

Република С.Македонија

УНИВЕРЗИТЕТ “Св.КИРИЛ И МЕТОДИЈ”СКОПЈЕ

ФИЛОЗОФСКИ ФАКУЛТЕТ

ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР

Магистерски труд

**Улогата на корпоративната безбедност во справување со
современи безбедносни предизвици**

Ментор:

Проф. Д-р Оливер Бакрески

Изработил:

Душко Тасевски

Апстракт

Целта на овој труд е да ја претставиме улогата на корпоративната безбедност во делот на менаџирање на корпорациите за успешен просперитет на пазарот од аспект на внатрешни и надворешни закани кои и претстојат на една компанија. Давање на поголем акцент на корпоративната безбедност која најчесто е маргинализирана од страна на сопствениците и останатите гранки во корпорацијата, сметајќи ја за гранка која не е толку битна за да се даде поголемо значење. Вклучувањето на корпоративната безбедност во целиот систем на раководење на една корпорација претставува предизвик за менаџерите, а е неминовен дел за ефикасно менаџирање на безбедноста како дел од една компанија. Корпоративната безбедност е единственото решение кое гарантира мир, стабилност на внатрешни и надворешни вредности, како и стабилна економија која е значаен фактор без кој денешните мултинационални компании неможат да опстанат. Со критичка дискусија ќе се фокусираме на безбедноста на компаниите и критичните прашања кои го попречуваат нејзиното спроведување во делот на корпорацијата. Од аспект на физичката и информациската безбедност ќе се фокусираме на справување со современите безбедносни предизвици.

Во дел од трудот ќе се фокусираме на теоретскиот пристап на безбедноста во компанијата, важноста, формите и квалитетите на добро поставените стандарди на корпоративната безбедност. Развивањето на дискусија околу постапките за безбедносните процедури на компанијата, во кои се планираат безбедносните процедури што треба една компанија да ги следи во рамките на корпоративната безбедност за вработените, клиентите и имотот. Овие постапки вклучуваат планирање, проценка и анализа на ризик, безбедносни мерки и безбедносни политики, спроведување и мониторинг на усогласеноста на безбедносните мерки/политики на една компанија.

Клучни зборови: Корпоративна безбедност, планирање, проценка, закани, ризик.

СОДРЖИНА

Апстракт	1
Вовед.....	4
ГЛАВА I	
БЕЗБЕДНОСТ.....	7
Поим на безбедноста.....	8
Потреба од безбедност.....	10
Концептуализација на безбедноста.....	16
ГЛАВА II	
КОРПОРАТИВНА БЕЗБЕДНОСТ.....	20
Општо за корпоративната безбедност.....	21
Значење на корпоративната безбедност.....	23
Функции на корпоративната безбедност.....	25
Улогите на менаџерите.....	25
Структура на корпоративен безбедносен менаџмент.....	26
Техничка корпоративна безбедносна дисциплина.....	27
Стратегија за управување со корпоративната безбедност.....	30
Односот на корпоративната безбедност и приватната безбедност.....	37
Физичко обезбедување.....	45
Техничко обезбедување.....	47
Детективски работи.....	48

ГЛАВА III

ПРОЦЕНА НА РИЗИЦИ ВО КОМПАНИИТЕ.....	54
Општо за процените.....	55
Безбедносни процени за корпорациите.....	57
Методологија за безбедносни процени.....	61
Идентификација на заканите.....	61
Ефективност од корпоративната безбедност во компаниите.....	62
Форми на корпоративна безбедност.....	63
Корпоративна безбедност во областа на информатичката заштита.....	65
Корпоративна безбедност структура.....	67
Активности на организациските единици за корпоративна безбедност.....	70

ГЛАВА IV

СОВРЕМЕНИ БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ ВО КОМПАНИИТЕ.....	74
Општо за заканите.....	77
Облици на загрозување на корпорациите.....	78
Закани предизвикани од антропогени појави.....	80
Закани предизвикани од асиметрични закани.....	83

ГЛАВА V

БЕЗБЕДНОСТ НА КОРПОРАЦИИТЕ.....	87
Справување со потенцијални закани.....	88
Современи пристапи во справување со заканите.....	102
Заклучок.....	105
Користена литература.....	110

Вовед

Управувањето и контролирањето на корпорациите се состои од систем на правила со кои се изнаоѓаат решенија за менаџирање во корист на сопствениците на корпорациите. Повеќето дефиниции се фокусираат на финансиските аспекти и на правната регулатива на корпоративното управување. Успешното управување на една корпорација има потреба од безбедносни методи и техники од корпоративна безбедност. Со нејзина помош се постигнува намалување на заканите, како и ризикот од непосредни последици кои имаат намера да го загрозат директно или индиректно опстанокот на компанијата и фирмата на домашниот или странскиот пазар. Приоритет на корпоративната безбедност без сомнеж е заштитата на имотот на компанијата за која цел мора да биде добро организирана, земајќи ги предвид заштитата на капиталот на сопствениците. Имено, корпоративната безбедност ја насочуваме да оневозможи губење на капиталот или имотот, како последица од различни обиди на нивно завземање и намалување на материјалните загуби од различни закани настанати како резултат на можните ризици со кои се предизвикува безбедноста на самата компанија.

Гледано низ призмата на компаниите кои придонесуваат во општеството и зајакнувањето на економската состојба на државите неизбежен е фактот на важноста на корпоративната безбедност како и нејзина неопходност.

Глобализацијата како економски двигател во светот ја носи и технолошката револуција во индустрискиот свет. Оттука и трендот на новите начини на организиран криминал и нови хибридни закани кои им претстојат на самите компании.

Во делот на стопанското работење сè повеќе е застапена опасноста од инциденти од отровни и експлозивни испарувања како и од модерна технологија која е проследена со деструктивни појави кои предизвикуваат трајни и штетни последици на компанијата. Оттука е наметната потребата за менаџирање како овие опасности на современото општество да се минимизираат, со цел да се

спротивставиме на сè она што ги загрозува животите и здравјето на луѓето, имотот и работењето на корпорациите. Заштитата од ваквите опасности мора да биде професионална, стручна и ефективна, но и да вклучува широк спектар на мерки и постапки во поглед на планот за брза интервенција и санирање на штетните последици. Поради ваквата опасност големите техничко-технолошки системи и индустриските капацитети се принудени да применуваат соодветни превентивни мерки со кои ќе се дава поголем акцент на прашањата поврзани со безбедноста и заштитата.

Корпорациската безбедност, компаниите или фирмите се уште ја чувствуваат како една голема мистерија на денешницава во корпоративниот свет. Нејзината улога често е погрешно разбрана, исполнета со контроверзии и чести внатрешни конфликти. Погледот за безбедноста како помалку платен фактор во корпорациите полека се менува, а бизнисите сè повеќе сфаќаат дека безбедноста не го штити само капиталот, туку додава и поголема вредност на клучните деловни процеси. Во таа насока, корпорациската безбедност е сè повеќе застапена во работниот процес на организацијата која се состои од меѓусебно поврзани потсистеми. Организациската единица на истата мора континуирано да биде застапена во механизмите на корпоративното управување за да го заштити и обезбедува непреченото одвивање на деловните и производните процеси, како и отстранување на безбедносните проблеми. Корпорациската безбедност зазема клучна улога во плановите за целокупниот развој во корпорацијата и своевремено ги намалува облиците на ризик во работењето, со што и се доверува приматот да биде главен гарант во обезбедување на континуираното работење и решавањето на проблемите од комплексен карактер.

Корпоративната безбедност исто така има за цел да ги поткрепи безбедносните и одбранбените капацитети на национално ниво, кој во даден случај на загрозување на државата да дадат допринос во обезбедување на населението преку логистичка поддршка на клучните организациски структури во системот на националната безбедност. За ефективно и ефикасно преземање на

мерките, важно е да има синхронизација на постојните правила и прописи кои ќе допринесат за поголема функционалност на компаниите во различни ситуации.

I ГЛАВА

БЕЗБЕДНОСТ

БЕЗБЕДНОСТ

Поим на безбедноста

Од историски аспект гледано, човекот од самото постоење тежнее на својата заштита и спасување во сите периоди на развојот од социјален аспект. Со примена на разнобразни методи, облици и форми за својата безбедност. Имено, инстинктот за својата безбедност станува дел од начинот на живот. Всушност, тука е и прашањето дали може да зборуваме за безбедноста на самиот човек како една историска варијабла. Секако тоа произлегува како нужност за својата безбедност, заштита и спасување колку што е старо и самото човечко битие. На почетокот својата безбедност, заштита и спасување човекот ја реализирал инстинктивно, рефлексно, индивидуално или на еден начин неорганизирано. Ова дејствување се развивало и усовршувало адекватно на промените и постанало едно од главните причини за поставување на соодветна организираност на дејствијата.

Безбедноста вообичаено се поставува како прва превенција на несреќи, односно се избегнува да се случат несреќни и несакани настани. Безбедноста, како и да сè постави на неа сè гледа како на темелна вредност на работното место. Продуктивното размислување води кон тоа да безбедноста се постави како техничка отпорност во случај на непредвидливи закани и предизвици гледано на работните операции да се вратат во првобитна состојба со минимални штети. Во континуитет на работниот живот и работната средина безбедноста постојано треба да биде пофлексибилна и подобрена. За да успееме да ја доведеме безбедноста на повисоко ниво сè бара постојана работа на управувачко и оперативно ниво¹.

¹ Безбедност. (n.d.). Retrieve January 22, 2021, from <https://mzzpr.org.mk/tps://oshwiki.eu/wiki/%D0%91%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82>

Професорот Цане Т. Мојаноски во својата книга “Вовед во безбедноста” укажува дека безбедноста е тесно поврзана со опстанокот на државата². За безбедноста од егзистенцијална закана може да констатираме дека дефинирани објекти се подразбираат населението, државата и територијата. Најчесто специфична употреба наоѓа во оправданата примена во вонредните мерки при нејзино превентивно дејствување. Основајќи се на безбедносните закани кои претставуваат основа за овластување на сите органи од безбедноста им се дава законска употреба на сила. Под безбедност подразбираме состојба во која сме надвор од опасност и ослободени од повреди. Мултидимензионалниот концепт на безбедност има одредени нивоа на влијание врз поединци, корпорации, таргет групи и цели во општеството. На секое ниво се пристапува со различни методолошки начини, но влијанието од страна на безбедноста врз општата атмосфера е секогаш позитивно прифатено.

Безбедноста се заснова на неколку активности, димензија на ризикот и важноста која му се дава на ризикот. Безбедноста во делот на корпорациите се занимава пред се со здравјето на работниците да не биде загрозено додека трае работниот процес. Исто така, се занимава и со спречување на индустриски несреќи, кои можат да настанат од внатрешни или надворешни фактори, како на пример: пожар, ослободување на хемиски супстанции и итн.

Безбедносното работење е всушност дел од оперативно методолошките практики на рамниште на поединец и на самата организација, која како примарна дејност се ресурсите за управување со можните ризици. Кога станува збор за безбедноста, целта е да се спречат несреќите, а не само да се надминат. Мотивот за да се спречат евентуални или пак слични видови на несреќи настапува после несреќата откако ќе настане поголем економски трошок. И тогаш се пристапува кон анализа каде сè има потфрлено системот.

² Мојаноски, Ц. Т., Ѓуровски, М. & Павловиќ, Г. (2018). Вовед во безбедноста. Скопје, Македонија: Фондација Конрад Аденаурер. Retrieved May 08, 2019, from [https://fb.uklo.edu.mk/wp-content/uploads/2019/09/Voved-vo-bezbednosta-ucebnik-.pdf\(стр- 18\)](https://fb.uklo.edu.mk/wp-content/uploads/2019/09/Voved-vo-bezbednosta-ucebnik-.pdf(стр- 18))

Разбирањето на безбедноста како природен инстинкт на секоја личност и во пошироката човекова заедница, општество, фамилија, држава, нација, укажува на тоа дека безбедносниот концепт има поширока потреба во овие колективи.³ Новите димензии на безбедноста се посебно обликувани во националната и меѓународната безбедност. Валтер Липман (Walter Lipman) смета дека една нација е безбедна кога не е принудена да ги жртвува своите вредности ако сака да избегне војна, а е способна да ги зачува со победа во таква војна.⁴ За Арнолд Волферс (Arnold Wolfers), безбедноста се подразбира кога имаме отсуство од закани по главните вредности и интереси, а во објективна смисла на страв дека вредностите од посебно значење можат да бидат нападнати.⁵

Потреба од безбедност

Наместо да се обидуваме да ја објасниме безбедноста со анализа на јазичниот извор на зборот и неговото значење, за навистина да ја разбереме суштината на безбедноста, ќе се концентрираме повеќе на истражување на неговото вистинско потекло, суштина и принципи. Во суштина, иако се верува дека некои други професии се најстари, што може да биде вистина, безбедноста е дефинитивно една од најстарите процеси, датира од почетокот на животот и инстинктот истиот да се заштити.

Принципите на безбедност од времето на нашите далечни предци не се сменети. Пештерскиот човек ја чувал својата пештера со копје, додека друг бил во потрага по работ на населбата со мисија да ја забележи опасноста во најраната можна фаза и да ги алармира другите. Секој во заедницата точно знаел што да прави во случај на опасност и кој бил задолжен за донесување на одлуки.

³Т.Мојаноски, Ц, & Павловиќ, Г. (2018).*Вовед во безбедноста* (p. 22) (1167030035 875585280 М Ѓуровски, Ed.). Скопје, Македонија: Фондација Конрад Аденауер. doi:<https://fb.uklo.edu.mk/wp-content/uploads/2019/09/Voved-vo-bezbednosta-ucebnik-.pdf>

⁴Walter Lippmann. *US Foreign Policy: shield of the Republic* (Boston, Little, Brown, 1943), P. 51

⁵Arnold Wolfers. *Discord and collaborations, Essays on international politics* (Baltimore: John Hopkins University, Press, 1962) p. 150

Ја имаме пештерата како физички елемент на безбедноста, копјето како технологија, информации за приближната опасност, комуникација меѓу членовите на заедницата, сите членови на заедницата како човечки елемент и процедури, како поделба на задачите во рутина, така и како процедури за итни случаи, и шефот на заедницата како раководство. Кога некој од елементите би недостасувал, системот нема да работи правилно. И тогаш, како и сега, ги имаме седумте столба на безбедноста:

- Физички
- Технички
- Човечки
- Информации
- Комуникација
- Постапки
- Управување (контрола)

Она што се сменило со текот на времето, не е суштината на безбедноста, туку нејзината технологија. Сега, кога ги расчистивме столбовите на безбедносниот систем, ќе продолжиме со истражување на периодите и фокусот на заштитата. Периодите на заштита, фокусот на заштитата и нејзината вредност, заедно со веројатниот вид закана со која се соочуваме и влијанието врз материјални и нематеријални средства се елементите што ќе ја обликуваат стратегијата за заштита и ќе утврдат како да се распределат седумте основни безбедносни столбови и да се трансформираат во успешен безбедносен систем.

Заштитата најчесто се дели во три фази:

- Превенција
- Реакција
- Опоравување

Фазите на заштита соодветствуваат со фазите на инциденти:

- Превенцијата одговара на подготовката, која се состои од избор на цел, собирање информации и планирање. Подготвителната фаза може да трае долго - денови, месеци, а понекогаш дури и години пред акцијата.
- Реакцијата одговара на акција, која се состои од пристигнување, дејствување и бегство. Во зависност од видот на дејството, може да трае неколку минути, па дури и секунди.
- Опоравувањето одговара на последиците, што може да има катастрофално влијание врз луѓето, имотот, моралот и сл. Последиците може да се чувствуваат подолго време по инцидентот.

За да може да се дизајнираат применливи безбедносни стратегии и да се препознаат заканата, веројатноста за дејствување и неговиот режим, разбирањето на заштитниот фокус е клучна почетна точка. На пример, фокусот може да биде на:

- Луѓе
- Имот
- Процес
- Производ
- Информации

Фокусот може да биде и на комбинацијата на сите елементи со исти или различни нивоа на приоритет, на пример. Се применуваат различни стратегии и се користат различни ресурси во зависност не само од тоа што се штити, туку и од ситуацијата и веројатните ризици, заштитни пречки и последици од најлошото сценарио.

Ако се разбере природата на она што се штити и неговата вредност, исто така се разбира видот на закана со која се соочуваме (тероризам, кражба,

хулиганство, политичко насилство, итн.). Кога зборуваме за видот на заканата, ние исто така зборуваат за различни веројатни ризици поврзани со веројатниот режим на извршување на сторителите. Различни видови ризик се поврзани со различни видови закана. На пример, осамен ограбувач на банка на кој му требаат пари веднаш има за цел помала сума на готовина, но веројатно ќе предизвика поголема штета отколку организирана криминална група која цели многу поголема сума на готовина. Група криминалци ќе го испланираат грабежот за да ја постигнат својата цел што е можно поефикасно и се целосно свесни за различните последици од различните видови штети.

