrimo eigą, kuri parodyta 5 paveikslėlyje toliau bus pateikiami tyrimo, kuriame analizuojama pranešimų apie kibernetinius incidentus įtaka akcijų kainų pokyčiams rezultatai.

4. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimas

Šiame skyriuje bus vertinami, pagal 3.2 poskyryje patektą tyrimo metodologiją, atliktos analizės atskleistų pranešimų apie kibernetinius incidentus įtaką įmonės akcijų kainai, rezultatai. Gauti tyrimo rezultatai lyginami su mokslinės literatūros analizėje pristatytų tyrimų kibernetinių incidentų įtakos akcijų kainai tema rezultatais. Pabaigoje pateikiamos išvados pristatomi tyrimo ribotumai bei siūlymai kaip galima būtų plėtoti pranešimų apie kibernetinius incidentus tematiką ateityje.

4.1. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimo imtis

Pranešimų apie kibernetinius incidentus poveikio akcijų kainų pokyčiams tyrimas apima duomenų bazėse bei interneto žiniasklaidoje paskelbtus pranešimus apie įvykusius kibernetinius incidentus. Visi pranešimai, sudarantys imtį apima 2015-2019 metų laikotarpį. Kaip minėta literatūros analizėje, kibernetiniai incidentai apima įvykius, kurie įvyksta atsiradus informacinių technologijų saugumo spragoms, neteisėtai atskleidus, pasisavinus ar kitokiais būdais pažeidus duomenų privatumo teises elektroninėje erdvėje. Pirminis šio tyrimo duomenų šaltinis – PrivacyRights.org. Tai pelno nesiekiančios organizacijos duomenų bazė, kurioje sukaupta labai platus spektras – apie 8 tūkst. įvairaus pobūdžio pranešimų apie kibernetinius incidentus JAV. Šioje duomenų bazėje publikuojami valstybinių organizacijų, pelno nesiekiančių ir privataus kapitalo įmonių pranešimai apie kibernetinius incidentus. Kiekvieno incidento turinio ir datos patikslinimui bei papildomų incidentų paieškai pasitelkta „google“ paieška pagal raktinius žodžius – „cyber incident“, „Cyber attack“, „data breach“ ir kt.. Iš viso identifikuota 635 pranešimai, tačiau akcijų kainų pokyčių skaičiavimui yra tinkamos tik įmonės, kurių akcijos kotiruojamos akcijų biržoje. Šio tyrimo atveju imtis sudaryta iš nukentėjusių nuo kibernetinių incidentų įmonių akcijų, kurios kotiruojamos JAV NASDAQ ir NYSE biržose bei priklauso S&P500 indeksui. Šio indekso rezultatai naudojami tiesinės regresinės lygties ir laukiamos grąžos skaičiavimui. 5 lentelėje pateikta pranešimų apie kibernetinius incidentus imties atrankos detalizacija. Finansiniai duomenys naudoti iš “Bloomberg” duomenų bazės.

7 lentelė. Pranešimų apie kibernetinių incidentus imties atrankos detalizacija

Atrankos kriterijai	Pranešimų imtis	
	Eliminuoti pranešimai	Likę pranešimai
Pirminė imtis		635
Nelistinguojamų įmonių pranešimai	525	124
Įmonių, kurios nepriklauso S&P500 indeksui, pranešimai	38	97
Pranešimai, kurių įvykio lange įvyko esminių įvykių	8	89
Pranešimai apie kibernetinius incidentus, įvykę įvertinimo lango periodu.*	11	83
Pranešimai, kurių atskleidimo metu nukentėjusios įmonės akcijos dar nebuvo kotiruojamos biržoje.	1	52
Tyrimo imtis		**52**

Pastaba. Įtraukiamas ankstesnis pranešimas, o vėlesnis eliminuojamas.

Kalbant apie pranešimų atranką, taip pat svarbu paminėti, jog pranešimai apie kibernetinius incidentus paskelbti ne biržos prekybos dienomis neeliminuojami iš bendros pranešimų imties. Tokiais atvejais, skaičiuojant perteklines grąžas, pranešimo data perkeliama į artimiausią prekybos sesiją biržoje.

Apibendrinant galima pasakyti, kad tyrime yra analizuojami 52 pranešimai apie kibernetinius incidentus, kurie priskiriami 34 įmonėms.

Trylika iš visos imties įmonių turėjo viešai atskleistų kibernetinių incidentų daugiau kaip vieną kartą per penkerių metų laikotarpį, neįskaitant tų atvejų kai vietoje dviejų vienas paskui kitą einančių pranešimų buvo fiksuotas tik pirmasis. Iš šių įmonių dvi atskleidė iki 6 pranešimų apie kibernetinius incidentus per 5 metų laikotarpį, dvi – 4 kartus, o likusios devynios – 2 kartus.

Perskaičius ir išanalizavus turimus pranešimus apie kibernetinius incidentus, pašalinus pranešimus pagal paminėtus požymius 7 lentelėje, imtį sudarantys pranešimai suklasifikuoti pagal parinktus papildomus veiksnius: įmonės ir kibernetinio incidento charakteristikas (8 lentelė). Pranešimų apie kibernetinių incidentų įtaką akcijų kainų pokyčiui tyrimo imties įmonės, nurodant įmonės pavadinimą, pranešimo paskelbimo datą pateikta 2 priede.

Antroje tyrimo dalyje literatūros analizėje daugelio tyrimų autoriai, atlikdami atskleistų pranešimų apie kibernetinius incidentus įtakos akcijų kainai tyrimus, problemai analizuoti, įtraukia papildomus veiksnius, pvz. rinkos segmentas, incidento tipas, įmonės tipas, metai ir pan. Todėl šiame tyrime neapsiribota bendros imties skersinio pjūvio analize akcijų kainų pokyčiams tirti po pranešimų atskleidimo apie kibernetinius incidentus ir yra įtraukti keturi papildomi veiksniai, pagal kuriuos stebimi akcijų kainų pokyčiai sudarytos imties atžvilgiu. Šie papildomi veiksniai – rinkos segmentas, kibernetinio incidento tipas, incidento metu pažeistų duomenų kiekis bei kapitalizacijos dydis, leidžia platesniu kampu įvertinti pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams (8 lentelė)

8 lentelė. Imčių grupės pagal veiksnius

Įmonių imties grupė		**Kibernetinio incidento imties grupė**	
Rinkos segmentas	Kapitalizacija	Kibernetinio incidento (KI) tipas	Kibernetinio incidento (KI) apimtis
Finansinės, Informacinės technologijos Paslaugos, Kasdienio vartojimo prekės	Didelės Labai didelės Vidutinės	HACK INSD DISK	0-500 000 >500 000

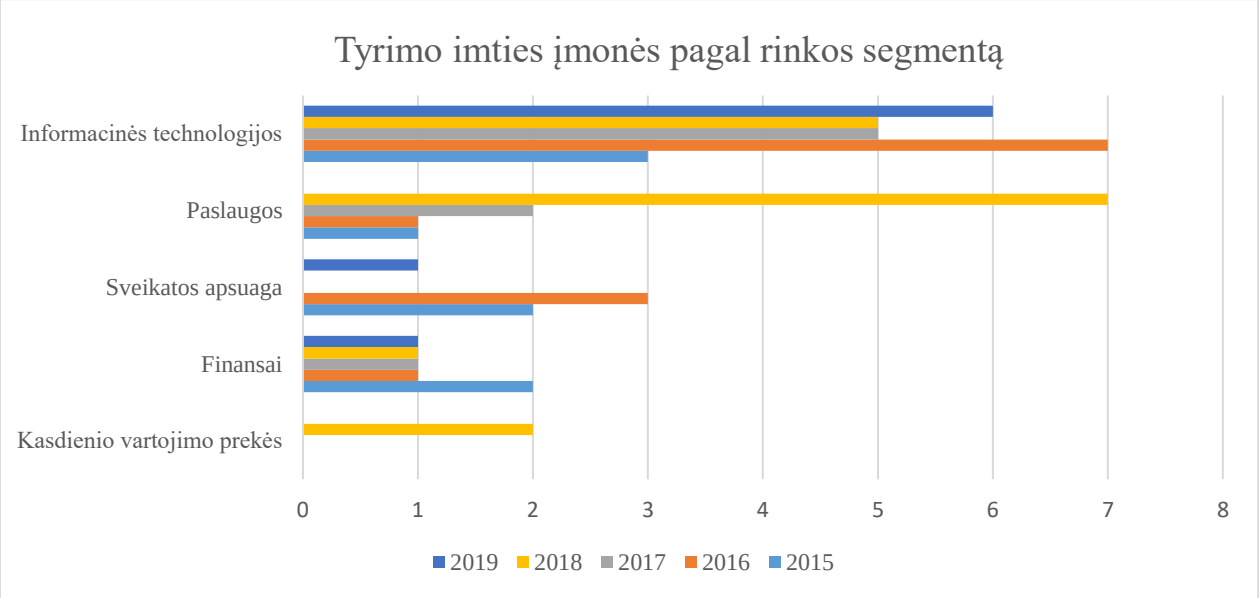
Įmonių duomenys, naudojami šiame tyrime, suklasifikuotos pagal rinkos segmentą bei kapitalizaciją Galima pastebėti, kad dažniausiai kibernetinius incidentus patiria informacinių technologijų bei paslaugų sektoriaus įmonės (tyrimo imties atveju). Šių rinkos segmento įmonių imtyje yra daugiausiai. Nuo 2016 m. kibernetinių incidentų skaičius informacinių technologijų ir paslaugų segmentuose išauga beveik dvigubai. Kasdienio vartojimo prekių segmente tik 2018 metais galima stebėti įvykusius kibernetinius incidentus.

Dažniau atakuojamos informacinių technologijų rinkos segmento sąraše esančios labai didelės kapitalizacijos įmonės – gerai visiems žinomos, stiprios: „Facebook“, „Google“, „Microsoft“, tačiau tyrimo imtyje pagal kapitalizacijos veiksnį, galima pastebėti, kad didžiausią incidentų skaičių

generuoja didelės kapitalizacijos įmonės. Taip pat stebimas didesnis nei kitų šių įmonių pranešimų apie kibernetinius incidentus pasikartojimo dažnis.
Pagal kapitalizaciją tyrimo imties įmonės suklasifikuotos į tris grupes:

- labai didelės („Mega“) – kapitalizacija siekia daugiau nei 200 mlrd. JAV dolerių,
- didelės („Large“) – kapitalizacija siekia nuo 10 iki 200 mlrd. JAV dolerių,
- vidutinės („Mid“) – kapitalizacija siekia nuo 2 iki 10 mlrd. JAV dolerių.

Tyrimo imtyje didžiausią dalį 67 proc. sudaro didelės kapitalizacijos įmonės, labai didelės sudaro 28 proc. visos imties ir tik 0,5 proc. sudaro vidutinio dydžio įmonės. Stebint tokį pasiskirstymą pagal kapitalizaciją, peršasi išvada, kad dažniau nuo kibernetinių incidentų kenčia vidutinės įmonės. Tačiau negalima atmesti ir to fakto, kad ne visi kibernetiniai incidentai yra paviešinti ar daugelis smulkių yra neatskleidžiami.



7 pav. Tyrimo imtis pagal rinkos segmentus

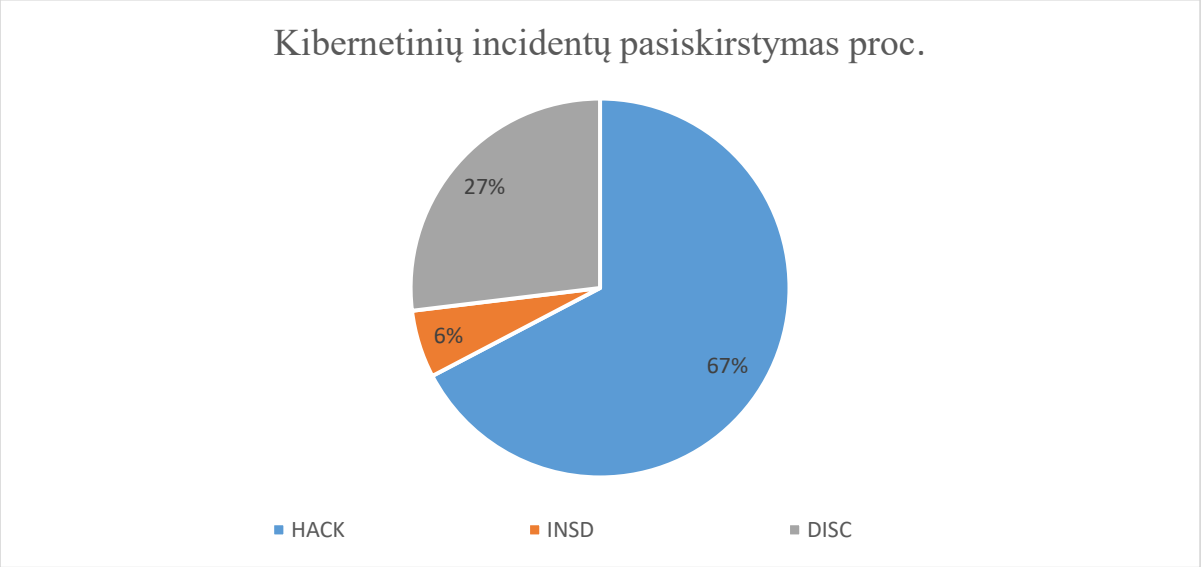
Kibernetinio incidento imties grupė padalinta į dvi dalis: pagal kibernetinio incidento tipą ir pagal kibernetinio incidento apimtį. Dėl patogumo kibernetinio incidento tipai sukoduoti, kurių aprašymai patekti žemiau.

HACK – išorinių veiksnių poveikis. Neautorizuotas įsilaužimas į kitas sistemas, poveikis iš išorės ar užkrėsta „Malware“ tipo virusu, siekiant pasisavinti svarbią informaciją (priskiriama nuskaityta kredito kortelių informacija pardavimo įtaisuose). Taip pat šiam tipui priklauso „Ransomware“ išpirkos reikalaujantys virusai.

INSD – vidinių veiksnių poveikis (gali būti įmonės darbuotojai piktybiškai ar nepiktybiškai prisidėję prie incidento, dėl neatsargaus elgesio internete, įvairių nuorodų paspaudimo, netyčinio duomenų persiuntimo išorės vartotojui ir pan.)

DISC – netyčinis informacijos atskleidimas, nesusijęs su įsilaužimu, tyčiniu pažeidimu ar praradimu (konfidenciali informacija paskelbta viešai, klaidingai išsiųsta informacija elektroniniu paštu ir pan.)

Dažniausiai sutinkamas šiame tyrime yra HACK tipo kibernetinis incidentas sudaro 67 proc. visos imties, mažiausiai 6 proc., kibernetinių incidentų sudaro, kai dėl įmonės darbuotojų buvo atskleista informacija (8 pav.)

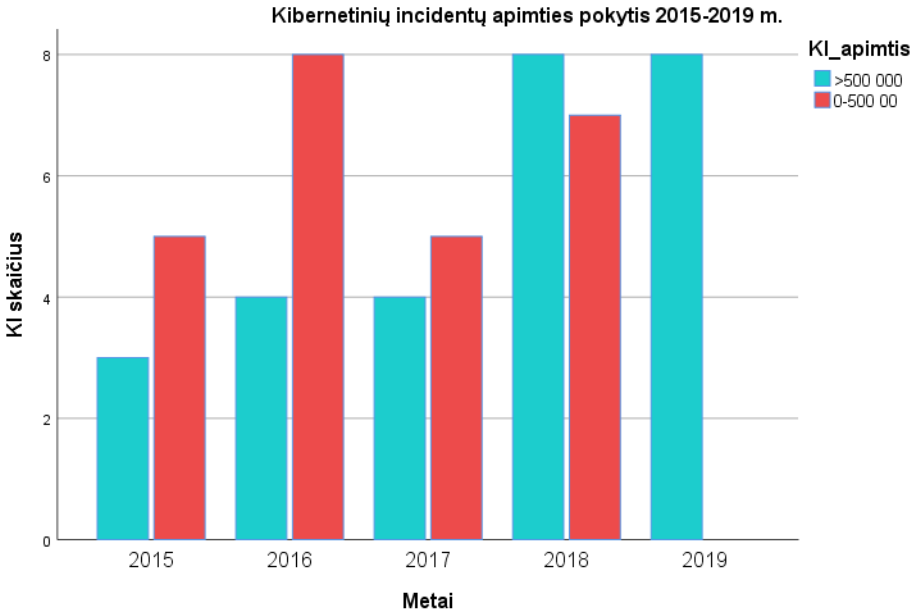


8 pav. Tyrimo metu surinktų pranešimų pagal incidento tipą imtis procentais

Remiantis literatūros analizėje atliktais tyrimais, sugrupuota pagal kibernetinio incidento apimties veiksnį. Imtis padalinta pusiau, todėl gautos dviejų tipų apimtys pagal nutekintų duomenų kiekį milijonais vienetų:

- 0<500 000;
- >500 000>

Didesnės apimties dalis, kurą sudaro kibernetiniai incidentai su nutekintų daugiau kaip 500 000 mln. duomenų kiekiu, yra 11 proc. didesnė nei kita dalis, kurios nutekintų duomenų kiekis yra nuo 0 iki500 00. Akivaizdžiai grafike (9 paveikslas) matyti, kad 2016 m. išaugo kibernetinių incidentų kiekis su mažesnių duomenų skaičiumi. Tai gali būti susiję su vis dažniau viešinamais pranešimais apie kibernetinius incidentus bei pareigą pranešti. Didesnės apimties kibernetinių incidentų kiekis išaugo tik 2018 m. ir išliko tame pačiame lygmenyje 2019 m.



9 pav. Kibernetinių incidentų skaičius pagal apimtį 2015-2019 m.

Kitame poskyryje bus aptariami tyrimo pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonės akcijų kainų pokyčiams rezultatai.

4.2. Pranešimų apie kibernetinius incidentus įtakos įmonių akcijų kainų pokyčiams tyrimo rezultatai

Pagrindinis šio tyrimo tikslas yra vertinti pranešimų apie kibernetinius incidentus atskleidimo įtaką įmonių akcijų kainų pokyčiams 2015-2019 m. laikotarpiu. Kiekvienas atskleistas pranešimas apie kibernetinius incidentus siejamas su tam tikra įmone, kurios akcijų kainų pokytis galėtų būti tiriamas, su prielaida, kad įmonės akcijos kotiruojamos biržoje. Tikslui įgyvendinti skaičiuojamos perteklinės, vidutinės perteklinės, suminės perteklinės bei suminės vidutinės perteklinės akcijų grąžos.

Galima teigti, kad rinkos reakcija į kibernetinių incidentų pranešimus yra investuotojų požiūrio į įmonės tęstinumą ir sėkmę ateityje atspindys. Efektyviosios rinkos hipotezę pritaikius kibernetinių incidentų pranešimų įtakos akcijų kainų vertinimui, būtų logiška tikėtis, kad po pranešimo paskelbimo akcijos kainos pokytis taptų neigiamu. Iš literatūros analizės aišku, kad investuotojai tokio tipo pranešimus turėtų vertinti kaip neigiamą grėsmę įmonei, pvz. pinigų srautams. Tai suprantama, nes literatūros analizėje konstatuota, kad įmonė gali susidurti su tiesioginėmis ir netiesioginėmis išlaidomis.

Šioje dalyje bus pateikiama vidutinių perteklinių akcijų grąžų (AAR) bei suminių vidutinių perteklinių grąžų (CAAR) rodikliai, kurie susidarė po pranešimo apie kibernetinius incidentus atskleidimo. Rodikliai apskaičiuoti pagal 3 skyriuje pateiktą akcijų grąžų skaičiavimo metodiką.

Pirminei analizei pasirinkta vertinti visos imties perteklinių akcijų grąžą, neskaidant pagal skirtingus rodiklius. Vertinimui pasirinktas vienuolikos dienų įvykio langas [-5,5], kuris yra pakankamai ilgas, kad visa informacija apie įvykį būtų inkorporuota į akcijos kainą.

4.2.1. Bendras imties vidutinių perteklinių akcijų grąžų vertinimas

Perteklinės akcijų grąžos paskaičiuotos 9 lentelėje, naudojant rinkos modelį, kiekvienai įvykio lango laikotarpio dienai [-5,5].
Stebimų vidutinių perteklinių akcijų gražų rodikliai vertinami ar yra reikšmingi *t-statistika* parametriniu testu.

9 lentelė. Vidutinės perteklinės grąžos (AAR)

	Dienos	AAR reikšmės	t-statistika
Bendra imtis	-5	-0,0012	-0,6551
	-4	-0,0004	-0,1094
	-3	-0,0039**	-1,8695
	-2	-0,0005	-0,2927
	-1	0,0017	1,1862
	0	-0,0021	-0,7574
	1	-0,043**	-1,9901
	2	0,002	0,8363
	3	0,003	1,3566
	4	-0,0007	-0,4191
	5	0,0029	1,3708

Pastaba. Lentelėje parodytos vidutinės perteklinės grąžos (AAR). Imtį sudaro 52 kibernetinių incidentų pranešimai, kurių AAR skaičiuotas, pasitelkiant rinkos modelį 11 prekybos sesijų dienų intervale. T=0 yra pranešimo apie kibernetinį incidentą diena.

* - 90 proc. patikimumas
** - 95 proc. patikimumas
*** - 99 proc. patikimumas

Statistiškai reikšmingai neigiama vidutinė perteklinė grąža yra trečią diena prieš pranešimo paskelbimą – t-3 (AAR=0.0039*, t- statistika = -1,8695). Galima spręsti, jog dalis investuotojų anksčiau sužinojo viešai neatskleistą informaciją apie kibernetinius incidentus analizuojamų įmonių atžvilgiu. Dažniausiai informacija apie kibernetinius incidentus paskelbiama ne iškarto po įvykio, o praėjus keliems mėnesiams ar metams, prieš pat paskelbiant pranešimą informacija gali būti nutekinta. Pranešimo apie kibernetinį incidentą dieną – t=0 vidutinė perteklinė grąžą yra neigiama, tačiau statistiškai nereikšminga. Tik pirmąją dieną po įvykio – t+1 (AAR= -0.043**, t- statistika = -1,9901) investuotojų reakcija yra statistiškai reikšminga su 95 proc. patikimumu. Neigiama vidutinė perteklinė grąžą pirmą dieną po pranešimo rodo, kad rinka reaguoja į naujai paskelbtą pranešimą, todėl rinką galima laikyti efektyvia bei likvidžia. Stebint likusias įvykio lango dienas, antrą dieną po paskelbimo kainos stabilizavosi, kas galėtų reikšti, kad neigiama informacija apie kibernetinius pranešimus asimiliavosi į akcijos kainą. Statistiškai reikšminga 95 proc. patikimumo lygyje, neigiama perteklinė akcijų grąža, susidariusi pirmosiomis dienomis po pranešimo patvirtina ankstesnių tyrimų išvadas (Yala ir kt., 2011)

Taigi 9 lentelėje pateiktos akcijų vidutinės perteklinės grąžos, atsiradusios paskelbtų pranešimų apie kibernetinius incidentus įtakoje leidžia daryti išvadą, kad svarbūs pranešimai apie kibernetinius incidentus gali būti pesimistinės nuotaikos ir sukelti neigiamą rinkos reakciją, t.y šie pranešimai gali sukelti perteklines akcijų grąžas.