Еден од клучните елементи на безбедноста е концептот на вредност. Безбедноста не ја пресметува вредноста врз основа на трошоците, туку на мотив за извршување на кривично дело и во смисла на оправданата цена на безбедносните мерки. Во суштина, вредноста на она што го штитиме ни дава веројатност предметот (процес, производ, личност и сл.) да биде мотив за дејствување против неа. Исто така, ни го кажува видот на заканата со која се соочуваме и начинот на работа на сторителите.

Понатаму, вредноста може да се подели на примарна и секундарна вредност: Примарната вредност е во основа непосредната вредност на производот. На пример, готовина, накит, алкохол, цигари и брендирана облека се производи од примарна вредност. Овие предмети може веднаш да се таргет мета од криминалецот или лесно да се продадат. Како такви, тие можат да бидат привлечни како мотив за злосторничко дело од осамен сторител, но и за организиран криминал. Секундарната вредност се однесува на предмети што немаат употребливост во нивната сегашна форма: на пример, брендираните кошули се предмети со примарна вредност, додека текстилот што се користи за нивно производство е ставка од втора вредност. Не може да се користи директно од сторителот на делото, но може да се користи, на пример, од друг производител на облека. За да се препродаде, треба да биде во поголем обем, што бара планирање, логистика и претходно договарање со купувачот. Ова укажува на тоа

дека такво злосторство не може да биде извршено од осамен сторител, туку само од организирана група што е во состојба да го организира и изврши дејствието.

Класификацијата на вредноста зависи и од волуменот. Во основа, големите количини на примарна вредност стануваат секундарна вредност затоа што извршувањето кражба на големи количини бара планирање и логистика. На пример, неколку шишиња вино се примарна вредност, додека целиот камион вино е секундарна. За кражба на товарно вино потребни се организација, купувач, логистика, простор за складирање доволно голем за да содржи толкава количина предмети и слично. Видот и обемот на заштитената вредност, усогласено со нивото на безбедносни мерки, исто така укажуваат на веројатноста за дејствието и режимот на извршување на сторителите. На пример, во примерот на шишиња со вино, осамен сторител веројатно нема да се насочи кон добро обезбеден склад што содржи големи количини спакувани шишиња со вино за да украде една или две од нив. Овој феномен го нарекуваме сооднос помеѓу напор (или ризик) и награда.

Друг аспект на вредноста е оправданата цена на безбедносните мерки во споредба со трошоците за загуба. Во основа, инвестициите во безбедносни мерки не смеат да ги надминуваат трошоците за инциденти за разумен временски период. Организациите претпочитаат да не губат пари без оглед каде одат парите. Безбедноста не генерира профит и нејзина мисија е да го заштити профитот и да заштеди трошоците.

Анализирајќи го концептот на вредност, во основа анализираме еден од трите елементи неопходни за извршување на кривично дело - мотив. Мотивот, можноста и средствата заедно го создаваат триаголникот на криминал.

Успешна безбедносна стратегија се концентрира на разбирање на мотивот, ограничување на можноста и попречување на средствата во најраната можна фаза на инцидентот со вклучување на сите безбедносни елементи за кои претходно разговаравме. Како пример, за да се спроведе акција, сторителот мора да собере информации (средства) за успешно да изврши некое кривично дело. Попречување на собирање информации во основа е попречување на средствата, затоа

ограничување на можноста во најраната можна фаза (фаза на подготовка) и спречување на инцидент.

Постојат два вообичаени безбедносни пристапи кои се користат во корпорацијата за безбедност. Тоа се „дефанзивен пристап“ и „пристап на одвраќање“. Овие пристапи може да се користат индивидуално или наизменично зависно од околностите.

Дефанзивен пристап. Ова е долг традиционален пристап што го применуваат безбедносните службеници во компаниите. Овој пристап се заснова на заштита наместо на превенција. Пристапот помага при дизајнирање на компанијата безбедносните службеници да бидат „бранители“ или „чувари на портата“⁶. Пристапот ја негира стратешката мерка за проценка и анализа на ризик, како и воспоставување на здрави безбедносни политики пред создавање на безбедносните мерки и системи. Главната безбедносна мерка од овој пристап е користење на чувари. Исто така, пристапот се користи со тактика „чекање чинот да се појави“, а потоа да се одговори на него и тоа ја негира идентификацијата на веројатните предизвикувачки фактори за појава на катастрофални дејствија во рамките на компанијата.

Пристап на одвраќање. Ова е скроман пристап за безбедноста на компанијата. Овој пристап главно се заснова на елиминација на сите ризици против појава на катастрофални акти. Пристапот ги утврдува процедурите за безбедност, како што се проценка и анализа на ризици, како и безбедносни политики пред воспоставување на безбедносни мерки. Овој пристап е стратешки и оперативен кон какви било ризици од недозволени акти. Ги идентификува ризиците, прави проценка и ја предлага сигурната политика за надминување на таквите ризици. Со други зборови, пристапот базиран на спречување на кој било од заканите со наоѓање на веројатните предизвикувачки фактори за секој ризик и применување на стратегиите на елиминација од такви ризици. Пристапот преку

⁶ Dulaney E ‘Picture this: A visual guide to security controls’ (2014) retrieved from www.certmag.com/picturethisvisualguidetosecuritycontrols as posted on 14th July 2014

неговата безбедносна политика ги утврдува безбедносните мерки и системи што можат да го одвратат лицето со лоши намери да изврши какво било незаконско дело во или надвор од компанијата.

Затоа, најдобриот пристап во современата корпоративна безбедност е пристапот на заплашување поради неговиот целосен пакет на сигурни механизми за безбедност врз безбедноста на компанијата. Безбедноста, менаџерите веќе не ја користат за да се однесуваат како „чувари на портата“, туку тие мора да бидат стручни и креативни за проценка на ризиците за безбедноста и изготвување на добри безбедносни политики, како и избор на соодветните безбедносни мерки за да се отстранат сите закани што можат да наштетат врз безбедноста на компанијата.

Концептуализација на безбедноста

Како што веќе беше кажано за концептот на безбедност –има многу дефиниции. Сепак, она што може да се издвои како неоспорно во сите дефиниции, а се одржува до денес како основа за утврдување на безбедноста, е разбирање на безбедноста како организација, држава, функција и наука или систем и наука.

Исто така, може да се наведе дека е надминато разбирањето на безбедноста како отсуство или непостоење на опасност, со општо прифатеното разбирање дека апсолутната безбедност е утописка и неостварлива цел. Во таа смисла, поимот безбедност постои заедно со поимот за потенцијална опасност или ризик, т.е. за безбедноста сè повеќе се смета дека се наоѓа во воочен и контролиран ризик што станува предмет на безбедност. За референтниот предмет на безбедноста, како основен критериум за поделба, може да се утврди:

- Држава
- Индивидуа
- Општество или социјални групи
- Меѓународна заедница
- Колективитети

Сепак, безбедносниот предмет може да биде и:

- деловна организација или корпорација
- активност или област како што се, работа, информации, сообраќај, итн.

Во науката и теоретските размислувања, безбедноста најчесто се поврзува со државата и потенцијалот на моќ и сила што државата ја има на располагање. Земајќи ја државата како референтен предмет на безбедност, најчести термини се националната безбедност и државната безбедност.

Националната безбедност е способност на една држава (нација) да преживее со заштита на нејзиниот територијален интегритет и суверенитет, постигнување политичка независност и, со помош на државните атрибути, заштита на нејзините внатрешни вредности од сите форми на закани, без оглед дали доаѓаат од надвор или се наоѓаат во рамките на државата. Заштита на основните вредности на општеството се заснова на активностите на структурите за национална безбедност во рамките на специфичен безбедносен систем. Безбедносниот систем, меѓу другото, служи за воспоставување внатрешна и надворешна рамнотежа во меѓународната заедница. Корпусот на вредности што се зачувани и подобрувани со работењето на системот за национална безбедност најчесто вклучуваат: идентитет, опстанок во најширока смисла на зборот, опстанок на државата, национален опстанок, физичко самоодржување, територијален интегритет, политичка независност, квалитет на живот, итн.

Во најширока можна смисла, терминот меѓународна безбедност се однесува на ситуација во која настаните во една држава не ги загрозуваат другите држави и луѓето што живеат во нив. Така дефинираната меѓународна безбедност претставува отсуство на војна меѓу држави, но исто така и отсуство на други закани што можат да влијаат на две или повеќе држави, како што се меѓународен тероризам, нуклеарни несреќи, транснационален организиран криминал, климатски промени, илегална прекугранична миграција, итн. Во потесна смисла, меѓународната безбедност е оној дел од меѓународната политика што настанува

кога актерите во меѓународните односи се подготвени да се заканат или да употребат сила за да се постигне посакуваниот исход.

Дефинирањето на поединецот како референтен предмет на безбедност воспоставило форма на индивидуална безбедност и отворило научен проблем на теоретско разгледување на односот помеѓу индивидуалната и националната безбедност, т.е. државната безбедност, каде што безбедноста на поединците и социјалните групи, формирана од индивидуи, е безбедноста на поединецот, покрај физичкото загрозување, во светло на други сложени фактори како што се здравјето, благосостојбата, слободата итн. Некои теоретичари, како Бузан, прават разлика помеѓу субјективната и објективната безбедност, почитувајќи го субјективното чувство на страв од објективната состојба. Според него, апсолутна безбедност не постои, потполното отсуство на страв, закани или опасност не може да се земе како критериум за проценка на безбедноста, туку нивното контролирано присуство, така што субјективната безбедност може да се изрази како контролирано присуство на страв, а објективната безбедност како контролирано присуство на закани или ризици.⁷

Социјалната сигурност, односно безбедноста на општеството, може да има неколку различни значења. Во безбедносните студии, тоа најчесто се однесува на стабилноста на колективниот идентитет. Во таа смисла, социјалното осигурување постои кога едно општество е во состојба да ги зачува своите суштински карактеристики поради променливите околности и покрај можните или реални закани. Главниот референтен објект на социјалното осигурување е колективен идентитет, односно збир на идеи и практики кои идентификуваат одредени лица како членови на социјална група.

Глобалната безбедност значи стремеж кон отсуство на закани ширум светот. Низ историјата, безбедноста се сфаќаше, пред сè, во домашни или меѓудржавни рамки. Сепак, само со развојот на технологијата и процесот на глобализација во текот на дваесеттиот век се појавија и првите закани што може да ја загрозат целата планета земја и свеста за нив. Покрај развојот на оружје за масовно уништување, а особено на нуклеарно оружје, врз развојот на концептот на

⁷ BAJAGIĆ, Mladen, Osnovi bezbednosti, Policijska akademija, Beograd, 2007, str. 57.

глобална безбедност влијаеше и избувнувањето на две светски војни, потоа избувнувањето на Студената војна, забрзано глобално затоплување и, конечно, почеток на Светската војна против тероризмот. Сепак, на идејата дека безбедноста на планетата е неделива, влијаеле и други фактори, како што се освојувањето на вселената (првите слики на планетата Земја направени од леталото Аполо 8), развојот на глобалната култура, правејќи холивудски филмови за планетарни катастрофи, информациска револуција, парадоксалнопостоење на растечко движење против глобализацијата.

II ГЛАВА

КОРПОРАТИВНА БЕЗБЕДНОСТ

КОРПОРАТИВНА БЕЗБЕДНОСТ

Општо за корпоративната безбедност

Растот на безбедноста е воден од поголемото потпирање на приватниот сектор за заштита од криминал и насилство, делумно, поради перцепираните неуспеси на законот и редот и поголемата способност на некои корисници да ја платат услугата. Ваквата безбедност се протега надвор од она што може да се смета за традиционално приватно обезбедување, односно, заштита и електронска безбедност. Понатаму, секторите како што се приватното обезбедување кои се занимаваат со овие експлицитни занимања, да ги даваат услугите како што се чувари и технички персонал, за да се практикуваат овие области во управувањето со безбедноста и во управувањето со ризикот и континуитетот на бизнисот.

Корпоративната безбедност е дел од безбедносниот домен; сепак, тоа не е дел од приватниот безбедносен сектор. Како што изјавиле, корпоративната безбедност е уникатна функција за поддршка која ефикасно се совпаѓа со корпорацијата и асистира во нејзиниот успех. Приватното обезбедување обезбедува стоки и услуги на трето лице. Но, корпоративната безбедност е вградена во самите организации, истражувајќи како што се бараат и другите елементи на приватната безбедносна индустрија. На пример, корпоративната безбедност од време на време ќе ги користи услугите од приватното обезбедување во службите за обезбедување и службите за патролно обезбедување. Во продолжение, тие можат да го користат техничкиот безбедносен сектор за одржување на надзор и контрола на пристапот на затворен канал (cctv). Корпоративната безбедност работи во разни области на безбедноста, како што се јавни, општински, владини институции и приватните корпорации, од мали па се до големи.

Оправданоста на корпоративната безбедносна функција може да се разгледува во два правци во неолиберален или нео-републикански поглед. Неолибералната форма се обидува да ја искористи традиционалната пазарна

логика, со што безбедноста е прашање на пресметка и профит. Неолибералистите се фокусираат да демонстрираат додадена вредност на безбедноста, на пример, менаџирање на контролата на губитоците во добавувачката линија.

Спротивно на тоа, нео-републиканската форма на владеење изразува органска визија за заедничка безбедносна одговорност, заеднички морал што "ние" сме способни да ги прифатиме противречностите помеѓу националната безбедност и бизнисот. И покрај неолибералниот и нео-републиканските гледишта за корпоративната безбедност, во предвид треба да се разгледа одговорноста и контролата.

Клучен двигател на растот на корпоративната безбедност во 21-от век е одговорноста и прифаќањето на корпоративното опкружување од страна на властите како целина на одговор на заедницата на заканите за националната безбедност, како што се тероризмот и транснационалниот организиран криминал. Постојат големи очекувања дека корпорациите што работат во индустријата за авијација, финансии и производство на електрична енергија или слично ќе назначат соодветни менаџери за корпоративна безбедност кои можат да се ангажираат со колегите од владините безбедносни структури. Моралната одговорност за придонесот кон безбедноста и благосостојбата на нацијата-државата доведува до големо значење дека корпорациите, јавноста и приватните лица мора да ја вградуваат безбедноста во нивната организација. Одговорноста е конструкција на нео-републиканските погледи за безбедноста.

Дополнителен двигател на корпоративната безбедност е улогата што ја има како внатрешен орган за контрола, кое го надополнува двигателот за одговорност. Контролната теорија за безбедноста сепак го надополнува и неолибералното и нео-републиканското гледиште за безбедноста. Корпоративната безбедност како контролна функција обезбедува средства за регулирање, истрага и гонење во контекст на организацијата.

Слично како приватното обезбедување, корпоративната безбедност има свои вештини и знаења во рамките на својот дискретен дел од безбедносниот домен.

Значење на корпоративната безбедност

Безбедноста нема дефиниција и структурно познавање, со различност во практиката, бидејќи е крос-дисциплинирана и без дефинирано или одредено знаење и вештина. Како што посочува Петерсен, безбедносните менаџери ниту се обединети од нивното формално образование, ниту поседуваат сертификација контролирана од државата. Ова прашање е проблематично кога се толкува за менаџерите за корпоративна безбедност, кои во многу земји не бараат никакво сертификарање бидејќи не обезбедуваат стоки или услуги на трети лица. Фондацијата за континуиран развој на безбедносното познавање и неговата примена во корпоративната безбедност ќе зависи од познавањето на принципите и концептите на новата дисциплина на безбедносната наука. Истражувањето и развојот на познавањето на дисциплината на безбедност е клучна за професионална примена на новата генерација на концептуални принципи на корпоративната безбедност. Ваквите истражувања и развој ќе водат до зголемување на професионалноста, со заедништво во јазикот, вештините и границите во практиката.

Професионалниот развој е есенцијален елемент во подемот на профилирањето и репутацијата на корпоративната безбедност, бидејќи му овозможува на менаџерот за безбедност да овозможи признание за својата кариера. Професионалниот диверзитет мора да биде врзан со дисциплина, со структурирано познавање. Карактеристика на една професија е континуирано и насочено развивање. Ваквиот развој овозможува доверба на заедницата во основата на знаењето и вештините на професијата.