10 lentelė. Visos imties Suminės vidutinės perteklinės akcijų grąžos

	Įvykio langas	CAAR	t-statistika
Bendra imtis	[-1, 1]	-0,0004	-0,106
	[-2, 2]	0,0011	0,2343
	[-3, 3]	0,0002	0,0437
	[-4, 4]	-0,0009	-0,1466
	[-5, 5]	0,0009	0,125
	[-1, 2]	0,0016	0,342
	[-1, 3]	0,0046	0,9237
	[-2, 1]	-0,0009	-0,2399
	[-1, 5]	0,0068	1,2041
	[0, 1]	-0,0021	-1,5206*
	[-1, 0]	-0,0004	0,0067

Pastaba. Lentelėje parodytos suminės vidutinės perteklinės grąžos (CAAR). Imtį sudaro 52 kibernetinių incidentų pranešimai, kurių CAAR skaičiuotas, pasitelkiant rinkos modelį įvairiais įvykio langų intervalais. T=0 yra pranešimo apie kibernetinį incidentą diena.

* - 90 proc. patikimumas

** - 95 proc. patikimumas

Stebima statistiškai reikšminga neigiama perteklinė akcijų grąžą tiek AAR atveju, tiek CAAR atveju (10 lentelė) įvykio lange t=1 AAR atveju ir įvykio lange [0, 1] CAAR atveju su 90 proc. patikimumu. Abiem atvejais perteklinė grąža generuojama pirmą dieną po pranešimo apie kibernetinį incidentą. Tačiau daugelyje dienų vidutinės perteklinės grąžos atveju, o ir įvykio languose suminės vidutinės perteklinės grąžos atveju neigiami rodikliai nėra statistiškai reikšmingi.

4.2.2. CAAR vertinimas pagal rinkos segmentą

Antrosios hipotezės patikrinimui visa tyrimo imtis suskirstyta pagal įmonių, kurios patyrė kibernetinį incidentą, priklausymą rinkos segmentui. 9 lentelėje pateikiami suminių vidutinių perteklinių akcijų gražų apskaičiuoti rezultatai. Galima pastebėti tendenciją, kad neigiamas CAAR generavo tik dvejiems rinkos segmentams priklausančios įmonės – finansų ir paslaugų. Finansų segmento įmonių CAAR reikšmė -0,0322, rodanti 3,2 proc. kritimą akcijos kainoje įvykio lange [4,4] ir yra statistiškai reikšminga 95 proc. patikimumo lygyje. Panaši situacija stebint [-2,1] įvykio langą, tik akcijos kainos kritimas ne toks stiprus ir sudaro 2,2 proc. Stebint nuo pirmos įvykio dienos finansų sektoriaus įmonių suminių vidutinių perteklinių akcijų grąžų kitimą, galima teigti, kad per visą laikotarpį iki ketvirtos dienos po pranešimų paskelbimo apie kibernetinius incidentus buvo generuojama neigiama grąža. CAAR– -0,188 įvykio lange [1,1)] ir -0,0216 [0,1] statistiškai reikšminga 90 proc. patikimumu.

11 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal rinkos segmentą

Rinkos segmentas	Įvykio langas	CAAR	pos:neg CAR	t-statistika
Finansai	[-1, 1]	-0,0188*	1:5	-1,6283
Informacinės technologijos	[-1, 1]	0.0061	15:11	1.2219
Paslaugos	[-1, 1]	-0,0076	4:7	-1.3112
Finansai	[-2, 2]	-0.0164	2:4	-1,4012
Paslaugos	[-2, 2]	-0,0141*	3:8	-1,6291
Finansai	[-3, 3]	-0.0066	2:4	-0.36
Informacinės technologijos	[-3, 3]	0.0036	15:11	0.4467
Paslaugos	[-3, 3]	-0,0119*	3:8	-1,8716
Finansai	[-4, 4]	-0,0322**	1:3	-2,5987
Paslaugos	[-4, 4]	-0,0102*	5:6	-1,4882
Finansai	[-1, 3]	-0,0012	1:5	-0,0497
Informacinės technologijos	[-1, 3]	0,0112	15:11	1,6419
Sveikatos apsauga	[-1, 3]	-0,0044	2:4	-0.3056
Paslaugos	[-1, 3]	-0,009	6:5	-1,2952
Finansai	[-2, 1]	-0,022**	1:5	-2,5709
Informacinės technologijos	[-2, 1]	0.006	16:10	1,1695
Paslaugos	[-2, 1]	-0,0121**	3:8	-1,9799
Paslaugos	[-1, 0]	-0,0114*	5:6	-1,3871
Finansai	[0, 1]	-0,0216*	2:4	-1,8662
Paslaugos	[0, 1]	-0,0084*	5:6	-1,6931

Pastaba. Lentelėje parodytos suminės vidutinės perteklinės grąžos (CAAR) pagal rinkos segmentus. Imtį sudaro 52 kibernetinių incidentų pranešimai, kurių CAAR skaičiuotas, pasitelkiant rinkos modelį įvairiais įvykio langų intervalais. T=0 yra pranešimo apie kibernetinį incidentą diena. Lentelėje nurodyti tik statistiškai reikšmingi rodikliai. Pilna lentelė pateikta 1 priede.

* - 90 proc. patikimumas

** - 95 proc. patikimumas

Paslaugų sektoriaus įmonės, tai pat išsiskyrė neigiamomis CAAR reikšmėmis, kas leidžia suprasti, kad investuotojai neigiamai reagavo į pranešimus apie kibernetinius incidentus. Šiuo atveju stipriausios reakcijos sulaukta [-2,2] įvykio lango dienomis, t.y. antrąja dieną po pranešimo paskelbimo akcijų kaina krito 1,4 proc., įdomu pastebėti ir tai, kad iš vienuolikos net aštuonių įmonių akcijos generavo neigiamą grąžą. Įvykio lange [-2,1] gauta CAAR reikšmė paslaugų segmente yra statistiškai reikšminga 95 proc. patikimumu.

Analizuojant pranešimų apie kibernetinius incidentus atskleidimo įtaką įmonių akcijų kainai pagal rinkos segmentą paaiškėjo, kad rinkos dalyvių reakcija yra neigiama. Statistiškai reikšminga 95 proc. patikimumu CAAR buvo gauta pirmą ir ketvirtą dienomis po pranešimų paskelbimo. Galima teigti, kad tendencija trumpuoju laikotarpiu reaguoti į rinkos naujienas yra reali. Investuotojai ypač aktyviai sureagavo į finansinių bendrovių patiriamus kibernetinius incidentus todėl, kad šios įmonės yra jautrios duomenų atskleidimui – kaupia pakankamai daug privačių asmenų ir kitų bendrovių konfidencialių duomenų, į kuriuos gali būti nusitaikę programišiai.

Iškelta hipotezė atskleisti pranešimai apie kibernetinius incidentus sukelia finansinių įmonių neigiamą perteklinę grąžą, priimama.

Kitų segmentų įmonės, kaip antai, kasdienio vartojimo prekių ar sveikatos apsaugos generavo ne taip stipriai išreikštas neigimas sumines vidutines perteklines akcijų grąžas. Sveikatos sektoriaus įmonės yra pakankamai jautrios, kai yra kalbama apie kibernetinius incidentus, kadangi kaupia nemažai asmeninių pacientų duomenų, tačiau šio tyrimo atveju neigiama CAAR visiškai statistiškai nereikšminga. Tokia situacija neatitinka literatūros analizėje aptiktų prielaidų. Reikėtų atlikti pakartotinus tyrimus norint patikslinti gautus rezultatus.

Informacinių technologijų segmento įmonių akcijos, šiuo atveju, generavo teigiamą akcijų grąžą visais įvykio lango periodais. Šio tyrimo imtyje informacinių technologijų segmento įmonės yra pakankami stiprios rinkoje, didelės kapitalizacijos, todėl turinčios pakankamai resursų kovai su kibernetinių incidentų poveikiui. Galima teigti, kad rinkos dalyviai pasitiki tokiomis įmonėmis ir nesureikšmina kibernetinių incidentų, kaip labai esminių įvykių, galinčių paveikti įmonės rezultatus.

Suminės vidutinės perteklinės akcijų grąžos (CAAR) pagal rinkos segmentą stebėjimo atveju susiformavo trumpalaikės neigiamos reakcijos tendencija į akcijų kainas [-2,1] ir [-2,2] įvykio languose, t.y. pirmą ir antrą dieną po įvykio.

Rinkos segmento veiksnio analizės atveju galima daryti išvadą, kad dėl kibernetinių incidentų atskleidimo įtakos, dažniausiai, poveikį akcijų kainai jaučia finansinės įmonės. Taip yra todėl, kad pinigai, informacija ir viešumas yra šių įmonė kasdienybė – kaupiami klientų konfidencialūs finansiniai duomenys, atliekamos finansinės operacijos. Šių duomenų pasisavinimas sudaro įmonėms nemažai tiesioginių ir netiesioginių kaštų.

Literatūros analizėje pastebėta, kad tyrėjai akcentuoja finansines įmones kaip galimą kibernetinių incidentų potencialų taikinį, o įvykus tokiai situacijai generuojamos neigiamos akcijų grąžos. Tai visiškai atitinka šios tyrimo dalies rezultatus

4.2.3. CAAR vertinimas pagal įmonės kapitalizaciją

Bendrąją imtį suskirsčius pagal kapitalizaciją į tris dalis – laibai dideles, dideles ir vidutines, gautos vidutinės perteklinės akcijų grąžos nurodytos 12 lentelėje. Stebimos CAAR reikšmės pirmą dieną po pranešimo apie kibernetinius incidentus paskelbimo susidarė neigiamos suminės vidutinės perteklinės akcijų grąžos Didelių ir Vidutinių įmonių atžvilgiu. Didelių įmonių neigiama CAAR nesiekė net 1 proc., todėl yra visiškai statistiškai nereikšminga, tačiau vidutinių įmonių neigiama CAAR įvykio lange [0,1] – 1,23 proc., tačiau nėra statistiškai reikšminga. Panaši situacija susidarė ir kitame lange [0,1], kai susiformavo neigiamas didelių ir vidutinių įmonių CAAR, tačiau tik vidutinių įmonių neigimas CAAR siekė 4,5 proc. todėl galima teigti, kad silpnai reikšminga 90 proc. patikimumu. Didelių įmonių CAAR nors ir neigiamas šio lango periodu, tačiau reikšmė statistiškai visiškai nereikšminga. Stebint įvykio langą [-1,0] matome, kad vidutinių įmonių neigimas CAAR vos didesnis už 1 proc., tačiau yra statistiškai reikšmingas 95 proc. patikimumu.

Galima padaryti išvadą, kad apie pranešimo paskelbimą investuotojai jau žinojo prieš jį paskelbiant, todėl informacija į kainą inkorporavosi labai greitai prieš paskelbiant pranešima ir iškart po paskelbimo, t.y. t=1 dieną.

12 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal įmonės kapitalizaciją

Įmonės kapitalizacija	Įvykio langas	CAAR	pos:neg CAR	t-statistika
Didelė	[0, 1]	-0,001	16:18	-0,202
Labai didelė	[0, 1]	-0,001	8:5	-0,2054
Vidutinė	[0, 1]	-0,0123*	2:3	-1,8816
Didelė	[-1, 1]	-0,0008	15:19	-0,1698
Labai didelė	[-1, 1]	0,0065	9:4	1,2062
Vidutinė	[-1, 1]	-0,0454*	2:3	-1,9421
Didelė	[-1, 0]	-0,0015	19:15	-0,3856
Labai didelė	[-1, 0]	0,0067	7:6	1,522
Vidutinė	[-1, 0]	-0,0111*	1:4	-2,7625

Pastaba. Lentelėje parodytos suminės vidutinės perteklinės grąžos (CAAR) pagal kibernetinio incidento apimtį. Imtį sudaro 52 kibernetinių incidentų pranešimai, kurių CAAR skaičiuotas, pasitelkiant rinkos modelį įvairiais įvykio langų intervalais. T=0 yra pranešimo apie kibernetinį incidentą diena.

* - 90 proc. patikimumas

** - 95 proc. patikimumas

Iškelta hipotezė kibernetinių incidentų sukelta perteklinė grąža yra neigiama ir priklauso nuo įmonės kapitalizacijos, priimama.