Јадрото во достигнувањето на професионалност во корпоративната безбедност е дефинирано тело на знаење, како и специјализирани технички и генерички менаџерски вештини. Корпоративната безбедност допрва ќе се дизајнира како академска дисциплина, бидејќи се уште има недостаток на валидност во карактеристиките на традиционалните дисциплини. Сепак, корпоративната безбедност содржи богата основа на знаење и оние кои работат во овој сектор имаат уникатни вештини и знаења. Еден аспект на професионализам во доменот на корпоративната безбедност се споделените поранешни искуства, како оние на поранешно-воените професионалци и професионалците за спроведување на законот.

Дисциплината бара дефинирана и инклузивна дефиниција; сепак, корпоративната безбедност останува недефинирана, разновидна имултидимензионална. Како што Смит и Брукс⁸ предлагаат, можеби безбедноста е еден концепт кој уште од неговата првобитна употреба, повеќе од неколку декади, не се променила; туку станала пошироко употребувана за да се опфати поразновидно значење. Сепак, во дадениот контекст, безбедноста може да се дефинира. Корпоративната безбедност овозможува ваков применлив контекст.

Безбедносната едукација се уште е нецелосна и се уште постои ограничено истражување да се сумира што содржи знаењето за безбедноста⁹, заедно со корпоративната безбедност како една негова област. Овој фактор е важен, земајќи го предвид порастот на терциалните едукативни безбедносни програми, особено во рамките на САД. Многу од оние кои влегуваат во корпоративната безбедност се второ кариерен воен персонал или персонал за спроведување на законот, кои

⁸ Smith, C. L. (2001b). Security science: An emerging applied science. *Journal of the Science Teachers Association of Western Australia*, 37(2), 8–10.

Brooks, D. J. (2009a). Key concepts in security risk management: A psychometric concept map approach to understanding. Saarbrücken: VDM Verlag.

⁹ Nalla, M. K. (2001). Designing an introductory survey course in private security. *Journal of Criminal Justice Education*, 12(1), 35–52.

можеби немаат бизнис искуство, но им бил даден приоритет кога биле назначувани како безбедносни менаџери.¹⁰

Се расправа дека корпоративните безбедносни менаџери регрутирани од редовите на војската и полицијата за спроведување на законот донесува лидерство, ресурсен менаџмент, стратегиски фокус, политичко разбирање, комуникативни вештини и соодветен јазик да се вклучи извршната власт. Тие исто така донесуваат искуство и степен на сериозност која на организацијата и дарува степен на кредибилитет. Понатаму се предложува дека потенцијална позитива е ширината на контакти и безбедносни мрежи кои доаѓаат со овие индивидуи. Како и да е, ваквиот сет на вештини не е неоспорен и постои перцепција дека може да бидат аверзни кон ризик и може да им недостасува мекост во менаџирањето и лидерските вештини кои што се потребни во корпоративната средина.

Функции на корпоративната безбедност

Улогите на менаџерите

Улогата е сет од очекувања за нечие однесување. Улогите на менаџерите се групирани во информациони улоги, интерперсонални улоги и одлучувачки улоги. Интерперсоналната улога вклучува фигуративна улога на водител, лидер и активности на воспоставување на врски. Информативната улога вклучува мониторирање, дисеминација и активности на портпарол. На крај, одлучувачката улога вклучува улога на претприемач, одговорен за справување со нарушувања, распределувач на ресурси и преговарач.

Краут и соработниците идентификувале седум групи на менаџерски задачи, кои тогаш биле споредени низ менаџерските класи. Овие задачи вклучувале менаџирање на индивидуалниот перформанс, давање на инструкции на

¹⁰ Gill, M. (2007). The challenges for the security sector: thinking about security research. Security Journal, 20, 27–29.

подредените, планирање и распределба на ресурси, координирање на меѓусебно зависни групи, менаџирање на групниот перформанс, надзор на бизнис средината и претставување на кадарот. Овие податоци потоа биле споредени низ функционалните оддели, во овој случај маркетинг, производство и администрација. Важноста на менаџерските активности останува разумно константна низ функционалните домени, укажувајќи повеќе на сличности отколку на разлики.

Структура на корпоративен безбедносен менаџмент

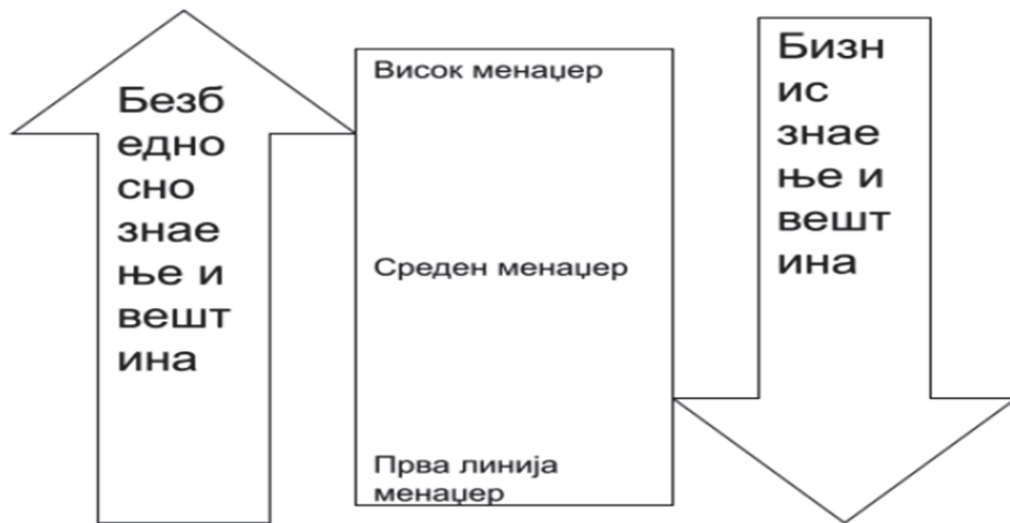
Корпоративниот безбедносен менаџер не се разликува од било кој друг менаџер во рамките на организацијата, освен по неговите технички вештини. Сепак, како со секој менаџер, степенот до кој ваквите технички вештини се потребни се намалува, како што безбедносниот менаџер се движи од прволиниски кон извршен менаџмент. Она што е потребно во пониските нивоа на менаџмент е специфичното корпоративно безбедносно знаење.

Знаењето треба да се развива врз истражување базирано на докази. Многу терцијално корпоративни безбедносни едукативни програми се развиле од слични дисциплини, како полициски студии, правни студии, криминологија, политички науки или инжињерски студии. Многу други програми за корпоративната безбедност се понудени само на стручно ниво, ограничувајќи го капацитетот на индустријата за вистински професионализам врз основа на точни информирани истражувања и цврсто тело на познавање.

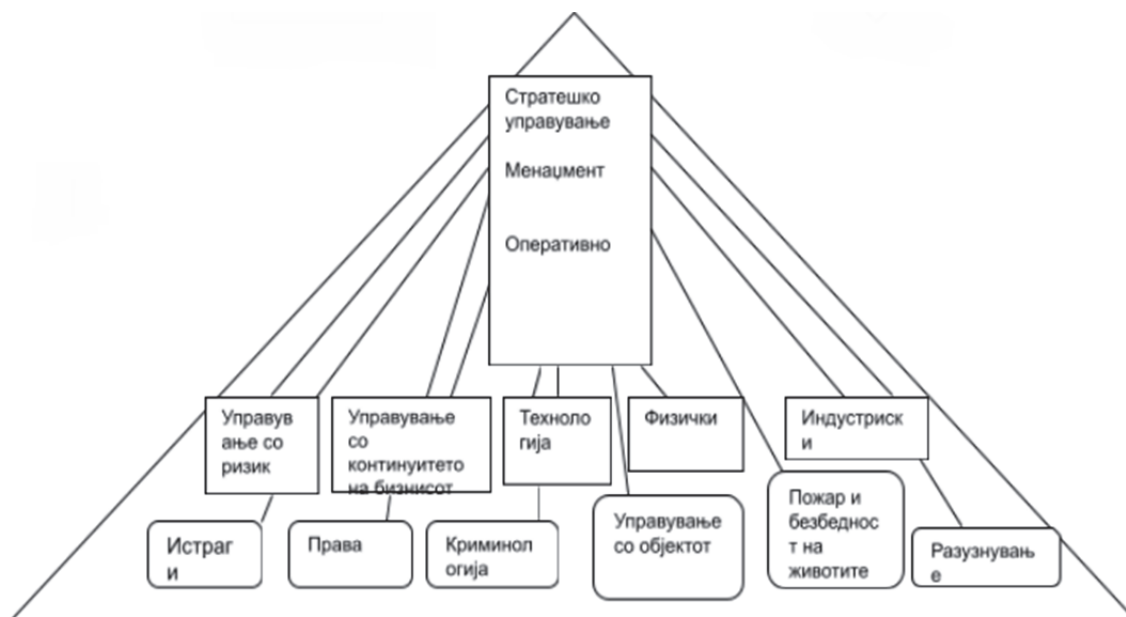
Во почетокот на нивната кариера, позицијата на корпоративниот безбедносен менаџер бара технички специфични познавања. Како што се унапредуваат во корпорацијата, таквото познавање станува повеќе генеричко деловно познавање. Сепак, ваквите ставови се спротивставуваат на некои индустриски групи, како ASIS International, кои имплицираат дека многу сојузнички дисциплини треба да бидат одделени од безбедноста.

Техничка корпоративна безбедносна дисциплина

Постои истражување за корпоративната безбедносна функција која започнува да ги дефинира вештините и знаењата во рамките на оваа дисциплина. На пример, Брокс¹¹ анализира 104 безбедносни курсеви за додипломски студии од Австралија, Јужна Африка, Велика Британија и САД. Од оваа анализа, откриени се 2.001 безбедносни концепти со уште 14 имплицитни концепти кои се сметаат за категории на познавање. Покрај тоа, студијата користела други поврзани научни трудови за поддршка и одобрение на овие категории на познавањето на корпоративната безбедност.



¹¹ Brooks, D. J. (2009a). Key concepts in security risk management: A psychometric concept map approach to understanding. Saarbrücken: VDM Verlag.



Слика 1. Менување на телото на знаење за менаџер за корпоративна безбедност

Дополнителните студии опфаќале курс за безбедност насочен кон кривично-право, интегрирана рамка на корпоративна безбедност, тело за познавање за управување со ризикот од безбедноста и Меѓународниот симпозиум за академски/практичари на ASIS.14-те категории на познавање беа интегрирани во рамките на корпоративната безбедност, спротивставувајќи се на многу минати студии кои претставија тесен пристап кон оваа разновидна улога, како што се Коои и Хиндија¹². Исто така сугерираат дека корпоративната безбедност е "поврзана со заштитата на ресурсите, физичкото обезбедување, безбедноста на информатичката технологија и безбедноста на персоналот". Ова гледиште може да биде точно, но нема пошироко познавање и вештини кои ги бара корпоративниот менаџер за безбедност. Овој домен беше поддржан од Јејтс¹³, кој изјави дека традиционалната безбедносна категоризација не го зема предвид големиот број на функции поврзани со безбедноста, вклучувајќи континуитет во

¹² Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. *Journal of Criminal Justice Education*, 19(2), 290–307.

¹³ Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. *Journal of Criminal Justice Education*, 19(2), 290–307.

работењето, одговор при катастрофи, безбедноста на информациите и управувањето со ризиците.

Интегрираната рамка за корпоративна безбедност ги означува клучните категории на познавање за безбедноста (Ниво 1), кои опфаќаат управување со безбедносниот ризик, управување со континуитетот на бизнисот, технологијата, физичко обезбедување, персоналот и индустријата. Технологијата се смета дека опфаќа системи како CCTV – систем на камерите за снимање, контрола на пристап, откривање на упад во компјутерскиот систем и компјутерите. Управувањето со континуитетот на бизнисот (BCM) ги опфаќа категориите на безбедносен модел за планирање на вонредни ситуации/континуитет на процесот на организацијата, управување со кризи и категории за управување со катастрофи. Индустриската безбедност ги дефинира аспектите на функциите поврзани со безбедноста, на пример во рамките на безбедноста во воздухопловството и меѓународната легислатива за меѓународно цивилно воздухопловство (ICAO).

Второто ниво (Ниво 2) може да се смета за сојузнички или пропратени дисциплини или практични домени, тесно поврзани со корпоративната безбедност. На пример, криминологијата може и се користи за подобро разбирање на стратегиите за спречување на криминалот или за криминалните мотиватори.

Потребно е дополнително истражување за да се развие и креира концензус за категориите на познавање со цел да се презентира робустната корпоративна безбедносна дисциплина. На пример, јазикот мора да стане попрецизен за да се постигне заедничко разбирање во корпоративната безбедност. Континуираното истражување на познавањето од таквите организации како ASIS International, како и развојот на национални и меѓународни професионални организации, ќе резултира со заедничко разбирање.

Стратегија за управување со корпоративната безбедност

Функцијата на корпоративниот менаџер за безбедност може да се подели на три различни вертикални нивоа на управување, започнувајќи со менаџер за безбедност на првата линија од управување и завршувајќи со високите извршни директори. Вештините на овие различни менаџери се разликуваат кога се движат нагоре кон корпоративната средина. Во крајна линија, се тврди дека менаџерот за корпоративна безбедност има највисоко достигнување во управувањето со средното ниво, и доколку не можат да развијат различни и пошироки корпоративни вештини, тие ќе останат на тоа ниво. Практичните области, од кои доаѓаат многу менаџери за корпоративната безбедност и вештините што ги добиваат во својата почетна кариера, ги ограничуваат да се движат само во рамките на управувањето на средниот менаџмент.

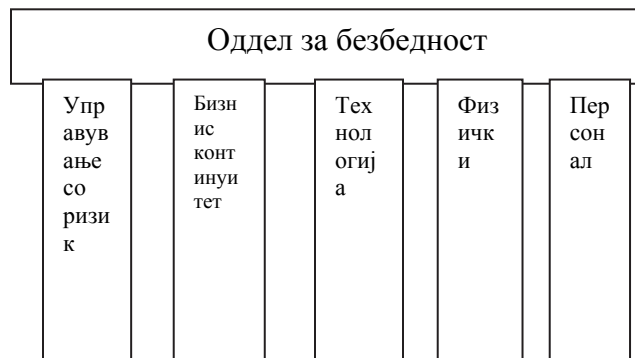
Прва линија безбедносен менаџер

Линиските безбедносни менаџери (Ниво 1) одговараат на безбедносниот среден менаџер (Ниво 2) за обезбедување на безбедносни совети, асистенција и политика конзистентна со пошироката корпоративна политика според потребите на местото, објектот или организацијата. Додека одговорноста за безбедноста на дадено место му е доделена на менаџментот на местото, линискиот менаџмент е одговорен за политиката и имплементацијата на безбедносните процедури.

Технички вештини

Линискиот безбедносен менаџер бара високо ниво на технички вештини. Оваа вештина подразбира специјализирано познавање, аналитичка способност и употреба на алатки и техники. На пример, за безбедносниот менаџер ваква способност е разбирањето на аналитиките на проценка на закани и развојот на стратегија на мерки за ублажување или поврзување на CCTV – систем на камерите за снимање.

Како што предлага Брукс, вештините може да се дефинираат како управување со безбедносните ризици, технологија за континуитет на бизнисот, физичка безбедност и лична безбедност. Како и да е, овие вештини се практикуваат внатрешно и изолирано од останатите, во затворен пристап. На пример, тие можат да се фокусираат на безбедноста како физичка или техничка или во рамките на личната безбедност.



Слика 2. Изолирани вештини на менаџерот за безбедност на предната линија

Контрола и одговорности

Прволинискиот безбедносен менаџмент се фокусира на директна контрола на внатрешната работна сила и стапува во интеракција со ограничена надворешна работна сила. На пример, практикувањето на безбедносниот менаџер во силосот на персоналните вештини може да менаџира со приватните безбедносни чувари кои се од надворешни приватни фирми. Техничкиот безбедносен менаџер ќе стапува во интеракција со интеграторите на електронскиот безбедносен сектор. Безбедносниот менаџер кој практикува бизнис континуитет или ризик менаџмент ќе има ограничена надворешна интеракција, но ќе се вкрстува со многу внатрешни бизнис единици.

Безбедносните линиски менаџери обезбедуваат технички специфични совети или безбедносна поддршка на сите нивоа во местото, објектот или организациониот менаџмент, како и за прегледување на соодветноста на

безбедносните договори. Одговорностите го вклучуваат спроведувањето на истражниот менаџмент на специфични безбедносни функции и проекти како што е наложено. Линискиот менаџер одржува соодветна врска со безбедноста и полициските организации, како и со други релевантни оператори во рамките на индустријата на локално ниво. Линискиот менаџер е исто така одговорен да обезбеди индустриски консултанти и други личности на кои им е дозволен пристап до местото објектот или организацијата, со кои се имплементираат и одржуваат стандарди за безбедност во согласност со локалните прописи и правила.

Средно ниво на безбедносен менаџер

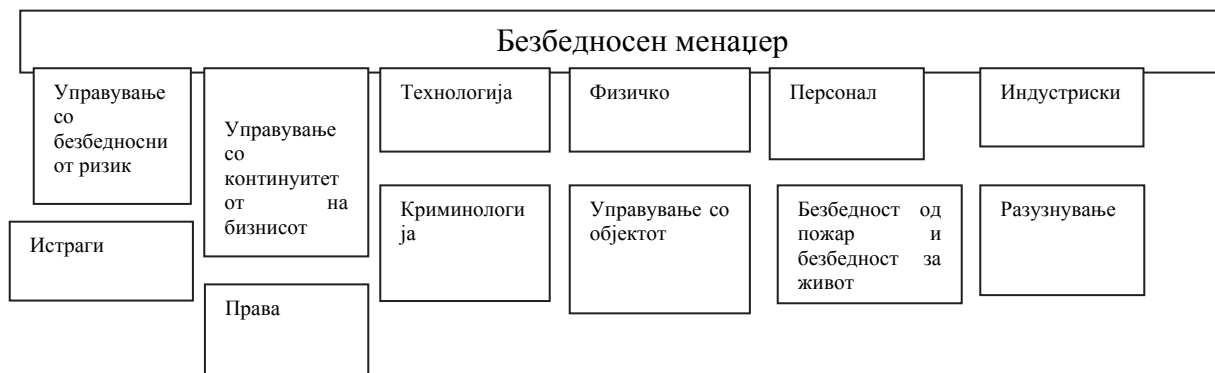
Безбедносниот менаџер (Ниво 2) е одговорен за менаџментот на безбедносните ресурси на бизнис единиците и средствата, како и за обезбедување на безбедносен совет за менаџментот на бизнис заедницата. Безбедносниот менаџер е исто така одговорен за обезбедување на анализи на закани и ризици за бизнис заедницата. Авторитетот на безбедносниот менаџер е делегиран од главниот извршен офицер или главниот безбедносен офицер.

Технички вештини

Техничките вештини за безбедносниот менаџер на средно ниво значително ја намалуваат важноста, како што фокусот се движи кон дијагностицирање на проблеми и концептуалните и хуманите вештини стануваат далеку поважни за решавањето на проблемите. Сепак, постои ограничено дефинирано разбирање за тоа какво познавање треба да имаат. Според тоа, земајќи предвид категоризацијата од учењето на Брукс, дефинирана е област на вештини и познавања што се протегаат од линискиот менаџер. На овој начин знаењето се шири низ широк спектар од управувањето со безбедносните ризици до специфична апликација за индустријата. Овие менаџери, исто така, можат да имаат директни одговорности за поврзаните вештини, како што се истрагите за разузнавачката функција.

Менаџерот за безбедност на средното ниво мора да стане помалку специјалист а повеќе генералист; сепак, ваквата генерализација мора да се прошири низ многу области во корпоративна безбедносна пракса. Како Прензлер и Сор.¹⁴ кои упатуваат дека ‘корпоративната безбедност мора да опфати голем број јасни области на пракса, како што се управувањето со безбедносните ризици, управувањето со безбедноста, управувањето со континуитетот на бизнисот и бизнисот, како и безбедносната технологија.

Таквиот широк пристап кон корпоративната безбедност е истакнат кога одредени закани потпаѓаат во функционалните јазови помеѓу безбедносните одделенија за физичка безбедност и информатичката технологија (ИТ), меѓу многу други функционални празнини. Историски гледано, ИТ - секторот се разликува од физичката безбедност, додека во современите корпорации овие улоги можат да паднат под еден ист среден менаџер. Искуството на менаџерите е помалку важно од нивната способност да планираат, организираат, да доделуваат должности на персоналот, да водат и да ги контролираат овие практикантски области .



Слика 3. Средно ниво на проширување на безбедносните менаџерски вештини и знаења

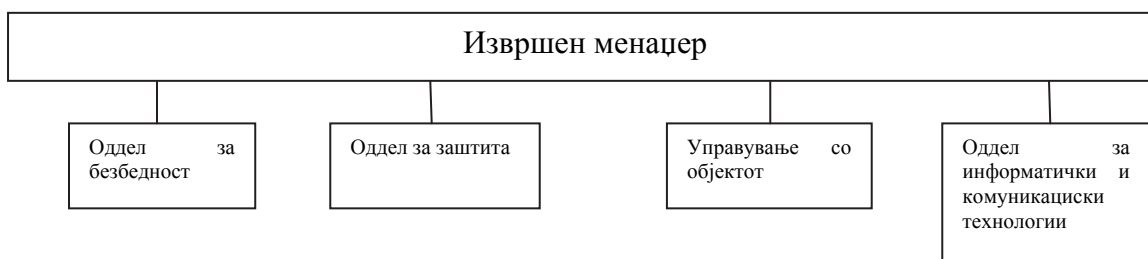
¹⁴ Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. Journal of Criminal Justice Education, 19(2), 290–307.

Контрола и одговорности

Генерално земено, "безбедноста е поставена на менаџерските позиции на средното ниво, што е скромно ниво со оглед на тековното меѓународно безбедносно опкружување". Управувањето со средното ниво на безбедност останува доминантно фокусирано како внатрешно контролна функција. Контролата на ова ниво е воспоставена преку примена на постапки и процедури и кога е потребно и истраги. Ваквата внатрешна контрола ја ограничува способноста на безбедносниот менаџер да ја води коорпоративната безбедност во рамките локалната средина.

Висок безбедносен извршен директор

Функцијата на високиот извршен менаџмент за безбедност (трето ниво) е фокусирана на водење на бизнисот до постигнување на стратешка контрола преку поврзување со надворешната социо-културна средина. Стратегија на ниво на корпорација се занимава со прашањето: "во каков бизнис сме ние?" однесувајќи се на целата организација, но и на целиот бизнис во комбинација на сите продуктни единици кои ја формираат целата целина. Безбедносниот менаџер веќе не го контролира само безбедносниот сектор, туку и неколку сектори заедно.



Слика 4. Висока извршна функција

Технички вештини

За безбедносниот извршен директор, функционалната и техничката експертиза стана помалку важна отколку разбирањето на основите на бизнисот и стратегијата. Искуството на високиот менаџмент станува неопходен квалитет како што безбедносниот менаџер се искачува нагоре низ нивоата на корпоративниот менаџмент.

Многу од безбедносно-специфичните технички вештини на менаџерите од средно ниво стануваат излишни. Извршниот директор не само што ќе ја менаџира безбедносната функција, туку веројатно е дека ќе менаџира и други области како менаџирање на ризик и бизнис континуитет, здравје и заштита, интелигенција и во зависност од контекстот на средината, грижата за заедницата, надворешната средина и менаџирањето на објектите. Корпоративниот безбедносен менаџер веќе не постои како функционален менаџер.

Контрола и одговорности

Високиот безбедносен менаџмент се фокусира на контролирање и оформување како на внатрешната така и на надворешната средина. Ваквата контрола се постигнува не само преку водство туку и преку политичка, културна свесност во водењето преку корпоративната безбедност. Безбедносниот извршен директор е дипломатот, кој гради соработка и врски на почит, како со внатрешните така и со надворешните акционери кои може да бидат афектирани од перспективите на корпоративната стратегија. Поседувањето свест за средината, спремноста на изненадувања, следењето и влијаењето врз акционерите, со цел да се постигне контрола соодветна на стратегиските перспективи бара значајно искуство и висок степен на когнитивни вештини.

Извршниот безбедносен директор е одговорен за обезбедување на стратегиска безбедносна интелигенција и за безбедносниот ризик менаџмент во поддршка на целиот бизнис. Безбедносниот извршен директор треба да биде бизнис лидер кој се бори за безбедноста за поголем бенефит на организацијата,

постигнат преку добро дефинирано разбирање на заканите со стратегија за намалување на трошоците која ќе ги заштити критичните функции на организацијата во бизнис смисла. Водството на безбедносните прописи и врски треба да биде обезбедено и воедно активно да ја оформува надворешната и внатрешната безбедносна средина во согласност со потребите на бизнисот од стратегиска перспектива. Безбедносниот извршен директор развива и одржува врски со владиното обезбедување, разузнавањето и полициските структури, како и други корпорации во рамките на индустријата на национално или интернационално ниво.

Функционалните вештини на безбедносниот корпоративен менаџер

Функционалните вештини и познавања на безбедносниот корпоративен менаџер се подобруваат во зависност од неговото менаџерско ниво. На пониско вертикално ниво, вештините и знаењето се подефинирани и врзани во рамките на практичната област

Најефективната безбедносна програма е комбинација од оперативен и стратегиски напор поддржан од информација, разузнавање и познавања кои потекнуваат од соработка со внатрешните и надворешните акционери. Безбедноста заснована на ефективна стратегија носи можности за водење на безбедносна средина, за разбивање и превенирање на криминална активност, за одржување на рамнотежата помеѓу побарувачката и добавувањето, како и ултимативно достигнување на позитивна исплатливост на индустријата и заедниците поврзани со неа. Таа позитивна исплатливост може да биде подобрен профит, репутација или одржливост.



Слика 5.Еволуција на менаџерските функционални вештини

Односот на корпоративната безбедност и приватната безбедност

Во осумдесеттите години на 20 век дошло до бран на приватизација во кој голем број од јавните сервиси и инфраструктури биле преместени во приватниот сектор. Податоците укажуваат на тоа дека помеѓу 1980-1992 година осумдесет држави во светот приватизирале приближно 6800 државни претпријатија.

Предводник била Велика Британија која најпрво ја денационализирала британската воена индустрија, за во текот на 1980 година, истата програма да ја прошири и на споредбените одбранбени услуги, како што се набавка, обезбедување, обука, снабдување и поддршка на операциите. Тоа било урнек кој го следела владите на бројни земји во тој период, а главен аргумент било намалување на трошоците, префрлање на ризикот, како и зголемување на економската флексибилност и ефикасност на државните институции.¹⁵

Преносот на државните функции на приватниот сектор се случува на сите полиња на државната активност, вклучувајќи ги и оние врз кои националната држава порано држела монопол.¹⁶ Одговарајќи на прашањето зошто безбедноста е приватизирана, П. Сингер, познат автор којшто се занимава со оваа тематика, истакнал дека не постои една причина која довела до оваа појава. Тој наведува дека приватизацијата на безбедноста е јасен и впечатлив претставник на променетата глобална безбедност и работното опкружување на почетокот на 21 век.¹⁷

На процесот за приватизација на секторот за безбедност многу влијаеле и транзиционите процеси, т.е. воспоставување на моделот на пазарна економија. Тоа довело до создавање на специјализиран пазар за одредени услуги од безбедноста, посебно во делот на заштита на имотот и лицата, како еден од битните фактори на стопанското работење.¹⁸

Во развиените земји на Запад главен поттик за приватизација на безбедносните функции се однесувал на барањето за зголемување на ефикасноста

¹⁵ Buckland, B., Winkler, T. (2011), *Javno-privatna saradnja: izazovi i mogucnosti upravljanja bezbjednoscu*. Beograd, forum za bezbednost i demokratiju.

¹⁶ Schreier F., Caparini, M. (2005), *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, Geneva, DCAF

¹⁷ Singer, P. (2003), *Corporate Warriors: The Rise of the Privatized Military Industry*, Ithaca, Cornell University Press

¹⁸ Trivan D., *Detektivska delatnost*, Beograd, 2014 godina, str. 65.

во државните институции, на кое е одговорено со outsourcing на безбедносните работи кои традиционално ги извршувал државниот сектор.¹⁹

Во литературата, постојат два основни пристапа за дефинирање на приватниот безбедносен сектор. Првиот пристап, приватниот сектор за безбедност го дефинира како збир организирани облици на дејствување на доброволниот и комерцијално насочен недржавен (приватен) персонал чии дејности вклучуваат спротивставување на криминалното однесување. Така, дефинираниот приватен сектор на безбедност го сочинуваат:

- 1) Доброволното граѓанско учество;
- 2) Приватното обезбедување;
- 3) Приватната детективска активност.²⁰

Во потесна смисла, односно според вториот пристап, приватната безбедност може да се дефинира како збир од законски втемелени активности, надвор од надлежните рамки на државните органи, кои се организирани за давање услуги за заштита на лична и имотна сигурност на граѓаните. Во вака дефинираниот поим се вклучени:

- 1) Договорното обезбедување - дејноста на приватни претпријатија и агенции специјализирани за давање физичко-техничко обезбедување на договорна основа;
- 2) Внатрешно (сопствено) обезбедување;
- 3) Приватна детективска дејност.

Дефиницијата на приватната безбедност која ја предложил А. Кржалиќ гласи; “Приватната безбедност е гранка на безбедноста која со организирано самостојно или со заедничко систематско и планско дејствување по пат на

¹⁹ Toyne Sewell Patrick, Private Security Companies: The Reasons Why, Military Technology, Vol. 31, Issue 3, Monch Publishing Group, Bonn, 2007, pp. 60-61

²⁰ Мојаноски, Ц, Т., Ѓуровски, М, & Павловиќ, Г. (2018). Вовед во безбедноста. Скопје, Македонија: Фондација Конрад Аденаурер.

поединци, организациите, приватни или професионални компании, обезбедува лична заштита или заштита на другите, како и заштита на соодветни високопозиционирани личности, простори, работење, а кои не се во надлежност на државните органи”.

Во согласност со ова, приватната безбедност може да има двојно значење: може да означува давање безбедности услуги од страна на претпријатијата во приватна сопственост или самите тие услуги, односно безбедносни работи кои се вршат по барање на приватните лица или приватни организации. Услугите кои ги нудат овие компании се: физичка заштита, техничка заштита, детективски услуги, стручно советување, обука и тренинг на полициски единици, разузнавачка дејност, заштита на високоризични објекти и постројки, обезбедување конвои на хуманитарна помош и превоз на стока, лична безбедност за ВИП личности, логистичка поддршка и друго.²¹

Оттаму, можеме да заклучиме дека приватната безбедност може да има двојно значење, односно, може да означува давање безбедносни услуги од страна на приватно претпријатие, или услуги кои се вршат по барање на приватни претпријатија.

Во најширока смисла, поимот приватна безбедност би можел да ги означува сите безбедносни дејности кои не ги врши државата и нејзините органи, додека приватниот сектор за безбедност би ги опфаќал приватните претпријатија кои даваат услуги на безбедност и/или производи наменети за безбедност.²²

За приватниот сектор за безбедност може да се каже дека настанал со трансформација на класичниот модел на заштитна функција на државата. Функцијата, сложеноста на работите и задачите на овој сектор, се одгледуваат низ мноштво карактеристики, од кои некои се иманентни само за него.

²¹ Krzalic, A., Stanje privatne sigurnosti u Bosni i Hercegovini, Sarajevo, 2009

²² Мојаноски, Ц, Т., Ѓуровски, М, & Павловиќ, Г. (2018). Вовед во безбедноста. Скопје, Македонија: Фондација Конрад Аденаурер.