4.2.4. CAAR vertinimas pagal kibernetinio incidento tipą

Suminių vidutinių perteklinių akcijų grąžų pagal kibernetinio incidento tipą, rodiklių reikšmės pateiktos 10 lentelėje. Nuodugniai išanalizavus imties pranešimų apie kibernetinius incidentus turinį, išskirti trys incidentų tipai – HACK, INSD, DISK (aprašymas yra pateiktas šio skyriaus pirmajame poskyryje). Pastebėta, tik dviejų iš jų (HACK ir INSD) įmonių akcijos sulaukė neigiamos investuotojų reakcijos. Rinkos reakcija į HACK tipo incidentus pakankamai stipresnė už INSD ir DISK tipo kibernetinius incidentus. CAAR reikšmės [-1,0] lange yra -1,9999 ir statistiškai reikšminga 95 proc. patikimu. INSD atvejų rinkos reakcija yra pakankamai neigiama – rinkos pokytis apie 2 proc., tačiau CAAR reikšmės nėra statistiškai reikšmingos nei viename įvykio lange. Tai reiškia, kad investuotojai nesureikšmina vidinių veiksnių poveikio kibernetinių incidentų aspekte, kaip galinčio prisidėti prie prastesnių įmonės rezultatų ateityje. Trečiojo tipo kibernetinių incidentų pranešimai DISC, kurie praneša apie netyčinius duomenų atskleidimus (el. laiško su konfidencialiais duomenimis išsiuntimas neteisingam gavėjui, konfidencialūs duomenys palikti be apsauginių slaptažodžių ir pan.), nesulaukė papildomos investuotojų reakcijos, nors pranešimuose buvo įvardijami pakankamai dideli duomenų kiekiai. Taip gali atsitikti todėl, kad investuotojai pasitiki įmone, ir jos sprendimais per pakankamai trumpą laiką pašalinti atsiradusias saugumo spragas.

13 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal kibernetinio incidento tipą

Kibernetinio incidento tipas	Įvykio langas	CAAR	pos:neg CAR	t-statistika
INSD	[-1, 1]	-0,0263	1:2	-1,5871
HACK	[-1, 1]	-0,0023	16:19	-0,5428
DISC	[-1, 1]	0,01	9:5	2,0088
INSD	[-2, 2]	-0,0103	1:2	-0,6396
HACK	[-2, 2]	-0,0039	14:21	-0,6643
DISC	[-2, 2]	0,016	10:4	2,2698
INSD	[-2, 1]	-0,0229	1:2	-1,1977
HACK	[-2, 1]	-0,0036	16:19	-0,8286
DISC	[-2, 1]	0,0107	10:4	1,7315
INSD	[-1, 2]	-0,0137	1:2	-0,9232
HACK	[-1, 2]	-0,0026	12:23	-0,4162
DISC	[-1, 2]	0,0154	11:3	2,5709
INSD	[0, 1]	-0,0291	1:2	-1,3901
HACK	[0, 1]	-0,0022	17:18	-0,4966
DISC	[0, 1]	0,004	8:6	1,0082
INSD	[-1, 0]	-0,0001	2:1	-0,0164
HACK	[-1, 0]	-0,0094**	15:20	-1,9999
DISC	[-1, 0]	0,0122	10:4	2,4737

Pastaba. Lentelėje parodytos suminės vidutinės perteklinės grąžos (CAAR) pagal rinkos segmentus. Imtį sudaro 52 kibernetinių incidentų pranešimai, kurių CAAR skaičiuotas, pasitelkiant rinkos modelį įvairiais įvykio langų intervalais. T=0 yra pranešimo apie kibernetinį incidentą diena. Lentelėje nurodyti aktualūs diskusijai rodikliai

* - 90 proc. patikimumas

** - 95 proc. patikimumas

Iškelta hipotezė kibernetinių incidentų sukelta neigiama perteklinė grąža priklauso nuo kibernetinio incidento tipo, priimama.

4.2.5. CAAR vertinimas pagal kibernetinio incidento apimtį

11 lentelėje matyti, investuotojų rinkos vertinimas pagal kibernetinio incidento apimtį. Išskirsčius imtį pagal kibernetinio incidento apimtį, t.y. duomenų kiekis, paveiktas kibernetinio incidento metu, paaiškėjo, kad reakcija į kibernetinį incidentą yra labai žema. CAAR reikšmės rodo neigiamą, tačiau labai nežymų pokytį akcijų kainoje vos nuo 0,1 proc. iki 1 proc., kai kibernetinio incidento apimtis siekia nuo 0 iki 500 tūkst. paveiktų duomenų. Pažymėtina, kad nulinė reikšmė pirmojoje imtyje (0-500 000), priskirta tiems pranešimams apie kibernetinius incidentus, kuriuose nenurodomas nutekintų duomenų skaičius kibernetinio incidento metu. Tai galėtų reikšti, kad investuotojai, labiau nepasitiki nežinoma kibernetinio incidento apimti, kurios reikšmė galėtų ateityje pasikeisti žinant tikslesnį mastą.

14 lentelė. Suminės vidutinės perteklinės akcijų grąžos pagal kibernetinio incidento apimtį

Kibernetinio apimtis	Įvykio langas	CAAR	pos:neg CAR	t-statistika
0-500 000	[-1, 1]	-0,0029	11:14	-0,6947
>500 000	[-1, 1]	0,0019	15:12	0,3613
0-500 000	[-2, 2]	-0,0044	10:15	-0,8212
>500 000	[-2, 2]	0,0061	15:12	0,8276
0-500 000	[-3, 3]	-0,0075	10:15	-1,3135
>500 000	[-3, 3]	0,0074	16:11	0,8459
0-500 000	[-4, 4]	-0,0046	10:15	-0,6339
>500 000	[-4, 4]	0,0026	15:12	0,277
0-500 000	[-5, 5]	-0,0052	9:16	-0,6808
>500 000	[-5, 5]	0,0065	13:14	0,583
0-500 000	[0, 1]	-0,0034	12:13	-1,0392
>500 000	[0, 1]	-0,0009	14:13	-0,1459
0-500 000	[-1, 0]	0,0006	12:13	0,2261
>500 000	[-1, 0]	-0,0013	15:12	-0,2711

Pastaba. Lentelėje parodytos suminės vidutinės perteklinės grąžos (CAAR) pagal kibernetinio incidento apimtį. Imtį sudaro 52 kibernetinių incidentų pranešimai, suskirstyti į dvi grupes, ir kurių CAAR skaičiuotas, pasitelkiant rinkos modelį įvairiais įvykio langų intervalais. T=0 yra pranešimo apie kibernetinį incidentą diena.

* - 90 proc. patikimumas

** - 95 proc. patikimumas

Tolimesnėje tyrimo dalyje, siekiant įvertinti tolimesnių dienų sumines vidutines perteklines akcijų grąžas, buvo suskaičiuota ilgesnio įvykio lango periodu [-5,10] šių grąžų rodikliai. Patikrinus patikimumą statistiškai reikšmingų pokyčių nepastebėta, visų CAAR rodikliai svyruoja -0,024 - 0,003 ribose, patikrinus t-statistika reikšmingumą, rezultatas statistiškai nereikšmingas, todėl atmetama prielaida, kad ilgesniame įvykio lange galėtų formuotis statistiškai reikšminga akcijų grąža. Patvirtinama, didžioji dalis pranešimų apie kibernetinius incidentus akcijų kainą veikia pirmosiomis dienomis po viešai paskelbto pranešimo.

Iškelta hipotezė kibernetinių incidentų sukelta perteklinė grąža neigiama ir yra didesnė tų įmonių, kurių kibernetinio incidento apimtis yra didesnė, atmetama.

4.3. Gautų tyrimų rezultatų palyginimas ankstesnių mokslinių publikacijų kontekste

Išanalizavus daugelio ankstesnių mokslo publikacijų, kuriose aprašomi atlikti tyrimai pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainų pokyčiams, prieita išvados, kad šie pranešimai gali turėti tam tikrą neigiamą įtaką akcijų kainai. Analizuojant pagal veiksnius, kuriuos ankstesniuose darbuose taikė kiti autoriai, galima teigti, kad galima identifikuoti veiksnius, kurie veikia akcijų kainą, tačiau skirtingu stiprumu.

Atlikus tyrimą buvo pastebėta, jog suskirsčius pranešimus apie kibernetinius incidentus pagal veiksnius, charakterizuojančius įmones ir kibernetinius incidentus, galima aprašyti statistinį įmonės prototipą, kurį veikia statistinis kibernetinis incidentas.

Taigi šiame tyrime nustatyta, kad dažniausiai atskleistų pranešimų apie kibernetinius incidentus poveikį akcijų kainų pokyčiui turi įmonės:

- priklauso rinkos segmentui:

a) finansinės;
b) paslaugų;

- pagal Kapitalizaciją yra:

a) vidutinio dydžio (kapitalizacija nuo 2 iki 10 mlrd.).

- Šias įmones veikia kibernetiniai incidentai:

a) HACK tipo (išorinių veiksnių poveikis – „Malware“, „Ransomware“ ir panašūs neautorizuoti įsibrovimai),
b) nepriklausomai kokios apimties kibernetinis incidentas.

Tyrime nustatyta, kad stipriausiai ir reikšmingiausiai įtaka akcijų kainai pasireiškė [-2,1] įvykio lango intervale, kas patvirtina autorių Rosati, (2017), Smith, (2018), Tweneboah-Kodua, (2018) teiginį, kad kibernetiniai incidentai akcijų kainų pokyčiams daro laikiną, trumpo periodo poveikį. Kitomis dienomis po pranešimo nebestebimi neigiami akcijų pokyčiai. Todėl galima teigti, kad visa neigiama informacija po pranešimo apie kibernetinį incidentą jau atsispindėjo akcijų kainoje.

Aptariant rinkos segmento veiksnius galima pastebėti, kad finansinių įmonių atveju rinka pirmą kartą sureaguoja labai anksti į pranešimus apie kibernetinius incidentus. Reakcijos požymių yra kelios dienos prieš ir dieną po įvykio. Įdomu pažymėti, kad autoriai, kurie atliko tyrimus iki 2016 m., teigia, kad investuotojai neigimai reaguoja į informacinių technologijų įmonių pranešimus apie kibernetinius incidentus (Campbel, 2003, Yayla ir kt., 2011), priešingai, pastarųjų metų tyrimų autoriai nurodo, kad investuotojai tiki informacinių technologijų įmonių gebėjimu operatyviai sureaguoti į kibernetinius incidentus ir turi tam pakankamai lėšų, todėl šiuo metu reikšmingos neigiamos reakcijos sulaukia finansinio rinkos segmento įmonės (Amir ir kt. 2018; Colivicci ir Vignaroli, 2019; Tweneboah-Kodua, 2018).

Labai svarbus rinkos segmentas paslaugos, kurios, šio tyrimo atveju apima, viešbučių, maitinimo įstaigų paslaugas. Investuotojų reakcija labai stipri neigiamai net keturias dienas po pranešimo apie įvykusius kibernetinius incidentus. Iš šių požymių galima spręsti, kad informacija apie incidentą buvo labai reikšmingai įvertinta investuotojų. Informacija į akcijos kainą inkorporavosi labai aiškia neigiama tendencija. Darytina išvada, kad nutekinti duomenys galėjo būti pakankami konfidencialūs ir didelio skaičiaus vartotojų, jog sulaukta stiprios neigiamos reakcijos.

Kitas įmonių imties skirstymo veiksnys, turėjęs nedidelio reikšmingumo rezultatams yra kapitalizacija. Pastebėta, jog šis veiksnys generuoja reikšmingą neigiamą poveikį akcijų kainoms tų įmonių, kurių kapitalizacija yra intervale nuo 2 iki 10 mlrd. Šios įmonės priskirtos vidutinio dydžio įmonėms. Didelės ir labai didelės įmonės, šiuo atveju, neturėjo reikšmingos neigiamos reakcijos (Tweneboah-Kodua, 2018). Tai reikštų, kad investuotojai pasitiki „mega“ įmonių įtaka, prestižu, gera valia (išmokamos kompensacijos) padedant nukentėjusiems klientams, todėl nemato prasmės parduoti akcijas ir sukelti rinkos svyravimus.