Карактеристиките на приватниот сектор за безбедност се подразбираат дека тоа се:

- Сектор кој го карактеризираат мноштво поддоговори;
- Конкурентен сектор. Конкуренцијата во овој сектор е многу голема. Договорите за давање безбедносни услуги најчесто се склучуваат по системот на најповолна понуда, отколку по системот на најдобра понуда, односно онаа понуда која гарантира висок квалитет на услуга, добри работни услови, во склад со колективните договори, важечките закони, должности и одговорности кон клиентот. Нелојалната конкуренција, која е евидентна, аматеризмот во работењето, илегалната практика и др., ја расипуваат сликата за приватниот сектор за безбедност и имаат негативно влијание врз него;
- Флексибилен сектор. Приватниот сектор за безбедност дава услуги 24 часа дневно и седум дена во неделата и е во состојба да одговори на различни барања на клиентот. Овој вид флексибилност се одгледува на различни начини, на пр. Во бројот на работници - што е поврзано со способноста на компанијата да вработи онолку работници колку што бараат различните ситуации за кои таа е одговорна. Понатаму, флексибилно работно време, односно нестандартни норми на работно време; се мисли на постојаната готовност, прекувремена и ноќна работа, работа за викенд, итн, флексибилност во можностите за вршење задачи кои мораат да ги спроведат работниците. Имено, тие мораат да бидат способни во секој момент да се приспособат на потребите на претпријатието и клиентот со цел да ги исполнат нивните различни непредвидливи барања. Претпријатијата се повеќе се потпираат на работниците кои покажуваат иницијатива во оваа смисла;
- Сектор кој се уште е потценет. Приватните компании кои даваат безбедносни услуги помагаат во тоа јавните места да бидат уште побезбедни и имаат придонес кон создавање безбедно општество во целина, така што јавните и приватните слободи и права можат да се уживаат без органичувања. Меѓутоа, овој придонес се уште не се

забележува во целост. Ова потценување на приватниот сектор за безбедност се рефлектира во извесна мера како игнорирање и недостиг на признавање на работата која ја вршат овие претпријатија и нивниот персонал, а што може да има негативни импликации за сликата во целокупниот сектор. За овој сектор да го добие признанието кое го заслужува, потребни се иницијативи кои ќе ја зголемат свесна за улогата која приватниот сектор за безбедност ја има во општеството и проекти кои ќе ја подобрат сликата за него.²³

Широкиот спектар на луѓе, организацијата и активностите можат да бидат вклучени во давање воени и безбедносни услуги, како дома така и во странство. Меѓутоа, во стручната литература, приватните претпријатија кои даваат безбедносни услуги најчесто се делат според видот на безбедносните услуги кои ги нудат и внатрешната организација. Меѓутоа, приватните компании кои нудат безбедносни услуги, многу често ја комбинираат својата работа во повеќе области, па повеќето автори ги означуваат како приватни воено-безбедносни компании. Приватните воени и приватните безбедносни компании заедно можат да се дефинираат како компании кои работат на комерцијална основа, директно даваат воени и безбедносни услуги за профит. Приватните безбедносни компании се дефинираат и како компании кои се специјализирани за давање безбедносни услуги и заштита на луѓе и имот. Ова значи дека нивните вработени не мора да бидат наоружани, поради тоа и се вели дека нивните услуги се повеќе од дефанзивна отколку одофанзивна природа.²⁴

Питер Сингер, исто така, не прави разлика помеѓу приватните воени и приватните безбедносни претпријатија, па така го користи терминот приватни воени фирми, опфаќајќи ги на тој начин двата вида компании. Според авторот,

²³ ULB, UNI-Europa and CoESS, Preventing occupational hazards in the private security sector (manned guarding and surveillance services), Bruxelles, 2004

²⁴ Schulz, S., Yeung, C., Private Military and Security Companies and Gender, DCAF, Geneva, 2005, 1-3

приватните воени фирми се приватни работни ентитети кои им нудат на клиентите широк спектар на воени и безбедносни услуги.²⁵

Приватното обезбедување денес во светот евидентно се етаблира како важен сегмент на безбедносниот систем во целина. Приватно обезбедување претставува заштита на лица и имот што се врши од страна на правни лица кои имаат дозвола за приватно обезбедување. Според Законот за обезбедување, приватното обезбедување претставува дејност од јавен интерес кое има за цел спречување и откривање на штетни појави и противправни дејствија кои го загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува.²⁶

Приватното обезбедување се заснова врз следните начела:

1. непрекинатост во работата, односно подготвеност во секој момент, на секое место и во сите услови да се извршат поставените задачи за обезбедување на лица, имот и работење;
2. благовременост, односно превземање на одредени мерки, дејствија и постапки пред да се оствари активноста спрема лицето кое се обезбедува, имотот или работењето;
3. целокупност, односно координирано и сеопфатно функционирање на системот на обезбедување, односно неговите делови;
4. ефикасност, односно успешност која се постигнува со оспособеност на сите непосредни извршители соодветно да реагираат на сите облици на загрозување или обиди на загрозување и превземање на мерки за отстранување на последиците и евентуално реактивно дејствување;
5. релевантност, односно степен на веројатност дека системот односно неговите делови ја остваруваат улогата која им е наменета. Исто така, означува способност да се примени тоа што е планирано;

²⁵ Singer, P. (2003), *Corporate Warriors: The Rise of the Privatized Military Industry*, Ithaca, Cornell University Press

²⁶ <http://www.pravdiko.mk/ovlastuvan-ata-na-litsata-koi-vrshat-privatno-obezbeduvan-e/>

6. доверба, односно позицијата која ја завзема лицето и/или организацијата во смисла ниту една информација за клиентот (лицето и/или организацијата) да не биде достапна за други лица и/или организации.²⁷

Како работник за приватно обезбедување се смета физичко лице кое поседува важечка лиценца за приватно обезбедување и легитимација за приватно обезбедување, кое има засновано работен однос во правно лице и врши приватно обезбедување, односно работи и работни задачи врз основа на овластувањата утрдени со Законот за обезбедување.²⁸

Овластувањата на работниците за приватно обезбедување се следни:

- ☐ Да врши проверка на идентитет на лица при влез во имотот што го обезбедува;
- ☐ Да предупреди лице да се оддалечи од имотот што го обезбедува, ако лицето неовластено се задржува во него, односно да го предупреди лицето кое со своето однесување или пропуштање да стори нешто ја загрозува сопствената или безбедноста на другите или може да предизвика оштетување на имотот што се обезбедува;
- ☐ Не дозволи влез на неповикано лице, како и да забрани неовластено снимање или внесување на средства и опрема за таа намена во имотот што го обезбедува;
- ☐ Задржи и предаде на полицијата лице затечено во вршење на кривично дело за кое се гони по службена должност, до доаѓањето на полицијата;
- ☐ Врши преглед на лица, предмети, возила и багаж и употреби средства за присилба²⁹

Овие овластувања може да ги примени само во објектот што се обезбедува или до границата на просторот што се обезбедува, кога врши телесна заштита,

²⁷ Институт за стандардизација на Србија, Друштвена безбедност-Услуги приватниг пбезбечеоа-Захтеви и упутства за пцеоиваое усаглашености, првп издаое, Бепград, 2008 гпдина, стр. 3.

²⁸ Gligoroska, M., (2017), Корпоративна безбедност и државниот безбедносен систем. Факултет за детективи и криминалистика, Европски универзитет - Република Македонија

²⁹ <http://www.pravdiko.mk/ovlastuvan-ata-na-litsata-koi-vrshat-privatno-obezbeduvan-e/>

обезбедување на транспорт и пренос на пари и други вредносни пратки и мониторинг-патролнообезбедување. За време на вршење на приватно обезбедување работникот за обезбедување е должен да носи легитимација за обезбедување. Во случај кога работникот за обезбедување се повикува на своите работи и работни задачи е должен истовремено да ја покаже и легитимацијата за обезбедување. При примената на овластувањата работниците за обезбедување се должни да ги почитуваат угледот и достоинството на граѓаните, како и основните човекови права и слободи. Примената на овластувањата мора да бидат пропорционални на потребата поради која истите се применуваат.³⁰

Иднината на приватното обезбедување треба да се гледа во амбиентот на вкупните глобални безбедносни предизвици, локалното, регионално и глобално безбедносно опкружување, промените во каталогот на новите безбедносни ризици и закани. За остварување на оваа цел потребно е развивање на научноистражувачката и апликативната дејност која е поврзана со приватното обезбедување и нејзино теоретско-емпириско истражување и проучување.³¹

Физичко обезбедување

Компаниите за физичко обезбедување се најголемата и највидливата компонента на приватните безбедносни компании. Физичкото обезбедување претставува збир на оперативни и тактички мерки, работи, средства и сила на заштита на луѓе, личности на одредени функции, простории и објекти од посебно значење. Тоа е еден вид обезбедување кое го вршат за тоа посебно обучени и оспособени кадри, а може да биде јавно, тајно и комбинирано. Кај позначајните објекти обезбедувањето се комбинира со мерките и средствата на техничкото обезбедување - со примена на алармни средства, електронски и механички уреди за заштита.

³⁰ <https://www.pravdiko.mk/ovlastuvan-ata-na-litsata-koi-vrshat-privatno-obezbeduvan-e/>

³¹ Kozarev A., Privatna bezbednost u Republici Makedoniji - aktuelno stanje i perspektive, Zbornik radova - Prvi međunarodni naučni skup: Privatna bezbednost - stanje i perspektive, USEE, Novi Sad, 2008 godina, str.177

Работите на физичкото обезбедување можат да се поделат во четири групи, и тоа:

- ☐ Заштита на лица и имот;
- ☐ Транспорт на пари и останати вредности;
- ☐ Лична заштита на лица (bodyguard);
- ☐ Обезбедување собири

Физичкото обезбедување најчесто се поставува во облик на служба за физичко обезбедување (раководен кадар и непосредни извршувачи) кое се состои од одреден број работници кои поседуваат оружје и опрема, а чија цел е обезбедување лица и компании со сите нивни вредности и интереси. Физичката заштита, во согласност со ова, претставува заштита на луѓе и имот од уништување, оштетување, кражба и други облици на дејствување кои се опасни или штетни по животот и имотот на претпријатието. Работникот на обезбедувањето непосредно го чува и го контролира просторот или објектот врз основа на план за обезбедување, спречува влез на неовластени лица во објектот или просторот кој го чува и ги употребува средствата за техничка заштита на објектот. Исто така, непосредно врши физичка заштита на објектот, собира безбедносни сознанија на работното место во врска со заштитениот објект, врши надзор врз влезовите на објектот, врши легитимирање, односно спречува пристап на неовластени лица во непосредна близина на заштитениот објект, води потребна евиденција, составува соодветни извештаи за извршената работа.³²

Три основни организациски облици на службата за физичко обезбедување се:

- I. Сопствена служба за физичко обезбедување како организациска целина на претпријатието, односно установата;

³² Мојаноски, Ц, Т., Ѓуровски, М, & Павловиќ, Г. (2018). Вовед во безбедноста. Скопје, Македонија: Фондација Конрад Аденаурер.

- II. Ангажирана служба за физичко обезбедување (служба за физичко обезбедување која ја изнајмуваат претпријатијата специјализирани во оваа област) и
- III. Комбинирана служба за физичко обезбедување (делумно сопствено, делумно изнајмена служба за физичко обезбедување).³³

Техничко обезбедување

Компаниите за техничко обезбедување се компании кои се занимаваат со вградување и одржување на системите за техничка заштита. Некои од тие системи се врзани со инсталирање аларм, уред за брза реакција, заштита, контрола на пристап и слично. Според ова, техничкото обезбедување подразбира механичка и електронска заштита на лица и имот, а најчесто е организациски поставено во рамките за службата за обезбедување во оние претпријатија каде е организирано.³⁴

Оттаму, техничкото обезбедување и заштита на лица и имот, претставува заштита односно спречување недозволен пристап од одредено лице или објект, информации и др., со употреба на технички средства. Меѓутоа, истото не мора да се подразбира и намалување на улогата на физичкото обезбедување. Техничките средства обезбедуваат заштита, но во момент на опасност, се активираат и преземаат мерки за отстранување на опасноста.

При изборот на технички средства и системи за заштита на објектот, постојат одредени околности кои мора да се земат предвид. Тие вклучуваат; безбедносна процена, големина и намена на објектот, опрема и предмети кои се содржат во објектот, режимот на работа на објектот, итн.

³³ Ivetić, S., Pavlović G. Uporedni modeli privatnog obezbjeđenja licnosti i objekata, Monografija, OEBS, Misija u BiH, Sarajevo, 2015.

³⁴ Ivetić, S., Pavlović G. Uporedni modeli privatnog obezbjeđenja licnosti i objekata, Monografija, OEBS, Misija u BiH, Sarajevo, 2015. Str-27

Други околности кои можат да влијаат, се следните:

- ☐ Физичка природа на објектот (на пр., положба, близина на други објекти, градбени материјали), план на зградата, големина, итн;
- ☐ Активност која се изведува во или околу објектот;
- ☐ Природа на околниот амбиент;
- ☐ Можност од закана (на пр., тероризам или организиран криминал);
- ☐ Минато искуство во врска со безбедносната заштита и филозофија на менаџментот.³⁵

Спроведувањето на техничка заштита, исто така подразбира:

- Изработка на процена на загрозеност на објектот којшто се штити;
- Изработка на безбедносен елаборат;
- Дефинирање на проектната задача;
- Проектирање на системот за техничка заштита;
- Изработка на системот за техничка заштита;
- Стручен надзор;
- Технички преглед и прием на системи за техничка заштита;
- Одржување и сервисирање на системите за техничка заштита

Детективски работи

Приватна детективска дејност, претставува специфичен вид на приватно безбедносно ангажирање на одредени лица во согласност со законските норми кои ја регулираат детективската дејност и другите правни норми кои се применливи на детективската дејност.³⁶

³⁵ Ivetic, S., Pavlovic G. Uporodni modeli privatnog obezbjedjenja licnosti i objekata, Monografija, OEBS, Misija u BiH, Sarajevo, 2015.str-123

³⁶ Boskovic, M., Osnovni detektivskog delatnosti, Novi Sad, 2006

Приватните детективи нудат различни услуги. Тие собираат податоци во врска со старателство, пронаоѓаат исчезнати лица, врачуваат судски пошти, собираат информации за деловни партнери и претпријатија, проверуваат податоци за лица кои аплицирале на одредена работна позиција, собираат информации во врска со кражба на автоски права, и слично.³⁷

Моќта на корпоративната безбедност

Усогласувањето помеѓу корпоративната безбедност и корпоративниот бизнис го има своето значење директно и индиректно. Следното е моќта и значењето на корпоративната безбедност за компаниите:

Обезбедување на заштита на персоналот, клиентите и имотот

Примарна цел на корпоративната безбедност е да се спречи и заштити компанијата, вработени, клиенти, податоци за клиенти, технички ресурси и средства на компанијата од внатрешни и надворешни закани. Ефективната корпоративна безбедност ги обезбедува вработените од какво било дело крадење, пожар, насилство, итн. Го обезбедува клиентот од хакирање на податоците како информации за клиентите, обезбедува средства од дело на злонамерна штета, пожар, кражба, злоупотреба. Ја обезбедува компанијата од дело на измама што може да ја сторат вработените или надворешните лица итн.

Обезбедување на економска и финансиска одржливост

Некои акти во рамките на компанијата влијаат врз економската и финансиската состојба на компанијата. На пример, ако има честа постапка за измами во компанијата е веројатност за компанијата да ги изгуби приходите, актите за проневери и акти на корупција во рамките на компанијата ја повредуваат економската и финансиската одржливост. Незаконските дејства може

³⁷ Vejinovic, D., i dr., Detektivska djelatnost, Banja Luka-Ljubljana, 2008

да се однесуваат на потрошувачите и тоа да доведе до клиентите да го проверат старателството со компанијата, па оттука и загубата на клиенти. Затоа, корпоративната безбедност е значајна бидејќи уверува отсуството на сите овие акти, па оттука и непречено одвивање на деловната активност што ја одржува економската и финансиската позиција на компанија.

Чување на угледот на компанијата

Повторното појавување на катастрофалните акти во компанијата е веројатно да го повреди угледот на компанијата социјално, економски и финансиски. Ефективната корпоративна безбедност дејствува како доверител за угледот на компанијата, ги елиминира сите закани и ја штити компанијата од секаков вид на нелегални намери упади, па оттука има создавање на погодно работно и деловно опкружување.

Корпоративни постапки за безбедност

Корпоративните безбедносни процедури се практики кои ја цртаат картата за тоа како безбедноста се претпоставува дека ќе се постапува со корпоративни субјекти и ефикасноста на корпоративната безбедност тестирана преку овие постапки. Стандардноста за усогласеност со овие постапки ја прави ефективност на корпоративната безбедност. Затоа, во делот се дискутираат заедничките безбедносни процедури кои се ризични за проценка и анализа, безбедносната политика и нејзиното спроведување, поставувањето на безбедносните мерки/системи и следењето на усогласеноста на безбедносните политики и мерки.

Безбедносна политика

Во бизнисот, безбедносна политика е документ во кој пишува писмено како компанијата планира да заштити имотот на компанијата и информатичката технологија (ИТ) на компанијата. Безбедносната политика често се смета за „жив документ“, што значи дека документот никогаш не е готов, туку континуирано се ажурира со промена на технологијата и побарувањата на вработените. Безбедноста на компанијата и политиката на самата компанија може да вклучува политики за прифатлива употреба, опис на тоа како компанијата планира да ги едуцира нејзините вработени за заштита на имотот на компанијата, објаснување за тоа како безбедноста ќе се извршува и спроведува, како и постапка за проценка на ефективноста на безбедносната политика за да се осигура дека ќе бидат направени неопходните корекции.³⁸

Со други зборови, безбедносната политика е писмена изјава за тоа како организацијата ги штити своите вработени, посетители, средства и податоци за информации. Честопати, бизнисите се наоѓаат со обемни безбедносни политики или дури повеќекратни политики, кои се скоро невозможни да се одржат и спроведат рачно. Организациите кои се многу сложени или работат во силно регулирана индустрија го чувствуваат тоа најостро, но дури и помалите бизниси се борат да најдат време и ресурси за да ги потврдат усогласеностите со политиката. Но, целта на безбедносната политика е да обезбеди поголема контрола и видливост во безбедносен систем во рамките на корпоративниот субјект и таа цел се постигнува само ако имате ефикасен начин за управување со вашата безбедносна политика. Решенија што ја автоматизираат безбедносната политика, управувањето е најефикасниот начин да се обезбеди ажурирање на политиката, а исклучоците брзо се идентификуваат и корегираат.

³⁸ Rouse M 'security Policy' retrieved from www.searchsecurity.techtarget.com as updated in May 2007

Квалитети на добрата безбедносна политика

Безбедносната политика е жив документ кој треба да биде мапа за да се демонстрира како корпоративната безбедност може да се одржува во рамките на компанијата. Најчесто корпоративната политика за безбедност се очекува да живее подолго и да ги постигне своите цели за безбедност на целата компанија, со што има број на квалитети што треба да се исполнат во рамките на кој било план за безбедност, за да бидат изводливи и да покажат позитивно влијание врз корпоративната безбедност.³⁹

а) Мора да биде јасно и видливо: безбедносната политика треба да го користи едноставниот јазик за секоја од заинтересираните страни да ја разбере и да ја почитува таквата политика. Исто така, мора да се постави на видливото место каде што секоја личност на која се однесува може да ја гледа, чита и разбере содржината.

б) Таа мора да ги покаже целите: безбедносната политика мора да ги покаже целите на создавање на таквата политика. Иако прикажувањето на целите мора да ги идентификува заканите што компанијата ги има е изложување на ризик и должноста на секоја личност е да се придржува до тоа. Мора јасно да се демонстрираат безбедносните стратегии и мерки: Политиката треба да ги постави стратегиите и мерките што треба да се преземат за надминување на какви било закани или ризици заради безбедност на персоналот, посетителите, имотот и сл. Безбедносните мерки на компанијата можат да бидат утврдени во полисата како што се

³⁹ Ng Cindy 'how to create a good security Policy' 2018 retrieved from www.veronis.com article posted on 29th March 2018

физичката контрола на чувари, поставеноста на електронските уреди за обезбедување на надзор на објектот, заштитни бариери, огради и сл.

в) Таа мора да содржи услов за усогласеност: политиката треба да ја постави изјавата за усогласеност на секое лице во компанијата вклучувајќи ја и казната за непочитување. Во изјава за усогласеност, политиката да биде строга и да има избегнување каква било толеранција за неисполнувачите безбедносни правила.

г) Мора да се спроведе: политиката треба да биде жива во смисла дека сè во што е во планот за политика мора да биде во состојба да може да се спроведува. Со други зборови, политиката е како закон во рамките на компанијата што ги регулира безбедносните прашања во рамките на компанијата, и како кардинален принцип на кој било закон е дека „секој закон мора да работи во општеството“.

д) Мора да биде релевантна: политиката мора да биде релевантна за природата на деловното работење на конкретниот субјект. Во врска со претходниот дел за проценка на ризик, беше дискутирано дека една од клучните цели на проценка на ризикот во корпоративната безбедност е да се проучи природата на бизнисот и да се идентификува ризикот, потоа да се создаде безбедносна политика и мерки во согласност со идентификуваните ризици. Затоа, политиката мора да ги адресира ризиците идентификувано.

ѓ) Политиката мора да се следи и да се разгледува: секоја безбедносна политика мора да биде во позиција да бидат надгледувани од сите засегнати страни без никакви исклучоци. Мониторингот може често да се проверува за да се обезбеди усогласеност. Исто така, политиката мора да биде прегледана, потоа времињата зависат од промените што се случуваат во корпоративниот субјект, како што се експанзијата бизнис, услуга, раст на базата на вработени, посетители итн., што на друг начин е исто така зголемување или воведување нови ризици во рамките на компанијата.

III ГЛАВА

ПРОЦЕНА НА РИЗИЦИТЕ ВО КОМПАНИИТЕ

ПРОЦЕНА НА РИЗИЦИ ВО КОМПАНИИТЕ

Општо за процените

Постојаниот економски и технолошки развој во општеството и појавувањето на нови компании, довело до потребата за заштита на компаниите и фирмите. Корпоративната безбедност е еден современ пристап кон заштитата на лица, имот како и начинот на работењето на една современа организација.

Импресивната репутација во услугата за клиентите, економските придобивки во рамките на компанијата / корпорацијата, меѓу другото, зависат од ефективната безбедност на персоналот и клиентите воопшто, како и на имотот на корпусот. Сигурноста на клиентите и помага на компанијата да им обезбеди доверба на клиентите кон компанијата, па оттука и проширување на база на клиенти и профит од истата. Сигурната безбедност на средствата од злоупотреба, штети, погрешна примена, и сл. ги намалува трошоците за чести одржувања или замена, па оттука и економската стабилност во рамките на компанијата. За да се обезбедат сите овие, концептот на корпоративна безбедност е од најголемо значење.

Концептот на корпоративна безбедност во компаниите не е само раководно барање, туку е и регулаторно барање. Бројот на закони и регулативи бара од сите компании да имаат солидна и добра безбедносна политика и мерки за осигурување на безбедноста на вработените и надворешните лица, како и на средствата од какви било незаконски активности во рамките на компанијата. На почетокот, финансиските институции, како што се банките и осигурителните компании, биле првите организации кои се фокусирале на ова задолжително барање заради бројни ризици на кои овие институции се изложени, како што се ризик од кражба, вооружен грабеж, перење пари, измами, итн. Сега, барањето за корпоративна безбедност се проширува на секоја компанија. Како одговор, секојакомпанија дизајнира свој оддел за безбедност, којшто се занимава со безбедносните прашања.

Во современото опкружување и современиот свет безбедносните предизвици и секојдневните закани за безбедноста на компаниите во нивното деловно работење се повеќе земаат голем замав во однос на ризиците и заканите кои биле актуелни во минатото. Корпоративната безбедност има за цел да осигура витални вредности и сигурна иднина на една современа компанија во согласност со важечките законски регулативи во државата во која компаниите функционираат и со тоа да се оправда своето место во системот на националната безбедност. Со самото тоа што корпоративната безбедност не може да функционира, потребна е и соодветна функционална рамка па доста битен сегмент која ја представува улогата на приватната безбедност во склопот на националната односно државната безбедност. Често пати се поставува прашањето дали корпоративната безбедност е во согласност и со државната безбедност и државниот безбедносен систем.⁴⁰

Исто така карактеристично е да се каже дека корпоративната безбедност не е само видео надзор во еден маркет тоа е цела плејада на безбедносни системи со кои сега гарантира сигурност на една современа компанија. Од друга страна пак корпоративната безбедност опфаќа и низа анализи на ризици кои можат да настанат и да бидат закана за една современа компанија или современа фирма и како истите ефикасно и ефективно да се надминат и решат. Државниот безбедносен систем гарантира основно ниво на безбедност но условите кои ги гарантира корпоративната безбедност се сложени и имаат за цел целосна заштита на имотот и функционирањето на фирмите или компаниите.⁴¹

Паралелно со ова, мора да се има предвид и фактот дека ризиците и заканите по безбедноста и сигурноста на резидентните компании се зголемени како никогаш до сега. За разлика од порано, како резултат на современите

⁴⁰Huntington, S. Why International Primacy Matters, International Security, 1993

⁴¹Gligoroska, M., (2017), Корпоративна безбедност и државниот безбедносен систем. Факултет за детективи и криминалистика, Европски универзитет - Република Македонија

трендови наметнати од процесот на глобализацијата, претпријатијата се изложени на ризици кои се неминовни и составен дел од концептот и стратегиите за остварување профит. Потребата од имплементација на современи безбедносни технологии и стратегии во таа насока е неминовност од приоритет затоа што ги прогнозираат трендовите на безбедноста, од кои пак зависи и комодитетот на сопствениците на денешните корпорации.⁴²

Безбедносни процени за корпорациите

Без оглед на видот на активноста и големината, обемот на производство и просторно димензионирање и позиционирање на пазарот, деловните организации денес се изложени на ризик од промени на пазарот и неизвесност. Проценка и предвидување на идните резултати на пазарот, без оглед дали се домашни или странски, се неопходен елемент на стратегијата на која било организација. Главните прашања што организацијата мора да ги реши се: како да ги заштити своите деловни активности и позиции во економскиот систем, во тешки економски услови или ако прогнозите на пазарот не се остварат и кои се инструментите за заштита во случај на неизвесни исходи?

Бидејќи ризикот е постојан, организациите се принудени да работат и да преживуваат во услови на ризик, и затоа мора да управуваат со него. Може да се намали, но не може да се елиминира. Управување со ризик најчесто се дефинира како придружна функција на управување каде што сите претприемачки активности се ориентирани кон можни ризици и притоа, тие се испитуваат и контролираат за можно потенцијално мешање, со цел да и се овозможи на компанијата да управува со такви потенцијални пречки и опасности.

Управувањето со ризикот е важно за широк спектар на индустрии, од мали претприемачи до големи компании кои работат низ целиот свет, од организации

⁴² Козарев А., Блажески В., Страторски А., Приватната безбедност во Република Македонија - теоретски и институционален дизајн, Зборник од втора меѓународна научна и стручна конференција во организација на Асоцијацијата за корпоративна безбедност, Скопје, 2016 година, стр. 14-17.

што ги ограничуваат своите активности до нивните сопствени простории до оние што ги извршуваат своите активности на отворено (изградба на тунели, мостови, итн.), од оние што произведуваат безопасни производи до оние кои произведуваат високо токсични или експлозивни производи.

Главната цел на развојот и спроведувањето на проценката на ризикот е да се создадат услови за донесување ефикасни и ефективни одлуки во процесот на заштита на лица, имот и деловно работење на компанијата, но и за донесување стратешки одлуки од страна на раководството на компанијата. Проценката на ризикот е составен дел од процесот на управување со ризик и претставува комплетен процес на идентификување на потенцијалните опасности, анализа и проценка на ризиците.⁴³

Проценка на ризик е израз што се користи за да се опише целокупниот процес или метод што вклучува идентификување, евалуација и утврдување на сите закани (ризичи) и нејзините предизвикувачки фактори и изнаоѓање на решение за отстранување на тие закани пред да се предизвикаат катастрофалните резултати.⁴⁴ Како една од процедурите за корпоративна безбедност, проценката на ризикот вклучува пет термини.

а) Идентификација на ризици: Тоа вклучува процес на наоѓање, наведување и карактеризирање ризици/закани и неговите предизвикувачки фактори пред појавата на катастрофален резултат.

б) Анализа на ризик: Тоа вклучува процес за разбирање на природата на ризиците/заканите и утврдување на нивото на ризик. Анализата на ризикот дава основа за проценка на ризикот и одлуки за контрола на ризик. Информациите можат да вклучуваат тековни и историски податоци, теоретска анализа, информирани мислења и загриженост на засегнатите страни. Анализа на ризик вклучува проценка на ризик.

⁴³ Keković, Zoran i dr., Procena rizika u zaštiti lica, imovine i poslovanja, Centar za analizu rizika i upravljanje krizama, Beograd 2011, strana 105.

⁴⁴ Rausand M 'Risk Assessment: Theory methods and Applications' (2013) John Wiley & Sons

в) Евалуација на ризик: Процес на споредување на проценет ризик со дадени критериуми на ризик за да се утврди значењето на ризикот.

г) Контрола на ризик: Тоа вклучува активности што ги спроведуваат одлуките за проценка на ризик. Контролата на ризик може исто така да вклучуваат следење, проценување и усогласеност со одлуките.

Проценките на ризиците се многу важни бидејќи тие претставуваат составен дел од безбедносната политика на корпорациите. Создаваат свесност за ризикот, идентификуваат кој може да биде изложен на ризик (на пример, вработени, чистачи, посетители, изведувачи, јавност и сл.), утврдуваат дали е потребна програма за контрола за посебен ризик / закана, утврдуваат дали постојните контролни мерки се соодветни или треба да има повеќе направено особено кога е направено во фазата на дизајнирање или планирање, да се даде приоритет на мерките за ризик и контрола и да ги исполнуваат законските барања каде што е применливо. Целта на процесот на проценка на ризикот е да се процени ризикот, потоа да се отстрани тој ризик или да се минимизира нивото на ризикот со додавање на контролни мерки, по потреба. За да се постигне целта, односно правилна проценка на ризикот обидете се да одговорите на следниве прашања:

- што може да се случи и под кои околности?
- кои се можните последици ?
- како веројатно се појавуваат можни последици ?
- дали ризикот се контролира ефикасно или и понатаму се бара акција?

Проценката на ризикот треба да се направи пред да бидат утврдени какви било безбедносни политики или мерки. Проценката на ризик обезбедува како треба да се фокусира безбедносната политика и кои се безбедносните мерки соодветно да се применат за да се спречи и заштити секоја закана. Планирање за проценка на ризик воопшто, е утврдување кој ќе биде опсегот на проценка на ризик, на пр., спецификација на област, обезбедена услуга, големината на персоналот и посетители, физичката област каде што се одвива работната активност, или видови на ризик, како ризик на извршител на опасност, измама,

кражба итн., потребните ресурси (на пример, обука А.) тим на поединци за извршување на проценката, видовите на извори на информации, безбедносни мерки итн.), каков вид мерки за анализа на ризик ќе се користат (на пример, колку е точна скалата или дали параметрите треба да бидат со цел да се обезбеди најрелевантна проценка), кои заинтересирани страни се вклучени (на пример, менаџер, супервизор, работници, претставници на работници, добавувачи, стручни лица од областа на безбедноста итн.), кои се релевантни закони, регулативи, кодови или стандарди кои можат да важат во вашата пресуда или проценка, како и организациони политики и процедури.

Менаџерот за корпоративна безбедност треба да биде надлежен за проценка на ризикот и да направи научна анализа на ваквите ризици. Менаџерот за безбедност мора да ја знае природата на бизнисот во рамките на субјект пред да ја достави проценката. Природата на бизнисот го одредува бројот на ризик во рамките на компанијата, на пример, ризикот во банкарскиот бизнис е прилично различен од ризикот во деловниот субјект на осигурување или деловните компании во трговијата на мало.⁴⁵ Така, службеникот за безбедност има должност да спроведе темелно истражување на деловната активност на компанијата за да му овозможи идентификување, проценка и утврдување на какви било закани по безбедноста. Важно е да се запамети дека проценката мора да ја земе предвид не само моменталната состојба во компанијата, туку и при какви било потенцијални ситуации исто така. Со утврдување на нивото на ризик поврзано со ризикот, на работодавачот, менаџментот и тимот за безбедност (каде што е соодветно), можат да одлучат дали контролната програма е потребна и на кое ниво.

Како би требало да се проценат и анализираат ризиците, зависи од законодавството на државата и регулативите, меѓународни безбедносни стандарди и упатства и практики во рамките на компанијата субјект. Должност е службеникот за безбедност и неговиот тим да ја истражат природата на бизнисот и тогаш да направат усогласување на ваквите наоди од истражувањето во рамките

⁴⁵ Rausand M 'Risk Assessment: Theory methods and Applications'(2013) John Wiley&sons

на регулаторните, меѓународните стандарди и упатства за проценка и анализа на ризиците.

Методологија за безбедносни процени

Иако постојат различни пристапи, а со тоа и поделби, повеќето автори генерално ги разликуваат следните фази во систематскиот процес на управување со ризик:

- 1) Идентификација на потенцијалните опасности
- 2) Анализа на ризик
- 3) Проценка на ризик
- 4) Третман на ризик
- 5) Избор на методи и инструменти за управување со ризик
- 6) Контрола на ризик

Сите овие активности се следат едни со други по логичен редослед и затоа може да се разберат како низа фази во процесот на управување со ризик.

Идентификација на заканите

Деловните субјекти се, како што беше посочено погоре, изложени на различни опасности, од кои секоја на свој начин може да предизвика штета со различен интензитет. Затоа, идентификувањето на изворот на опасност и природата на ризикот и несигурноста, што е поврзано со активноста или појавите што се разгледуваат, е првиот чекор во процесот на проценка на ризикот. Важен аспект на процесот на идентификација е да се разгледа изложеноста на ризици, т.е. потенцијални опасности, а со тоа и на штетите поврзани со одреден вид ризик, во следните категории: физички средства, финансиски ресурси, човечки ресурси и одговорности. Компанијата треба поблиску да ги обележи или идентификува потенцијалните опасности, фактори на ризик, настани, како и нивните потенцијални последици, со цел да состави сеопфатен список или каталог на опасностикоишто може да резултира со негативни последици.