Neigiamas poveikis akcijų kainai stebimas labai trumpu laikotarpiu, praktiškai, tik pranešimo dieną, kas leidžia pritarti Rosati, (2017) tyrimo rezultatams, tačiau tyrime stebėtos didesnės neigiami akcijų pokyčiai leidžia paneigti šios autorės mintis, jog tik dėl didelių įmonių investuotojai kelia susirūpinimą, kai kabama apie kibernetinius incidentus.

Dar vienas svarbus veiksnys, pagal kurį galima spręsti kokio tipo kibernetinis incidentas įvykdytas yra incidento tipas. Pagal surinktų pranešimų apie kibernetinius incidentus pobūdį šis yra dažiausiai minimas ir ankstesnių tyrimų autorių Yayla ir kt., 2011, Shinichi‘o ir kt., 2018 ir Colivicci ir Vignaroli, 2019 bei Kammoun ir kt., kaip vienas iš reikšmingą akcijų kainai poveikį turinčių veiksnių. Neautorizuoti įsibrovimai į įmonių tinklus arba kitaip vadinami „hacking“ tipo kibernetiniai incidentai įmonių atžvilgiu gali turėti nepataisomos žalos, todėl atskleistas pranešimas apie tokio tipo kibernetinį incidentą tyrime turėjo įtakos akcijų kainų pokyčiui. Tyrime stebėtas pranešimo dienoje reikšmingai neigiama investuotojų reakcija, tačiau išsisėmė po kelių neigiamos rinkos krypties dienų. Tokios tendencijos leidžia patvirtinti autorių Bianchi ir kt., 2019 ir Colivicci ir Vignaroli, 2019.

Svarbu paminėti, reikšmingai neigiama rinkos reakcija dažniausiai stebėta dvi dienos prieš pranešimą ir viena diena po pranešimo, tik finansinių ir paslaugų įmonių atveju neigiama perteklinė grąža generuojama keturių dienų prieš ir keturių dienų po pranešimo apie kibernetinius incidentus intervale. Tai galima paaiškinti tuo, kad pranešimai įvairiuose interneto portaluose pasirodo ne visada tą pačią dieną, todėl gali būti, kad investuotojai kas kart pastebėję ar išgirdę gandų (iracionalių investuotojų atveju), priima sprendimą parduoti akcijas. Akivaizdu, kad pranešimai apie kibernetinius incidentus sukelia tik trumpalaikio akcijų nuosmukio tendencijas (Rosati, 2017; Smith, 2018).

Taigi, apibendrinus gautus rezultatus, galima teigti, jog šiame tyrime dalis iškeltų hipotezių yra priimamos, nors vienareikšmiškai tvirtinti, kad visi atskleisti pranešimai apie kibernetinius incidentus turi vienodai reikšmingą įtaką įmonių akcijų kainų pokyčiams negalima.

Paminėtina, kad tokių išvadų priežastis galėtų būti per siaura tyrimo imtis, kadangi pranešimų apie kibernetinius incidentus įmonės ne visada linkusios viešinti žiniasklaidoje, o paieška tarp daugybės kitų nefinansinių pranešimų apsunkina tyrėjo darbą. Duomenų gavimas yra pakankamai probleminis, jei tie duomenys nėra viešai prieinami ar yra mokami Taip pat paminėtina, jog padaryta prielaida apie pranešimo išplatinimo metu teoriškai neįvyksiantį įmonei svarbų įvykį, ne visada pasiteisina, todėl dviejų skirtingų įvykių („gero-blogo“) sinergija gali turėti „lengvesnį“ poveikį įmonių akcijų kainai.

Akcentuojant, svarbu paminėti, kad tyrimas pagrindė tik trumpalaikę, atskleistų pranešimų apie kibernetinius incidentus, įtaką įmonių akcijų kainoms. Tokią išvadą patvirtina analizuotoje mokslinėje literatūroje aptartų tyrimų autoriai.

Ateityje gali būti atlikti tolimesni tyrimai, kuriuose analizuojama pranešimų apie kibernetinius incidentus atskleidimo įtaka įmonių akcijų kainų pokyčiams, sudarant didesnę imtį pagal metus, lyginant rezultatus skirtingais laikotarpiais. Praplečiant tyrimą į kitas rinkas, gauti rezultatai galėtų parodyti ir kitų rinkų investuotojų požiūrį į pranešimus apie kibernetinius incidentus.

Išvados

1. Atlikus pranešimų apie kibernetinius incidentus atskleidimo įtakos įmonių akcijų pokyčiams tyrimą, galima daryti šias išvadas:
2. Šiame darbe analizuojama problema, pranešimų apie kibernetinius incidentus įtaka įmonių akcijų kainai, jau kelis dešimtmečius nagrinėjama mokslo visuomenės., todėl šiame projekte paliesta tematika aktuali ne tik įmonėms, bet ir investuotojams priimant sprendimus.
3. Verslo įmonės keičia tradicinius verslus į skaitmeninius verslus, diegiamos debesų kompiuterijos paslaugos, daiktų internetas išgyvena pakilimą. Už visų šių globalaus pasaulio naujovių atsiranda duomenų nutekėjimo problema, kurios pagrindinis variklis yra kibernetiniai incidentai. Šiame darbe analizuojama problema, pranešimų apie kibernetinius incidentus įtaka įmonių akcijų kainai, jau kelis dešimtmečius nagrinėjama mokslo visuomenės, todėl šiame projekte paliesta tematika aktuali įmonėms, bei investuotojams.
4. Literatūros analizė pateikia įžvalgų, kad norint apsaugoti intelektinį turtą nuo kibernetinių incidentų, reikėtų, visų pirma suprasti kaip veikia, kokių motyvų vedami sukeliami bei kas skatina šiuos incidentus. Prieinama išvados, kad išaiškintos kibernetinių incidentų prielaidos, padėtų išvengti arba sušvelninti ateityje įvyksiančių kibernetinių incidentų bei su jais susijusių neigiamų akcijų kainų pokyčių.
5. Kibernetiniai incidentai remiasi šiais kertiniais taškais – technologijų spragos ir žmogiškasis veiksnys.
6. Įmonių akcijų kaina paveikiama informacijos apie kibernetinę ataką ir jos sukeliamos žalos.
7. Kalbant apie kibernetinių incidentų poveikį, pirminiame lygmenyje, reikėtų vertinti tiesiogines ir netiesiogines pasekmes. Tai svarbūs akcentai investuotojams, ieškantiems atsakymų kokia žala gali paveikti įmonę kibernetinis incidentas ir įmonėms, norinčioms ateityje apsaugoti savo intelektinį turtą nuo kibernetinių incidentų. Su šiuo teiginiu siejama išvada, kad aiškiai įvardintos ir pamatuotos grėsmės yra pagrindas ateityje išvengti ar sušvelninti rizikas dėl nesibaigiančių kibernetinių incidentų.
8. Remiantis literatūros analizėje pateiktais autorių duomenimis apie informacijos saugos sistemos įmonėje svarbą kaip prevencijos priemonę nuo kibernetinių incidentų ir investuotojų požiūrio į įmonės nusiteikimą apsaugoti klientų duomenis, darytina išvada, kad investuotojai įvertina pozityviai informacijos saugos sistemos naudą, kas pozityviai atsiskleidžia investavimo pasirinkime.
9. Svarbi įžvalga atsiranda kalbant apie kibernetinius incidentus lemiančius veiksnius, kai yra kalbama apie žmogiškąjį faktorių, nulemiančius kibernetinio incidento vyksmą. Yra konstatuojama, kad bene daugiausiai kibernetinių incidentų įvyksta dėl žmogiškojo faktoriaus (paspausta nuoroda, atidarytas kenkėjiškas laiškas, išsiųsti duomenys neteisingam adresatui ir pan.). Šią įžvalgą patvirtina atliktame tyrime stebima 64 proc. įsilaužimo tipo kibernetinių incidentų. Galima teigti, kad be žmogiškojo faktoriaus tokie incidentai vyktų rečiau.
10. Analizuojant ankstesniuose tyrimuose taikytus metodus, nustatyta, kad dažniausiai pranešimų apie kibernetinius incidentus atskleidimo įtakos akcijų kainai tyrimuose naudojamas įvykio analizės metodas. Su šiuo faktu sutinka visi autoriai, tačiau nežymiai jų nuomonė išsiskiria dėl tinkamo grąžos skaičiavimui taikomo modelio pasirinkimo. Tyrimuose, grąžos skaičiavimui, randami pritaikyti keli skirtingi modeliai, tačiau, vėliau, tyrimų pabaigoje daugelis autorių konstatuoja, kad neverta naudoti pakankami apsunkintus

ir neekonomiškus laiko atžvilgiu modelius, kurių reikšmingumai rezultatuose nežymiai skiriasi nuo rinkos modelio.

11. Susisteminus tyrimo imtį pagal pasirinktus veiksnius pastebėta, kad didžiausias pranešimų apie kibernetinius incidentus augimo šuolis įvyksta per 2016-2017 metus. Ypač išauga didelės apimties kibernetinių incidentų. Literatūros analizėje panaudoti statistiniai duomenys pateikia panašias tendencijas.
12. Analizuojant tyrimo imtį galima tvirtinti, kad dažniausiai kibernetinių incidentų atakuojamos yra informacinių technologijų įmonės, tačiau remiantis atliktos tyrimo dalies rezultatais, kai imtis buvo padalinta pagal rinkos segmentus, galima daryti išvadą, kad informacinių technologijų įmonės akcijų kainos neturi poveikio dėl šių incidentų. Tai atsitinka dėl investuotojų pasitikėjimo informacinių technologijų įmonių finansiniu stiprumu ir technologinėmis galimybėmis pažaboti kibernetinius incidentus.
13. Išnagrinėjus dar kelis rinkos segmento imties atvejus, galima teigti, kad tendencijos dėl atskleistų pranešimų apie kibernetinius incidentus poveikio skirtingų įmonių akcijų kainoms tendencija, metams einant, keičiasi. Tokia išvada padaryta stebint tyrimų rezultatus literatūros analizėje, kai prieš gerą dešimtmetį informacinių technologijų įmonės patirdavo neigiamus akcijų šuolius, atskleidus pranešimus apie kibernetinius incidentus, tačiau iš dabartinių tyrimų rezultatų matyti, jog pastaruosius keletą metų šias tendencijas perima paslaugų ir finansų įmonės. Suprantama, kad šios įmonės labiau atkreipia programišių dėmesį dėl kaupiamų klientų duomenų jautrumo (kredito kortelių duomeny, finansinės atskaitos ir pan.).
14. Tyrimo rezultatai parodė, kad pranešimai apie kibernetinius incidentus turi neigiamą poveikį įmonių akcijų kainai pranešimo paskelbimo dieną ir dažniausiai dvi dienas po paskelbimo. Tokios išvados pagrindu nulinė hipotezė buvo atmesta, o tai reiškia, kad pranešimų apie kibernetinius incidentus atskleidimas turi įtakos įmonių akcijų kainai.
15. Galiausiai svarbu pabrėžti, kad tyrimo metu gauti informatyvesni rezultatai, tik suskirsčius duomenų imtį pagal įmones ir kibernetinius incidentus charakterizuojančius veiksnius, todėl ateityje, atliekant panašius tyrimus rekomenduojama laikytis šios tyrimo logikos.