Не постои единствен метод или техника за идентификување на ризиците, бидејќи секој од нив има одредени слабости. Изборот на методот зависи од природата на бизнисот со кој се занимава компанијата, делокругот на деловната активност и експертите кои компанијата ги вработува за да се занимаваат со овој бизнис.

Идентификација на ризик значи препознавање на надворешни и внатрешни фактори за деловната активност на деловната организација. Надворешните фактори се многубројни. Како што расте големината на компанијата, така расте и списокот на потенцијални ризици. Најголемо влијание има работењето на пазарот и технолошкиот процес. Внатрешните фактори се одраз на: стратегијата и организацијата на компанијата, планирањето и управувањето, менаџерските вештини и деловната ефикасност.⁴⁶ Откако ќе се идентификува што може да се случи, потребно е да се земат предвид причините што покажуваат какви можат да бидат последиците. Следниот чекор е да се создаде матрица на ризик што јасно ја покажува изложеноста на организацијата и нејзините клучни вредности и потенцијални ефекти врз организацијата како целина или кон индивидуалните заштитени вредности.

Ефективност од корпоративната безбедност во компаниите

Корпоративната безбедност мора да содржи број на квалитети за да биде обезбедена. Следно се дадени вообичаени квалитети за управување со компанија со цел до ефетивна безбедност:

- Стратешки и оперативни квалитети

Ефективната корпоративна безбедност мора да ги утврди стратегиите за тоа како вработените, клиентите и средствата ќе бидат обезбедени за нивна поддршка. Тие стратегии мора да бидат способни да бидат управувани. Безбедносниот тим мора да ги дизајнира безбедносните стратегии што можат да

⁴⁶Šabović, Šerif, Upravljanje rizikom u uslovima krize, u Zborniku radova „Menadžment 2010“, Kruševac, 2010, strana 478.

работат во рамките на компанијата и може да донесе добар резултат како што е планирано.⁴⁷

- Содржи јасна безбедносна политика и безбедносни мерки

Ефективната корпоративна безбедност има јасни безбедносни политики и мерки.⁴⁸ Безбедносната политика предвидува обезбедување содржина, целта на таквото обезбедување содржина, безбедносни мерки и правила што треба да се следат кон тие мерки, исто така, безбедносната политика предвидува должности на секое лице во компанијата за почитување на тие правила на безбедност и казна за не усогласеност на правилата за безбедност. Корпоративната безбедност мора да има безбедносни мерки и системи и за физичката и за безбедноста на информациите, како што е безбедноста на електронски надзор на системи/уреди, безбедносни уреди за контрола на пристап, чувари итн.

- Способност за превенција и заштита

Примарната цел на корпоративната безбедност е да ги спречи и заштити луѓето и средствата на компанијата, ако оваа цел не се постигне, тогаш значењето да се има корпоративната безбедност не е ништо. И безбедносните политики и мерки/системи мора да бидат во состојба да спречат веројатен ризик од катастрофални дела, откривање на извршување на недозволени дела и одговори кон извршените дела.

Форми на корпоративна безбедност

Долго време физичката безбедност беше вообичаена форма на корпоративно обезбедување, но поради развој и наука и технологии, како и појава на експерти за модерна безбедност, се појавува нова форма што е безбедноста на информациите.

- Физичка безбедност

⁴⁷ White G 'strategic, tactical and operational security management model' (2006) texas state university, US

⁴⁸ Briggs R and Edwards C 'The Business Resilience: corporate security for the 21th century'(2006) upstream,London uk

Оваа форма на корпоративна безбедност ги опишува безбедносните мерки што се дизајнирани да ги негираат неовластените пристапи до објекти, опрема и ресурси и да се заштити персоналот и имотот од оштетување или штета (како што се кражба, шпионажа, терористички напади итн.). Физичкото обезбедување вклучува употреба на повеќе слоеви на меѓузависни системи кои вклучуваат електронски уреди за набљудување, како што се камери за кружни телевизии (CCTV), чувари, заштитни бариери, брави, протоколи за контрола на пристап и сл.

Системите за физичка безбедност за заштитени објекти ги имаат следниве цели:

а) Одвраќање: тие дејствуваат како да ги негираат потенцијалните натрапници од напад или извршување на незаконски дела. Целта на одвраќање е да се убеди потенцијалниот натрапник или напаѓач дека успешниот напад е поради немање на силна одбрана. Оние системи за одвраќање на безбедноста вклучуваат предупредувачко испуштање на звук, заштитни бариери и огради, периметарски ознаки итн.

б) Откривање: Постојат системи за физичка безбедност кои имаат намера да ја откријат прогресијата на извршување на актите или откривање на упадите. Овие системи вклучуваат видео надзор како камери, аларми за натрапници итн.

в) Одговор: Системите за физичка безбедност имаат за цел да одговорат на ситуацијата. Тука спаѓаат на пример, обезбедувањето и полицијата.⁴⁹

На безбедносните дизајнери, архитекти и аналитичари им останува да ги балансираат безбедносните контроли против ризици, земајќи ги предвид трошоците за специфицирање, развој, тестирање, спроведување, користење, управување, следење и одржување на контролите заедно со пошироки прашања

⁴⁹ United States Department of Army 'Physical security challenges' chapter one (2013)

како што се човечки права, здравје и безбедност и општествени норми или конвенции.⁵⁰

Корпорациска безбедност во областа на информатичката заштита

Безбедност на информации

Безбедноста на информациите, InfoSec, е практика на спречување на неовластен пристап, употреба, откривање, нарушување, модификација, проверка, евидентирање или уништување на информации. Информациите или податоците може да имаат каква било форма, на пр. електронски или физички. Примарен фокус на безбедноста е балансираната заштита на доверливоста, интегритетот и достапноста на податоците, задржувајќи фокус на ефикасно спроведување на политиките, сето тоа без попречување на продуктивноста на организацијата.⁵¹ Ова во голема мерка се постигнува преку повеќестепен ризик, процес на управување што ги идентификува средствата, изворите на заканите, ранливоста, потенцијалните влијанија и можните контроли, проследени со проценка на ефективноста на планот за управување со ризици.

Што се однесува до проширувањето на науката и технологиите, повеќето информации се чуваат во електронска форма на уреди, како што се компјутерски сервери, е-пошта, дискови итн., исто така, информациите за клиентите се складираани по електронски пат. Овој развој го воведува новото кривично дело сајбер-хакерство, сајбер кражба, шпионажа, штета од злонамерни податоци итн., кражба и уништување на доверливите и криминални информации. Како резултат, корпоративна безбедност освен што се фокусира на физичката безбедност, се фокусира и на безбедноста на информациите кои имаат потреба од различен вид експерти во информатичката технологија (ИТ).

Компаниите за да обезбедат ефективна употреба на корпоративна безбедност на информации треба да дизајнираат сајбер безбедносна единица во која се вклучени

⁵⁰ Lynn M and Garcia 'design and evaluation of physical protection system' (2007) butterworth-Heinemann, UK

⁵¹ Andress J 'The Basics of Information security: understanding the fundamentals of infosec in theory and practice' (2014) 2nd Ed Elsevier Science Publisher

ИТ експерти. Овој информатички персонал има должност да ја дизајнира сајбер безбедносната политика и мерки за да се обезбеди дали дигитализираните податоци се добро обезбедени. Персоналот за ИТ користи број на технички системи за надминување на сајбер заканите кои вклучуваат поставување на сигурна лозинка, антивирусен софтвер, заштитен сид, софтвер за криптирање, правила за правна одговорност и стандарди за обука на корисници/администратори.

Сепак, имплементација на какви било стандарди и упатства за безбедност на информациите во рамките на компанијата може да има ограничен ефект доколку не се усвои култура на постојано подобрување. Оваа форма на безбедност е поскапа бидејќи вклучува скапи технологии и претежно компанијата бара да ги вработи специјализираните ИТ компании за формулирање на компјутерски системи за одржување на безбедноста на информациите.

Теорија на информатичко војување

Спектарот на прашања за информатичката заштита е толку широк што ги допира и прашањата за националната безбедност. Како појдовна основа во дефинирање на основните поими од оваа област, се применува теоријата на информатичко војување. Примат за современата теорија и практика на информатичката заштита имаат САД. Во Стратегијата на националната безбедност на САД од 2002 година, наведено е дека четирите основни столба на меѓународната моќ на таа земја се дипломатската, воената, економската и информатичката моќ.⁵² Една од причините за масовно користење на информатичката сфера како оружје во современата ера е фактот дека модерните достигнувања во областа на техниката, медиумите и комуникациите станале достапни и за неразвиените земји. Тие нови околности придонесуваат кон можноста за изедначување на конкурентноста на појаки и на послаби земји во меѓусебното натпреварување, што може да доведе до поништување на воениот

⁵² The National Security Strategy of the United States of America, President of the United States, Washington DC, September 2002., p.14.

принцип, решени на маса, односно до тоа воената моќ повеќе да не е пресудна во одмерување на силите помеѓу две или повеќе држави. Оружјата на информатичката ера им помагаат на малите држави против големите и ги фаворизираат слабите во однос на силните. На наведеното укажуваат и т.н. Сајбер напади на неформални групи врз значајните воени и индустриски информатички системи на моќните држави како САД, Велика Британија и Германија. Од тие причини, на прагот во новата информатичка ера осмислувањето на правилната национална стратегија за безбедност може да има големо влијание за конечниот резултат на современите конфликти.⁵³

Корпоративна безбедносна структура

Во дефинирањето на соодветно ниво на корпоративната безбедност неопходно е претходно да се утврдат и да се формулираат следните елементи:

- Актуелни разлики, причини и облици на загрозување лица, имот и работењето на корпорацијата кои треба да се очекуваат во идниот период;
- Прецизирање на надлежностите и овластувањата на лицата кои работат во компанијата на работи околу заштита на нејзините витални вредности и утврдување на состојбата на нивната стручност и мотивираност;
- Организација и дејствување на физичко-техничкото обезбедување на сите објекти кои и припаѓаат на компанијата;
- Мерки за заштита поврзани за безбедноста и здравјето, заштита на животната средина, заштита од пожари, хаварии и експлозии;
- Мерки за заштита на работењето на корпорацијата од сите облици на корупција, различни видови злоупотреба, проневери, измами и други методи на отуѓување и присвојување на нејзиниот имот;
- Прецизирање на мерките на заштита на деловна и на службена тајна;
- Конкретизирање на мерките во однос на контрола на движењето и престојувањето на надворешни лица во објектите и на просторот кој припаѓа на деловниот субјект;

⁵³ Миљковиќ Милан, “Информационо ретовање у савременој теорији и пракси”, Војно дело, Министерство одбране Републике Србије, Београд, лето 2010., стр 258-259.

- Организација и функционирање на информациските системи и обезбедување на лицата, имотот и работењето на корпорацијата, особено на мерките за заштита на информациите;
- Хармонизација на нормативните акти во сите сегменти на безбедноста, со националните прописи и стандарди на ЕУ;
- Оцена на степенот на загрозеност на лицата кои во корпорацијата извршуваат работи поврзани со заштита на нејзините витални вредности.⁵⁴

Начела на функционирање и развој на системот на корпоратиска безбедност

Корпоратиската безбедност се развива преку воспоставен систем, според следниве начела:

- Единственост (сите елементи и актери на системот на корпоратиско ниво и во делови на компаниите се развиваат според истите начела, функционално се поврзани и обединети во извршната функција на ниво на корпорацијата со почитување на субординацијата и обврската на спроведување на налогот на повисокото ниво на одлучување);
- Рационалност (вклучување во функција на безбедноста на сите расположливи човечки, материјални и организациски ресурси на компанијата, формирање на оперативни и високостручни служби за безбедносни работи кои ефикасно ќе го планираат, ќе го насочуваат, ќе го усогласуваат, ќе го следат и ќе го контролираат функционирањето на сите сегменти на системот);
- Сеопфатност (органizaциско и функционално уредување кое ќе овозможи ефикасно отстранување на последиците од сите проценети реални извори и облици на загрозување и истовремено ангажирање во повеќе правци за да се остварат најдобрите ефекти);
- Селективност (прецизно и концизно дефинирање, делегирање и дистрибуција на елементите на системот на корпоратиска безбедност);

⁵⁴ Barney Jay, Hesterly S. William, Strategic Management and Competitive Advantage, Prentice Hall, London 2005., pp. 432-435.

- Приспособливост (можност за брзо и за ефикасно пренесување на тежиштето на дејствување на актерите и прераспоредување на елементите на системот на безбедност во согласност со промената на условите на дејствување, изворите и облиците на загрозување);
- Доверливост (способност на системот да биде во постојана функционална состојба независно од чија било поединечна желба и способност да ги стимулира актерите на пожелно и пропишано однесување).⁵⁵

Имајќи ја предвид значајноста на корпоративската безбедност за остварување на стратегиските цели на компанијата, организациската единица која ќе ги извршува тие работи треба да се престрои така да поседува јасни одговорности и прецизни овластувања во исполнување на своите основни задачи. Ако се работи за корпорација со голем број вработени, или компанија која работи на различни локации, тоа треба да биде организациска единица на прво ниво на поделбата на работите. Во малите компании, потребно е да се воспостави одбор за безбедност или да се именува менаџер за безбедност кој ќе биде непосредно одговорен за врвниот менаџмент. Во случај тоа да не е економски исплатливо, еден од врвните менаџери на компанијата мора да ја преземе улогата на менаџер за безбедност.⁵⁶

Во врска со тоа, треба да се потенцира дека во стандардната организација овие работи, во согласност со насоките од ЕУ, во големите корпорации се користи поимот интегрална безбедност, кој понатаму се расчленува на работи на безбедност (security), заштита (safety) на работата, заштита од пожари, заштита на околината. Ако тие работи се групираат во една организациска единица, компанијата добива рационална и ефикасна организација со воспоставена координација и контрола над сите работи врзани со безбедноста.⁵⁷

⁵⁵ Chief Security Officer Guidelines (GDL CSO 06 2004), ASIS International Commission on Guidelines, Alexandria VA 2006., pp 6-7.

⁵⁶ Ivanovic Vidovic Darija, Karlovic Lidija, Ostojic Alen, op. Cit. str. 68.

⁵⁷ Banner K. David, Designing Effective Organizations: Traditional & Transformational Views, SAGE Publications, Thousand oAKS ca 1995., p. 320.

Активности на организациските единици за корпоративна безбедност

Организациската структура на секторот за безбедност во корпорациите е симбиоза од човечки и од материјални ресурси, така што на оптимален начин придонесува за успешна реализација на своите задачи. Каква организациска структура на секторот за безбедност во корпорацијата ќе биде избрана зависи од редица фактори, при што основниот критериум е успешно реализирање на стратегијата или конечната цел на корпоративната безбедност. Во врска со тоа, потребно е најнапред да се анализираат расположливите начини на организирање на секторот на безбедност во корпорациите или модели на формирање на организациските структури. Британскиот теоритичар Маси го застапува ставот дека ефективната примена на стратегијата бара од менаџерите да разработуваат бројни клучни влијанија, додека лидерот има улога да одреди како ќе ја структурира организацијата за реализација на стратегијата и како треба да управува со луѓето и со средствата за да се реализираат дефинираните организациски планови.⁵⁸

Управите на корпорацијата при идентификувањето и при дефинирањето на елементите на организациската структура на секторот за корпоративна безбедност се соочуваат со четири основни прашања: “Кои делови од секторот за безбедност треба да бидат организациски единици?”, “Кои работи од безбедноста треба да се групираат, а кои да се раздвојат?”, “Која големина и облик одговара на различните организациски единици во секторот за безбедност?”, “Како да се распоредат безбедносните менаџери и службеници и како меѓусебно да се поврзат различните организациски единици?”. На овие прашања не постојат однапред дадени одговори, но врз основа на определени принципи, критериуми, методи и правила во секој конкретен случај може да се дефинира ефективната организациска структура. За да може да се дојде до неа, потребно е да се анализираат: клучните активности кои се очекуваат од секторот за безбедност во корпорациите и нивните цели; придонес кон постигнување на потребната состојба на корпоративната

⁵⁸ Massie L. Joseph, *Essential of Management*, Prentice Hall International, London 1987., pp. 41-42.

безбедност; активности за произведување мерливи резултати; активности за поддршка и општи работи, т.е. Правење рационална анализа заради утврдување на позицијата на поединечните компоненти на секторот безбедност.

Според мислењето на Т. Веиќ, организациската единица за корпоративна безбедност по правило треба да биде поспоставена како интерна служба за корпорацијата да работи на безбедност и заштита, а евентуално може да биде и професионална агенција која постапува според плановите на менаџерот за безбедност на компанијата. Работите на таа единица треба да ги опфатат следните активности:

а) Собирање информации и проценка на ризикот.