Informacijos šaltinių sąrašas

1. Abdel-Meguid, A., Fernando, G.D., Schneible, R.A. and Suh, S. (2016), "Trading volume and earnings quality", Working Paper, University at Albany.
2. Abhishta, A., Joosten, R., & Nieuwenhuis, L. J. M. (2017). Comparing Alternatives to Measure the Impact of DDoS Attack Announcements on Target Stock Prices. *Journal of wireless mobile networks, ubiquitous computing, and dependable applications*, *8*(4), 1-18. https://doi.org/10.22667/JOWUA.2017.12.31.001
3. Ahmad, Z., Ibrahim, H. and Tuyon, J. (2017), "Institutional investor behavioral biases: syntheses of theory and evidence", *Management Research Review*, Vol. 40 No. 5, pp. 578-603. https://doi.org/10.1108/MRR-04-2016-0091
4. Amir, E., Levi, S., & Livne, T. (2018). Do Firms Underreport Information on Cyber-Attacks?
5. Ang J.S., Zhang S. (2015) Evaluating Long-Horizon Event Study Methodology. In: Lee CF., Lee J. (eds) Handbook of Financial Econometrics and Statistics. Springer, New York, NY https://doi.org/10.1007/978-1-4614-7750-1_14
6. Arcuri, M., C., Brogi, M. and Gandolfi, G., 2017. How does cyber crime affect firms? The effect of information security breaches on stock returns. In: *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, Venice, Italy, 2017.
7. Ashley, J. W. (1962). Stock Prices and Changes in Earnings and Dividends: Some Empirical Results. J. Polit. Econ, 70(1), 82-85.
   Available SSRN: https://ssrn.com/abstract=3190454 or http://dx.doi.org/10.2139/ssrn.3190454
8. Azmi, R., Tibben, W. and Win, K.T. (2018), "Review of cybersecurity frameworks: context and shared concepts", Journal of Cyber Policy, Vol. 3 No. 2, pp. 258-283, doi: 10.1080/23738871.2018.1520271.
9. Ball, R. y Brown, P. (1968). An Empirical Evaluation of Accounting Income Numbers. J. Acc. Res. , Autumn, 6(2), 159-78.
10. Barron, O., Schneible, R. and Stevens, D. (2018), "The changing behavior of trading volume reactions to earnings announcements: evidence of the increasing use of accounting earnings news by investors", forthcoming Contemporary Accounting Research.
11. Berkman, H., Jona, J., Lee, G. and Soderstrom, N. (2018), "Cybersecurity awareness and marketvaluations", Journal of Accounting and Public Policy, Vol. 37 No. 6, pp. 508-526, doi: 10.1016/j.jaccpubpol.2018.10.003.
12. Bernardi, C., & Stark, A. W. (2018). Environmental, social and governance disclosure, integrated reporting, and the accuracy of analyst forecasts doi:https://doi.org/10.1016/j.bar.2016.10.001
13. Bianchi, D. and Tosun, O., Cyber Attacks and Stock Market Activity (January 19, 2019).
14. Blankespoor, E., Miller, G.S., White, H. D., (2016) The role of dissemination in market liquidity: Evidence from firms' use of Twitter™ The Accounting Review, 89 (1), pp. 79-112,
15. Brody, R.G., Chang, H.U. and Schoenberg, E.S. (2018), "Malware at its worst: death and destruction", International Journal of Accounting and Information Management, Vol. 26 No. 4, pp. 527-540.
16. Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. Journal of Computer Security, 11, 431-448. https://doi.org/10.3233/JCS-2003-11308

17. Chan, K.C., Chen, N.F. and Hsieh, D.A. (1985), “An exploratory investigation of the firm size effect”, Journal of Financial Economics, Vol. 14 No. 3, pp. 451-471.
18. Chang, L.Y., Wong, S.F., Eze, U. and Lee, H. (2019), “The effect of IT ambidexterity and cloud computing absorptive capacity on competitive advantage”, Industrial Management & Data Systems, Vol. 119 No. 3, pp. 613-638, available at: https://doi.org/10.1108/IMDS-05-2018-0196
19. Chen, N.F. (1991), “Financial investment opportunities and the macroeconomy”, Journal of Finance, Vol. 46 No. 2, pp. 529-554.
20. Chen, W., Han, J. and Tan, H.T. (2016), “Investor reactions to management earnings guidance attributions: the effects of news valence, attribution locus, and outcome controllability”, accounting”, Organizations and Society, Vol. 55, pp. 83-95.
21. Colivicchi, I. and Vignaroli, R. (2019) Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest. Journal of Mathematical Finance, 9, 402-454. https://doi.org/10.4236/jmf.2019.93024
22. David E. Allen & Michael McAleer & Abhay K. Singh, 2019. "Daily market news sentiment and stock prices," Applied Economics, Taylor & Francis Journals, vol. 51(30), pages 3212-3235, June.
23. Dolley, J. C. (1993). Characteristics and Procedure of Common Stock Split-Ups. Harvard Bus. Rev., Apr. 1933, 11, 316-26.
24. Evans, M., He, Y., Yevseyeva, I. and Janicke, H. (2019), "Published incidents and their proportions of human error", Information and Computer Security, Vol. 27 No. 3, pp. 343-357. https://doi.org/10.1108/ICS-12-2018-0147

    Evidence from Capital Markets. *Review of Accounting Studies*, 23, 1177-1206
25. F. Douglas Foster and Professor Petko S. Kalev, P., Xu, X., Ramiah, V., Moosa, I. and Davidson, S. (2016), "An application of the information-adjusted noise model to the Shenzhen stock market", *International Journal of Managerial Finance*, Vol. 12 No. 1, pp. 71-91.
26. Fama et al. (1969). □e Adjustment Of Stock Prices To New Information. International Economic Review, 10 (1), 1-21. https://doi.org/10.2307/2525569
27. Fama, E. F. (1991). Efficient Capital Markets: Journal of Finance, 46 (5), 383-417. https://doi.org/10.2307/2328565
28. Felimban, R., Floros, C. and Nguyen, A. (2018), "The impact of dividend announcements on share price and trading volume: Empirical evidence from the Gulf Cooperation Council (GCC) countries", *Journal of Economic Studies*, Vol. 45 No. 2, pp. 210-230. https://doi.org/10.1108/JES-03-2017-0069
29. Fernando, G., Giboney, J. and Schneible, R. (2018), "Voluntary disclosures and market response to earnings announcements", *Review of Accounting and Finance*, Vol. 17 No. 1, pp. 2-17. https://doi.org/10.1108/RAF-06-2016-0087
30. French, J. (2018), "Market moods: an investor sentiment event study", *Foresight*, Vol. 20 No. 5, pp. 488-506. https://doi.org/10.1108/FS-02-2018-0018
31. Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018), “Investigating the information security management role in smart city organisations”, World Journal of Entrepreneurship, Management and Sustainable Development, Vol. 14 No. 1, pp. 86-98, doi: 10.1108/WJEMSD-07-2017-0042.

32. Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), "The relationship between board-level technology committees and reported security breaches", Journal of Information Systems, Vol. 30 No. 3, pp. 79-98, doi: 10.2308/isys-51402
33. Horne, C.A., Maynard, S.B. and Ahmad, A. (2017), "Organisational information security strategy: review, discussion and future research", Australasian Journal of Information Systems, Vol. 21, doi: 10.3127/ajis.v21i0.1427.
34. Hwang, I., Kim, D., Kim, T. and Kim, S. (2017), "Why not comply with information security? An empirical approach for the causes of non-compliance", Online Information Review, Emerald Publishing Limited, Vol. 41 No. 1, pp. 2-18, doi: 10.1108/OIR-11-2015-0358.
35. Yang, J., Segara, R. and Feng, J. (2019), "Stock price movements and trading behaviors around merger and acquisition announcements: Evidence from the Korean stock market", *International Journal of Managerial Finance*, Vol. 15 No. 4, pp. 593-610. https://doi.org/10.1108/IJMF-07-2018-0204
36. Yang, L., Lau, L. and Gan, H. (2020), "Investors' perceptions of the cybersecurity risk management reporting framework", International Journal of Accounting & Information Management, Vol. 28 No. 1, pp. 167-183. https://doi.org/10.1108/IJAIM-02-2019-0022
37. Jain, J., Walia, N. and Gupta, S. (2019), "Evaluation of behavioral biases affecting investment decision making of individual equity investors by fuzzy analytic hierarchy process", *Review of Behavioral Finance*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/RBF-03-2019-0044
38. Joakim Westerholm, P., Mudalige, P., Kalev, P. and Duong, H. (2016), "Individual and institutional trading volume around firm-specific announcements", *International Journal of Managerial Finance*, Vol. 12 No. 4, pp. 422-444. https://doi.org/10.1108/IJMF-01-2016-0007
39. Jouini, M., Rabai, L.B.A. and Aissa, A.B. (2014), "Classification of security threats in information systems", Procedia Computer Science, Vol. 32, pp. 489-496.

    Journal of Accounting and Finance, 15 (3), pp. 39-52

    Journal of Information Systems, 29 (2) (2015), pp. 107-136, 10.2308/isys-50994
40. Juma'h, A. and Alnsour, Y. (2020), "The effect of data breaches on company performance", International Journal of Accounting & Information Management, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJAIM-01-2019-0006
41. Kammoun, N., Bounfour, A., (2019), Altay Özaygen & Rokhaya Dieye Financial market reaction to cyberattacks, Cogent Economics & Finance , 7:1645584
42. Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S. and Ramanauskaite, S. (2017), "High-level self-sustaining information security management framework", Baltic Journal of Modern Computing, Vol. 5 No. 1, p. 107, doi: 10.22364/bjmc.2017.5.1.07.
43. L. Liu, L., Wu, J., Li, P., Q. (2015)LiA social-media-based approach to predicting stock comovement Expert Systems with Applications, 42 (8) , pp. 3893-3901,
44. Layton, R., and P. A. Watters. 2014. A methodology for estimating the tangible cost of data breaches. Journal of Information Security and Applications 19 (6): 321–330. https://doi.org/10.1016/j.jisa.2014.10.012
45. Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate Governance, Social Responsibility,and Data Breaches. *Financial Review*, 53, 413-455.

46. McLeod, A. and Dolezel, D. (2018), “Cyber-analytics: modeling factors associated with healthcare data breaches”, Decision Support Systems, Vol. 108, pp. 57-68, doi: 10.1016/J.DSS.2018.02.007.
47. McWilliams, A., Siegel, D. (1997), „Event studies in management research: theoretical and empirical issues“, Academy of Management Journal, Vol. 40, No. 3, pp. 626-657
48. Myers et al. (1948). In□uence of Stock Split-Ups on Market Price. Harvard Bus. Rev, 251-55
49. Morgan, S. (2016), “Cyber crime costs projected to reach $2 trillion by 2019”, Forbes. 17 Jan. 2016, available at: www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillionby-2019/#81fe0503bb0c (accessed 2 October 2016).
50. Mutuku, C. and Ng’eny, K. (2015), “Macroeconomic variables and the kenyan equity market: a time series analysis”, Business and Economic Research, Vol. 5 No. 1, pp. 1-10.
51. Nicho, M. (2018), “A process model for implementing information systems security governance”, Information and Computer Security, Vol. 26 No. 1, pp. 10-38, doi: 10.1108/ICS-07-2016-0061.
52. Ozo, F. and Arun, T. (2019), "Stock market reaction to cash dividends: evidence from the Nigerian stock market", *Managerial Finance*, Vol. 45 No. 3, pp. 366-380. https://doi.org/10.1108/MF-09-2017-0351
53. Pearce, D.K. and Roley, V.V. (1983), “The reaction of stock prices to unanticipated changes in money: a note”, Journal of Finance, Vol. 38 No. 4, pp. 1323-1333.
54. Pearce, D.K. and Roley, V.V. (1983), “The reaction of stock prices to unanticipated changes in money: a note”, Journal of Finance, Vol. 38 No. 4, pp. 1323-1333.
55. Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. Journal of Information Security and Applications, 19, 257-271.
56. Prokofieva, M., Twitter-based dissemination of corporate disclosure and the intervening effects of firms’ visibility: Evidence from Australian-listed companies
57. Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H. (2015), “Empirical evaluation of a cloud computing information security governance framework”, Information and Software Technology, Vol. 58, pp. 44-57.
58. Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. International Review of Financial Analysis, 49, 146-154.
59. Roztocki, Narcyz and Weistroffer, Heinz Roland, "Event Studies in Information Systems Research: An Updated Review" (2009). *AMCIS 2009 Proceedings*. 191. https://aisel.aisnet.org/amcis2009/191
60. Schatz, D. and Bashroush, R. (2016), "The impact of repeated data breach events on organisations’ market value", Information and Computer Security, Vol. 24 No. 1, pp. 73-92. https://doi.org/10.1108/ICS-03-2014-0020 Download as .RIS
61. Schmidt, P.J., Wood, J.T. and Grabski, S.V. (2016), “Business in the cloud: research questions on governance, audit, and assurance”, Journal of Information Systems, Vol. 30 No. 3, pp. 173-189
62. Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper No. 24409 March 2018, Revised July 2018

63. Smith, K., Jones, A., Johnson, L. and Smith, L. (2019), "Examination of cybercrime and its effects on corporate stock value", Journal of Information, Communication and Ethics in Society, Vol. 17 No. 1, pp. 42-60. https://doi.org/10.1108/JICES-02-2018 0010 Download as .RIS
64. Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", International Journal of Information Management, Vol. 36 No. 2, pp. 215-225, doi: 10.1016/j.ijinfomgt.2015.11.009.
65. Spanos, G. and Angelis, L. (2016), "The impact of information security events to the stock market: asystematic literature review", Computers and Security, Vol. 58, pp. 216-229. [2 kartus]
66. Sprenger, A. Tumasjan, P.G. Sandner, I.M. Welpe (2015) Tweets and trades: The information content of stock microblogs European Financial Management, 20 (5), pp. 926-957,
67. Strauss, N. and Smith, C. (2019), "Buying on rumors: how financial news flows affect the share price of Tesla", *Corporate Communications: An International Journal*, Vol. 24 No. 4, pp. 593-607. https://doi.org/10.1108/CCIJ-09-2018-0091
68. Tversky, A. and Kahneman, D. (1974), "Judgment Under Uncertainty: Heuristics and Biases", Science, Vol. 185, pp. 1124-31.
69. Tweneboah-Kodua, S., Atsu, F. and Buchanan, W. (2018), "Impact of cyberattacks on stock performance: a comparative study", Information and Computer Security, Vol. 26 No. 5, pp. 637-652. https://doi.org/10.1108/ICS-05-2018-0060 Download as .RIS

Interneto nuorodos

Statista.com [žiūrėta 2020-02-10] prieiga internete https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Morgan, S. 2017b. 2018 cybersecurity market report. [žiūrėta 2019-10-19], prieiga interenete https://cybersecurityventures.com/cybersecurity-market-report/

American Institute of Certified Public Accountants (AICPA (2018b), "SOC for cybersecurity: a backgrounder", [žiūrėta 2020-01-05] nuoroda internete:

www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-backgrounder.pdf

Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 [žiūrėta 2020-04-17] prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf

Harris, K. (2016), "California data breach report 2012-2015", [žiūrėta 2020-04-05], prieiga interenete https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

Commity on National Security Systems, *National Information Assurance (IA) Glossary* (2010, Nr. 4009), p. 22 [žiūrėta 2020-04-05] prieiga internete https://www.hsdl.org/?abstract&did=7447

Schimmer, M., Levchenko, A., and Müller, S. (2014). EventStudyTools (Research Apps), St.Gallen. prieiga internete: www.eventstudytools.com. [žiūrėta 2020-04-10]

Ponemon Institute. 2017. 2019 cost of cyber crime study: Global. Available at: https://www.ibm.com/downloads/cas/ZYKLN2E3

IBM security, Ponemon Institute 2019 How much would a data breach cost your bussiness. 2019 Cost os a Data Breach Report [žiūrėta 2020-02-15] prieiga per internetą https://www.ibm.com/security/data-breach?cm_sp=CTO-_-en-US-_-ZBZLY7KL

De Groot, J. 2019. The history of data breaches. Available at: https://digitalguardian.com/blog/history-data-breaches

The Economic Impact of Cybercrime No Slowing Down [žiūrėta 2020-04-30] prieiga per internetą https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Priedai

1 priedas. Suminės vidutinės perteklinės akcijų grąžos pagal rinkos segmentus

	Įvykio langas	CAAR	t-statistika
Finansai	(-1, 1)	-0,0188	-1,6283*
Informacinės technologijos	(-1, 1)	0,0061	1,2219
Sveikatos apsauga	(-1, 1)	-0,0011	-0,1156
Paslaugos	(-1, 1)	-0,0076	-1,3112
Kasdienio vartojimo prekės	(-1, 1)	0,0053	1,1263
Finansai	(-2, 2)	-0,0164	-1,4012
Informacinės technologijos	(-2, 2)	0,0087	1,2632
Sveikatos apsauga	(-2, 2)	-0,0003	-0,0257
Paslaugos	(-2, 2)	-0,0141	-1,6291*
Kasdienio vartojimo prekės	(-2, 2)	0,0296	2,7581
Finansai	(-3, 3)	-0,0066	-0,36
Informacinės technologijos	(-3, 3)	0,0036	0,4467
Sveikatos apsauga	(-3, 3)	-0,0102	-0,7258
Paslaugos	(-3, 3)	-0,0119	-1,8716*
Kasdienio vartojimo prekės	(-3, 3)	0,0636	1,6053
Finansai	(-4, 4)	-0,0322	-1,5287*
Informacinės technologijos	(-4, 4)	0,0009	0,1033
Sveikatos apsauga	(-4, 4)	0,0101	0,6769
Paslaugos	(-4, 4)	-0,0102	-1,4882*
Kasdienio vartojimo prekės	(-4, 4)	0,0759	2,4804
Finansai	(-5, 5)	-0,0239	-1,3378
Informacinės technologijos	(-5, 5)	-0,0003	-0,0325
Sveikatos apsauga	(-5, 5)	0,0145	0,8789
Paslaugos	(-5, 5)	-0,0079	-0,6515
Kasdienio vartojimo prekės	(-5, 5)	0,0834	1,556
Finansai	(-1, 2)	-0,0132	-0,8903
Informacinės technologijos	(-1, 2)	0,0089	1,2804
Sveikatos apsauga	(-1, 2)	-0,0044	-0,3056
Paslaugos	(-1, 2)	-0,0097	-1,1099
Kasdienio vartojimo prekės	(-1, 2)	0,0226	4,7474
Finansai	(-1, 3)	-0,0012	-0,0497
Informacinės technologijos	(-1, 3)	0,0112	1,6419*
Sveikatos apsauga	(-1, 3)	-0,0093	-1,0514
Paslaugos	(-1, 3)	-0,009	-1,2952
Kasdienio vartojimo prekės	(-1, 3)	0,0455	1,6308
Finansai	(-1, 5)	-0,0033	-0,1184
Informacinės technologijos	(-1, 5)	0,0108	1,3094
Sveikatos apsauga	(-1, 5)	0,0066	0,6295
Paslaugos	(-1, 5)	-0,0012	-0,1181
Kasdienio vartojimo prekės	(-1, 5)	0,03	1,8379
Finansai	(-1, 4)	-0,0044	-0,1677
Informacinės technologijos	(-1, 4)	0,0086	1,1064

Sveikatos apsauga	(-1, 4)	0,0037	0,3885
Paslaugos	(-1, 4)	-0,0091	-1,2983
Kasdienio vartojimo prekės	(-1, 4)	0,0358	7,099
Finansai	(-2, 1)	-0,022	-1,9409*
Informacinės technologijos	(-2, 1)	0,006	1,1695
Sveikatos apsauga	(-2, 1)	0,003	0,2453
Paslaugos	(-2, 1)	-0,0121	-1,9799*
Kasdienio vartojimo prekės	(-2, 1)	0,0124	9,96
Finansai	(-1, 0)	-0,0026	-0,5536
Informacinės technologijos	(-1, 0)	0,0059	1,7243
Sveikatos apsauga	(-1, 0)	-0,0053	-0,5528
Paslaugos	(-1, 0)	-0,0114	-1,3871*
Kasdienio vartojimo prekės	(-1, 0)	-0,0048	-0,343
Finansai	(0, 1)	-0,0216	-1,8662*
Informacinės technologijos	(0, 1)	0,0032	0,5899
Sveikatos apsauga	(0, 1)	0,0015	0,2519
Paslaugos	(0, 1)	-0,0084	-1,6931*
Kasdienio vartojimo prekės	(0, 1)	0,0032	2,0968

Pastaba. - *90 proc. patikimumas,** - 95 proc. patikimumas. Rinkos segmentams klasifikuoti naudojamas JAV pramonės klasifikavimo standartas (Standard Industrial Clasification - SIC).

2 priedas. Pranešimų apie kibernetinius incidentus datos ir įmonės

Pranešimo data	Įmonės pavadinimas	Pranešimo data	Įmonės pavadinimas
2015-01-05	Morgan Stanley	2017-05-04	Alphabet, Inc. - Google+
2015-01-06	NVIDIA Corporation	2017-08-30	Facebook, Inc.
2015-02-04	Anthem, Inc	2017-09-17	Equifax Inc.
2015-04-03	Microsoft Corporation	2017-09-25	Adobe Inc.
2015-05-12	Starbucks Corporation	2017-10-12	T-Mobile US, Inc
2015-07-18	CVS Health Corporation	2017-11-17	Yum! Brands, Inc.
2015-10-01	T-Mobile US, Inc	2018-01-22	The Coca-Cola Company
2015-11-10	JPMorgan Chase & Co.	2018-02-19	FedEx Corporation
2016-01-26	Centene Corporation	2018-03-14	United Parcel Servise, Inc
2016-03-16	PerkinElmer, Inc.	2018-03-20	Expedia Group, Inc.
2016-05-03	The Charles Schwab Corporation	2018-03-30	Under Armour, Inc.
2016-05-06	Alphabet, Inc. - Google+	2018-04-06	Delta Air Lines, Inc.
2016-05-17	Microsoft Corporation	2018-04-20	Expedia Group, Inc.
2016-06-13	Twitter Inc.	2018-05-01	Lincoln National Corporation
2016-07-30	The Walt Disney Company	2018-05-24	T-Mobile US, Inc
2016-08-08	Oracle Corporation	2018-06-12	Facebook, inc.
2016-11-23	Hewlett Packard Enterprise Company	2018-09-28	Facebook, Inc.
2016-11-30	Alphabet, Inc. - Google+	2018-10-08	Alphabet, Inc. - Google+
2016-12-05	CVS Health Corporation	2018-11-30	Marriott International
2016-12-07	T-Mobile US, Inc	2018-11-30	Marriott International, Inc.
2017-02-27	The Boeing Corporation	2019-03-06	Citrix Systems, Inc
2017-03-15	Moody's Corporation	2019-03-21	Facebook, Inc.
2017-03-15	Twitter Inc.	2019-04-02	Facebook, Inc.
2019-10-25	Adobe Inc.	2019-07-03	Quest Diagnostics Incorporated
2019-11-22	T-Mobile US, Inc	2019-07-29	Capital One Financial Corporation
2019-12-19	Facebook, Inc.	2019-10-18	CenturyLink, Inc.

3 priedas. Perteklinės akcijų grąžos.

Event ID	Firm	Reference Market	Event Date	Actual Stock Return	Actual Market Return	Alpha	Beta	Residual Standard Deviation	Expected Market Return	First-order Autocorellation
1	MS	SP500	2015-01-05	-0,0318	-0,0184	0,001	1,2731	0,0083	-0,0224	0,1621
2	NVDA	SP500	2015-01-06	-0,0308	-0,0089	0,0003	1,2606	0,0142	-0,011	-0,1767
3	ANTM	SP500	2015-02-04	0,005	-0,0042	0,0014	1,1827	0,0108	-0,0035	-0,2034
4	MSFT	SP500	2015-04-03	-0,0106	0,0035	-0,0012	1,2252	0,012	0,0031	-0,0075
5	SBUX	SP500	2015-05-12	0,0042	-0,003	0,0022	0,9207	0,012	-0,0005	-0,1291
6	CVS	SP500	2015-07-18	0,0083	-0,0024	0,0006	0,8374	0,0055	-0,0014	0,0518
7	TMUS	SP500	2015-10-01	0,008	0,002	0,0022	0,66	0,0141	0,0035	0,2046
8	JPM	SP500	2015-11-10	0,0043	0,0015	0,0002	1,1346	0,0067	0,0019	-0,0521
9	CNC	SP500	2016-01-26	-0,0229	0,014	-0,0005	1,1776	0,0214	0,0161	0,0401
10	PKI	SP500	2016-03-16	0,0052	0,0056	-0,0001	1,1456	0,012	0,0063	0,0275
11	SCHW	SP500	2016-05-03	-0,0278	-0,0087	-0,0005	1,7943	0,0147	-0,0162	0,0053
12	GOOG	SP500	2016-05-06	0,0137	0,0032	0,0005	0,9222	0,0109	0,0034	-0,035
13	MSFT	SP500	2016-05-17	-0,0188	-0,0095	-0,0005	1,1904	0,0115	-0,0117	-0,1018
14	TWTR	SP500	2016-06-13	0,0371	-0,0081	-0,0052	1,307	0,0345	-0,0158	-0,1879
15	DIS	SP500	2016-07-30	0,0113	0,0031	-0,0006	0,8899	0,0084	0,0022	-0,087
16	ORCL	SP500	2016-08-08	0,0007	-0,0009	-0,0006	1,1179	0,0084	-0,001	-0,1463
17	HPE	SP500	2016-11-23	0,0293	0,0008	0,0026	1,787	0,0133	0,0041	-0,0837
18	GOOG	SP500	2016-11-30	-0,0167	-0,0027	-0,0001	0,9285	0,0077	-0,0026	0,2716
19	CVS	SP500	2016-12-05	0,0048	0,0058	-0,0022	0,4087	0,0161	0,0001	-0,2317
20	TMUS	SP500	2016-12-07	0,042	0,0131	0,0013	1,3746	0,0133	0,0193	-0,2049
21	BA	SP500	2017-02-27	0,0112	0,001	0,0013	1,0911	0,0088	0,0025	0,1141
22	MCO	SP500	2017-03-15	0,0069	0,0083	-0,0006	1,1365	0,0093	0,0089	0,0379
23	TWTR	SP500	2017-03-15	-0,0191	0,0083	-0,0021	0,305	0,0393	0,0004	-0,0358
24	GOOG	SP500	2017-05-04	0,005	0,0006	-0,0005	1,1445	0,0078	0,0001	0,1243
25	FB	SP500	2017-08-30	0,0111	0,0046	0,0015	1,3199	0,0078	0,0076	0,0362
26	EFX	SP500	2017-09-17	0,0052	0,0011	0,0002	1,0243	0,0066	0,0014	-0,0342
27	ADBE	SP500	2017-09-25	-0,0268	-0,0022	0,0013	1,3157	0,0073	-0,0016	-0,0722
28	TMUS	SP500	2017-10-12	0,0016	-0,0017	-0,0008	1,4363	0,0109	-0,0033	-0,124
29	YUM	SP500	2017-11-17	0,0008	-0,0026	0,0007	0,6938	0,0092	-0,0011	-0,0342
30	KO	SP500	2018-01-22	0,0047	0,008	0,0003	0,0668	0,0061	0,0009	0,0547
31	FDX	SP500	2018-02-19	-0,0034	0,0004	0,0007	1,1532	0,0095	0,0012	0,0082
32	UPS	SP500	2018-03-14	-0,0052	-0,0057	-0,0012	0,7544	0,0116	-0,0055	0,0895
33	EXPE	SP500	2018-03-20	-0,007	0,0015	-0,0026	0,2939	0,0262	-0,0022	0,1533
34	UAA	SP500	2018-03-30	0,0012	0,0137	-0,0014	1,4716	0,0383	0,0188	0,0904
35	DAL	SP500	2018-04-06	-0,0216	-0,0222	0,0008	1,031	0,0146	-0,0221	0,1314
36	EXPE	SP500	2018-04-20	-0,0145	-0,0086	-0,0025	0,4541	0,0269	-0,0064	0,1173
37	LNC	SP500	2018-05-01	-0,0062	0,0025	-0,001	1,2857	0,0113	0,0023	-0,1111
38	TMUS	SP500	2018-05-24	-0,0007	-0,002	-0,0003	0,8438	0,0145	-0,0021	0,0424
39	FB	SP500	2018-06-12	0,0045	0,0017	0,0001	1,2671	0,0156	0,0024	0,0308
40	FB	SP500	2018-09-28	-0,0263	0,0017	-0,0013	1,4596	0,0239	-0,0013	-0,0063
41	GOOG	SP500	2018-10-08	-0,0073	-0,0004	-0,0003	1,5808	0,0089	-0,001	0,1372
42	MAR	SP500	2018-11-30	-0,0575	0,0081	-0,0013	1,1181	0,012	0,0078	0,2632
43	MAR	SP500	2018-11-30	-0,0575	0,0081	-0,0013	1,1181	0,012	0,0078	0,2632
44	CTXS	SP500	2019-03-06	-0,0072	-0,0065	-0,0003	0,6624	0,0092	-0,0046	-0,0217
45	FB	SP500	2019-03-21	0,0039	0,0108	0,0008	1,285	0,0186	0,0146	-0,0503
46	FB	SP500	2019-04-02	0,0321	0,0108	0,0002	1,2675	0,019	0,0002	-0,0036
47	DGX	SP500	2019-07-03	0,0071	0,0076	0,0008	0,7112	0,0126	0,0062	-0,0244
48	COF	SP500	2019-07-29	-0,0119	-0,0016	-0,0007	1,3076	0,0124	-0,0028	-0,1966
49	CTL	SP500	2019-10-18	0,0327	-0,0039	-0,0001	0,9701	0,0233	-0,0039	0,0823
50	ADBE	SP500	2019-10-25	0,0047	0,0041	-0,0001	1,3962	0,0112	0,0056	-0,0465
51	TMUS	SP500	2019-11-22	0,0114	0,0022	-0,0002	0,8969	0,0111	0,0017	-0,1593
52	FB	SP500	2019-12-19	0,0174	0,0044	-0,0002	1,2937	0,0104	0,0057	-0,1975

4 priedas. Suminių vidutinių perteklinių akcijų grąžų reikšmingumo tikrinimui naudojama *t-statistikos* reikšmingumo lentelė

d.f.	0.40	0.25	0.10	0.05	0.04	0.025	0.02	0.01	0.005	0.0025	0.001	0.0005
1	0.325	1.000	3.078	6.314	7.916	12.706	15.894	31.821	63.656	127.321	318.289	636.578
2	0.289	0.816	1.886	2.920	3.320	4.303	4.849	6.965	9.925	14.089	22.328	31.600
3	0.277	0.765	1.638	2.353	2.605	3.182	3.482	4.541	5.841	7.453	10.214	12.924
4	0.271	0.741	1.533	2.132	2.333	2.776	2.999	3.747	4.604	5.598	7.173	8.610
5	0.267	0.727	1.476	2.015	2.191	2.571	2.757	3.365	4.032	4.773	5.894	6.869
6	0.265	0.718	1.440	1.943	2.104	2.447	2.612	3.143	3.707	4.317	5.208	5.959
7	0.263	0.711	1.415	1.895	2.046	2.365	2.517	2.998	3.499	4.029	4.785	5.408
8	0.262	0.706	1.397	1.860	2.004	2.306	2.449	2.896	3.355	3.833	4.501	5.041
9	0.261	0.703	1.383	1.833	1.973	2.262	2.398	2.821	3.250	3.690	4.297	4.781
10	0.260	0.700	1.372	1.812	1.948	2.228	2.359	2.764	3.169	3.581	4.144	4.587
11	0.260	0.697	1.363	1.796	1.928	2.201	2.328	2.718	3.106	3.497	4.025	4.437
12	0.259	0.695	1.356	1.782	1.912	2.179	2.303	2.681	3.055	3.428	3.930	4.318
13	0.259	0.694	1.350	1.771	1.899	2.160	2.282	2.650	3.012	3.372	3.852	4.221
14	0.258	0.692	1.345	1.761	1.887	2.145	2.264	2.624	2.977	3.326	3.787	4.140
15	0.258	0.691	1.341	1.753	1.878	2.131	2.249	2.602	2.947	3.286	3.733	4.073
16	0.258	0.690	1.337	1.746	1.869	2.120	2.235	2.583	2.921	3.252	3.686	4.015
17	0.257	0.689	1.333	1.740	1.862	2.110	2.224	2.567	2.898	3.222	3.646	3.965
18	0.257	0.688	1.330	1.734	1.855	2.101	2.214	2.552	2.878	3.197	3.610	3.922
19	0.257	0.688	1.328	1.729	1.850	2.093	2.205	2.539	2.861	3.174	3.579	3.883
20	0.257	0.687	1.325	1.725	1.844	2.086	2.197	2.528	2.845	3.153	3.552	3.850
21	0.257	0.686	1.323	1.721	1.840	2.080	2.189	2.518	2.831	3.135	3.527	3.819
22	0.256	0.686	1.321	1.717	1.835	2.074	2.183	2.508	2.819	3.119	3.505	3.792
23	0.256	0.685	1.319	1.714	1.832	2.069	2.177	2.500	2.807	3.104	3.485	3.768
24	0.256	0.685	1.318	1.711	1.828	2.064	2.172	2.492	2.797	3.091	3.467	3.745
25	0.256	0.684	1.316	1.708	1.825	2.060	2.167	2.485	2.787	3.078	3.450	3.725
26	0.256	0.684	1.315	1.706	1.822	2.056	2.162	2.479	2.779	3.067	3.435	3.707
27	0.256	0.684	1.314	1.703	1.819	2.052	2.158	2.473	2.771	3.057	3.421	3.689
28	0.256	0.683	1.313	1.701	1.817	2.048	2.154	2.467	2.763	3.047	3.408	3.674
29	0.256	0.683	1.311	1.699	1.814	2.045	2.150	2.462	2.756	3.038	3.396	3.660
30	0.256	0.683	1.310	1.697	1.812	2.042	2.147	2.457	2.750	3.030	3.385	3.646
31	0.256	0.682	1.309	1.696	1.810	2.040	2.144	2.453	2.744	3.022	3.375	3.633
32	0.255	0.682	1.309	1.694	1.808	2.037	2.141	2.449	2.738	3.015	3.365	3.622
33	0.255	0.682	1.308	1.692	1.806	2.035	2.138	2.445	2.733	3.008	3.356	3.611
34	0.255	0.682	1.307	1.691	1.805	2.032	2.136	2.441	2.728	3.002	3.348	3.601
35	0.255	0.682	1.306	1.690	1.803	2.030	2.133	2.438	2.724	2.996	3.340	3.591
36	0.255	0.681	1.306	1.688	1.802	2.028	2.131	2.434	2.719	2.990	3.333	3.582
37	0.255	0.681	1.305	1.687	1.800	2.026	2.129	2.431	2.715	2.985	3.326	3.574
38	0.255	0.681	1.304	1.686	1.799	2.024	2.127	2.429	2.712	2.980	3.319	3.566
39	0.255	0.681	1.304	1.685	1.798	2.023	2.125	2.426	2.708	2.976	3.313	3.558
40	0.255	0.681	1.303	1.684	1.796	2.021	2.123	2.423	2.704	2.971	3.307	3.551
60	0.254	0.679	1.296	1.671	1.781	2.000	2.099	2.390	2.660	2.915	3.232	3.460
80	0.254	0.678	1.292	1.664	1.773	1.990	2.088	2.374	2.639	2.887	3.195	3.416
100	0.254	0.677	1.290	1.660	1.769	1.984	2.081	2.364	2.626	2.871	3.174	3.390
120	0.254	0.677	1.289	1.658	1.766	1.980	2.076	2.358	2.617	2.860	3.160	3.373
140	0.254	0.676	1.288	1.656	1.763	1.977	2.073	2.353	2.611	2.852	3.149	3.361
160	0.254	0.676	1.287	1.654	1.762	1.975	2.071	2.350	2.607	2.847	3.142	3.352
180	0.254	0.676	1.286	1.653	1.761	1.973	2.069	2.347	2.603	2.842	3.136	3.345
200	0.254	0.676	1.286	1.653	1.760	1.972	2.067	2.345	2.601	2.838	3.131	3.340
250	0.254	0.675	1.285	1.651	1.758	1.969	2.065	2.341	2.596	2.832	3.123	3.330
inf	0.253	0.674	1.282	1.645	1.751	1.960	2.054	2.326	2.576	2.807	3.090	3.290