Единицата за корпоративна безбедност е одговорна за собирање на релевантни информации од областа на безбедноста и заштитата, коишто можат битно да влијаат на безбедноста и заштитата на вработените, на странките, на регулацијата и на конкурентноста на работната организација. Врз основа на вака собраните податоци потребно е да се направи проценка на ризикот.

б) Подготовките на организацијата за вонредни состојби.

Единицата за корпоративна безбедност одговорна е и за подготвеноста на организацијата да се заштити во случаи на големи измами, напади, катастрофални случувања, минирање на производството од страна на конкурентните фирми или поединци и сл. Во таа смисла, постојано треба да се контролираат безбедносните мерки и планови и да се обучуваат вработените.

в) Обезбедување и заштита на виталните интереси на организацијата.

Обезбедување на интегритетот на организацијата, вработените, процесите и недвижностите од штети и загуби, исто така, е една од клучните одговорности на единицата за корпоративна безбедност. Притоа, оваа единица ги штити недвижностите и финансиите на организацијата, но и на интелектуалната сопственост, трговската марка, регулацијата, службените тајни (договори и сл.) итн.

г) Превенција на инцидентни состојби.

Клучната одговорност е анализа на информациите и во државните институции за да се предвидат можните напади врз организацијата, односно како да се направат превентивните процедури. Во таа смисла, единицата за корпоративска безбедност мора да биде во состојба да ги разбере конкретните извори на безбедносните проблеми и да изнајде адекватни решенија за нивно отстранување.

д) Реагирање и управување со инцидентни состојби и санирање на последиците.

Единицата за корпоративска безбедност мора да посвети максимално внимание за враќање на организацијата во нормална работна состојба по инцидентни и акцидентни состојби. Таквото враќање на организацијата во нормална состојба мора да се координира со надлежните институции (полиција, војска, итна помош. итн.).⁵⁹

Штетни влијанија на информатичката инфраструктура

Информатичката инфраструктура може да биде изложена на штетни влијанија од различна природа кои директно или индиректно можат да ја загрозат нејзината функционалност. Тие влијанија можат да се класификуваат на: дефекти, инциденти и напади.⁶⁰

Дефектите се потенцијално штетни настани, предизвикани од внатрешни дефекти на системот или дефекти на надворешните елементи неопходни за негово функционирање. Тие можат да бидат и како последици на грешки при самото проектирање на софтверот, дефекти на хардверот, човечки грешки и др. Категоријата на инциденти ги вклучува сите случајни настани како што се

⁵⁹ Veic Tomislav, "Korporativna sigurnost", Posta, godiste II, broj 3, Zagreb, veljaca 2007, str. 41-42.

⁶⁰ Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R., Survivable Network Systems: An Emerging Discipline, Technical Report

природните непогоди и катастрофи. За разлика од дефектите, инцидентите се настани чии причини се наоѓаат надвор од системот.⁶¹

Нападот на информатичкиот систем може да се дефинира како директна акција против мрежата или информатичкиот систем со цел неовластено да се пресретне или да се прекине некоја операција, да се преземе контрола и да се уништи, да се промени или да се корумпира податокот (со меморирање или обработка). Според некои автори, можат да се разликуваат три видови на напади на информатичкиот систем:

- Физички напад, насочен кон расположливоста на нападнатиот систем (употреба на конвенционални оружја против инфраструктурата во која се наоѓаат информатичките системи или против линијата на преносот на информацијата);
- Електронски напад (користење енергетско оружје кое е во можност да емитува електромагнетна енергија концентрирана во снопови со автоматски или субавтоматски честички или оружје кое испушта електромагнетни импулси со цел да се преоптоварат или да се онеспособат електричните споеви на системот);
- Сајбер напад (примена на т.н. Злонамерни информатички програми чија задача е да го заразат информатичкиот систем на противникот со цел негово оштетување или крадење на различни доверливи или чувствителни податоци).⁶²

⁶¹ Stallings William, Network and Internetwork Security - Principles and Practice, Practice Hall, Englewood Cliffs, New Jersey 1995., pp. 29-30.

⁶² Петкович Тодор, оп. Цит. Стр. 293

IV ГЛАВА

СОВРЕМЕНИ БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ ВО

КОМПАНИИТЕ

СОВРЕМЕНИ БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ ВО КОМПАНИИТЕ

Безбедносните предизвици со кои се соочува светот денес се далеку посложени и меѓусебно поврзани отколку во кој било момент од нашата историја. Доказите сугерираат дека бидејќи меѓугрупниот и меѓучовечкиот конфликт започнал да се повлекува, се појавува соодветна ескалација на други, помалку разбрани познати закани, вклучувајќи ги заканите за природните, економските и социјалните развиени системи од кои зависи општеството.

Многубројни истражувања убедливо тврдат дека меѓугрупното и меѓучовечкото насилство експоненцијално опаднало од ерата на просветителството, достигнувајќи историски најниско ниво на крајот на дваесет и првиот век. И покрај извештаите за заканата од исламски тероризам, урбани убиства и други видови насилство, систематската анализа на податоците за стапката на насилство со текот на времето сугерира дека денес можеби живееме во најмирољубивата ера од постоењето на нашиот вид.

На меѓународно ниво, општеството станува сè поефикасно во својата посветеност на мировните операции од 1980-тите и доделува поголеми ресурси на мировните иницијативи. Покрај тоа, според едно истражување, присуството на мировници во општеството кое преминува од конфликт го намалило ризикот од повторна ескалација на меѓугрупниот конфликт за 80 проценти. Прво, силните мировни сили можат директно да одговорат на насилството од страна на нарушен режим. Второ, процесот на олеснување на договорот преку присуство на меѓународни сили може да дејствува за смирување на недржавните актери со доделување признание за политички лидери. Напредокот идентификуван во овие проценки, сепак, е барем делумно ублажен со појавата на значајни граѓански конфликти на Блискиот исток во последните пет до десет години.⁶³

⁶³ Fortna, V. P.: Does Peacekeeping Work? Shaping Belligerents' Choices after Civil War. Princeton University Press, Princeton, NJ (2008)

Најимпресивниот напор за контрола на насилството во последните 70 години е успехот на светот во избегнување на егзистенцијална закана од нуклеарна војна меѓу големите сили. Ова достигнување е постигнато со развојот на меѓународни и билатерални договори кои значително го намалија ризикот од голема нуклеарна војна.⁶⁴

Овие извонредни намалувања на меѓучовечкото и меѓугрупното насилство се препишуваат на низа паралелни случувања. Како што тврди Пинкер, пет големи настани им помогнале на општествата да станат помалку насилни. Тие вклучуваат развој на Левијатанска држава, поседување судство за легитимна употреба на сила и норми и институции што им овозможуваат на општествата да го смират искушението за експлоатационите напади, да ги инхибираат импулсите за одмазда и да ги заобиколат пристрасностите од конфликти. Појавата на трговијата како технолошки напредок сè повеќе ја поддржувала размената на стоки и идеи на подолги растојанија и меѓу поголемите групи трговски партнери. Развојот на културните норми кои ги почитуваат интересите и вредностите на жените и ги поттикнуваат жените им помогнало на општествата да се оддалечат од величењето на насилството. Зголемувањето на космополитизмот преку писменост, мобилност и масовни медиуми ги поттикнало луѓето да ја прошират перспективата на луѓето. Покрај тоа, засилената примена на знаењето и рационалноста во човечките работи може им помогнало на луѓето да ја препознаат бескорисноста на циклусите на насилство, да ги намалат привилегирањата на нивните интереси над другите, преформулирајќи го насилството како проблем што треба да се реши наместо натпревар што ќе се победи.⁶⁵

Од теоретска перцепција, развојот на настаните идентификувани од Пинкер и другите може да се смета како општества што развиваат множества на институционализирани точки, кои тој ги опишува како „фокусна точка за

⁶⁴ Hough, P.: Understanding Global Security, 3rd Edition. Routledge, New York (2013)

⁶⁵ Pinker, S.: The Better Angels of our Nature: Why Violence has Declined. Penguin, New York, NY (2011)

очекувањата на секоја личност за тоа што другиот очекува од него да направи “.⁶⁶ Тука се повикуваме на општествени вредности, норми, договори, закони и институции како фокусни точки кои дејствуваат како што е договорено и често се применуваат водичи за многу сложени и опасни интеракции. Овие институционализирани патокази обезбедуваат механизми за решавање на насилството и конфликтите, бидејќи општествата ги прифатиле до крајот на 20 век. Сепак, ова не се едноставно лекции од минатото, ниту пак оваа дискусија е ограничена на дијалог за конфликт и насилство. Како што се појавуваат нови закани, без оглед дали се од областа на конфликт, економија, природни / еколошки системи или пошироко, општеството може да учи од овие минати успеси и да развива и спроведува нови фокусни точки (на пр. вредности, закони, институции) за да се спротивстави на новите растечки закани.

Општо за заканите

Заканата за која секогаш постои, голема е веројатноста дека ќе се случи и ќе предизвика сериозни последици по корпорацијата. Заканата е несаканиот, намерен или ненамерен момент кој може да предизвика повреда врз одреден или посочен субјект. Заканата најчесто ја користи ранливоста против кого е насочена. Главните заканувачки аспекти од заканите кон корпорациите е прекин на производството на компанијата, огромни пречки во деловниот процес, нивото на нивната инфилтрација во економијата и општеството.

Во последните 20 години или приближно, меѓу компаниите има сè поголемо признание за стратешкото значење на безбедноста; според едно истражување од 2004 година, 97 проценти од испитаниците изјавиле дека безбедноста ги загрижува, и 57 проценти очекувале да потрошат повеќе на зајакнување на безбедноста во наредните години. Компаниите, се чини дека го ценат безбедносниот придонес што може да го направи за целокупните деловни проблеми. На прашањето во истото истражување дали ефективното управување со

⁶⁶Pinker, S.: The Better Angels of our Nature: Why Violence has Declined. Penguin, New York, NY (2011)

безбедноста ќе донесе придобивки за голем број основни цели, анкетата покажала дека безбедносниот капацитет на компанијата е се повеќе важна за инвеститорите: 87 проценти од инвеститорите сметале дека ако компанијата не успее да се справи со безбедносен инцидент брзо и ефикасно, тоа би ја променило нивната перцепција за таа компанија; а во случај на нарушување на безбедноста, 61 процент сметале дека ќе има влијание врз корпоративниот бренд или углед.⁶⁷

11.09 и новиот бренд на „глобален тероризам“го смениле профилот на ризик кај големите мултинационални компании. Променливата природа на заканата и режимот на работа - цивилни наместо воени цели, желба за масовност на жртви, можност за биолошки или хемиски напади, насочување на сите работи „западно“ и признавање на вредноста на политичката повреда на една земја преку нејзината економија - ги прават компаниите поатрактивни директни цели или колатерални штети. Бомбардирањето во Истанбул во 2003 година и нападите на Блискиот исток и југоисточна Азија го истакнуваат овој тренд.

Донекаде стана клише да се каже дека 11 септември се сменило сè, но тоа претставувало важна пресвртна точка во корпоративната безбедност на глобално ниво. Тероризмот можеби не е најважниот ризик со кој се соочуваат компаниите, но, 11.09. како настан создаде „момент“ кој бил шок за корпоративниот систем, кој ги насочил умовите, и ги натерал одборите да поставуваат прашања како се одвива нивната безбедност.

Облици на загрозување на корпорациите

Постојат бројни форми и модалитети на загрозување на имотот на компанијата. За потсетување, имотот на компанијата како што се инфраструктурни објекти, производствени капацитети, опрема, стоки, готови производи, сировините и слично може да бидат изложени на природни фактори,

⁶⁷Business Security Survey 2004, MORI, IPSOS and the Confederation of British Industry (CBI) in association with QinetiQ.

како што се поплави, пожари, земјотреси или на ефектите од технички фактори, како што се несреќи, дефекти или едноставно технички непогоди.

- Природа - Секаков број природни катастрофи може да влијаат на системите за поддршка на кои се потпира информацискиот систем на една организација. Ако заканата е природна закана, како што се бури или поплави, земјотреси тогаш „природата“ може да се смета како облик на загрозување на корпорациите
- Вработени - Организациите му доверуваат на својот персонал да ги извршува своите должности точно и во согласност со политиките на организацијата. Голема закана за организациите е заканата дека вработениот може да направи критична грешка при внесување на податоци, да објави комерцијални податоци или да одлучи да ја измами организацијата.
- Злонамерни хакери - Информациони системи кои се поврзани со други системи или Интернет, се изложуваат на милиони потенцијални хакери. Дури и оние системи кои не обезбедуваат јавен интерфејс, како што е Интернет, сè уште се изложени на хакери преку социјален инженеринг, модем врски или физички напади.
- Индустриски шпиони - Вредноста на комерцијалните информации за конкуренцијата не треба да се потценува. Индустриската шпионажа е значителна закана за повеќето организации и може да резултира со губење на профит, конкурентска предност, па дури и на самиот бизнис.
- Шпиони на странски влади - Странски шпиони би можеле да вршат шпионажа со цел унапредување на можностите на странска влада, ограничување на способностите на националната влада или дури може да вклучуваат и индустриска шпионажа спонзорирана од странство.

Закани предизвикани од антропогени појави

Антропогени закани и ризици

Генерално антропогените закани и ризици се појави кои ја загрозуваат критичната инфраструктура, а тоа се дела кои се поврзуваат со тероризам, криминал и саботажи кои се наменети за да предизвикаат застој во функционирањето на целокупната или само некои делови од критичната инфраструктура. Под критична инфраструктура подразбираме огромен или глобален сектор. Зависно од ова, неможе да се постигне комплетна заштита на сите места подеднакво и во секое време. Во однос на овие закани веројатноста да се случат терористички напади врз критичната инфраструктура е се поголема. Иделогитата на терористите повеќето автори ја дефинираат како цел да шират паника и вознемиреност, страв, се со цел да креираат перцепција дека секое население и главна гранка во инфраструктурата на земјата/државата се таргет група и посакани за напад. Вакви случаи се случиле на 22 март 2016 година, кога оперативци на ИСИЛ извршиле напади во Брисел на аеродромот „Завенгем“ (убиени 11 лица) и во метрото „Мајлбег“ (убиени 20 лица).⁶⁸ Терористичката организација „Ал-каеда“ по извршените напади на нафтените компании во Ирак, Алжир, Кувајт, Саудиска Арабија, Пакистан и Јемен се здобила со големи заработки од нафтените полиња. Со овие напади ООН проценуваат дека ИСИЛ во 2015 година од нафтените полиња генерирала приходи во износ од 400 до 500 милиони долари.⁶⁹ Повеќето автори даваат акцент на енергијата од нафта и гас кои привлекуваат голем интерес на терористички напади.⁷⁰

⁶⁸ 8 United Nations Security Council Counter-Terrorism Committee (2017) Physical Protection of Critical Infrastructure against Terrorist Attacks, <https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTEDTrends-Report-8-March-2017-Final.pdf>, стр.3-4 (цитирано 19 мај 2021 год)

⁶⁹ United Nations Security Council (2016) Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/92, (цитирано 19 мај 2021 година)

⁷⁰ Brookings Doha Center Analysis (2016) Risky Routes: Energy Transit in the Middle East, <https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf>, (цитирано 19 мај 2021).

Следна позначајна антрополошка закана е дејствието на саботажата, која е граничната линија помеѓу терористичкиот чин и кривичното дело, и секој начин на извршување треба посебно да се анализира. Главните закани за критичните инфраструктури се саботажите и терористичките напади. Најчесто овие напади ги таргетираат инфраструктурите како што се транспортните мрежи, телекомуникациските мрежи, производствените капацитети на енергија, мрежите за снабдување со вода и храна и итн.

Најчесто дејствијата на саботажите се извршуваат преку подметнување на пожар, употреба на оружје, направи за предизвикување експлозии и разни сајбер-напади. Сајбер нападите најчесто доаѓаат и од државните структури во различни форми од : платени терористи, поеди групи кои дејствуваат во корист на државата, странски разузнавачки агенции.

Ваквиот тип на непријателски напади се имплементираат со различни типови на техники и начини за воспоставување на сајбер-нападот. Развојот на технологиите носи нови предизвици за заштита и откривање од сајбер-нападите. Најчесто акцентот на напаѓачите кои дејствуваат преку интернет се става на хакерите или на терористичките групи, а се занемарува од можните или потенцијални напади од државните актери. Операциите околу шпионажа, агенциите за разузнавање ги реализираат преку интернет, што е релативно лесен начин со низок ризик за да се добијат саканите класифицирани или други сензитивни информации. Таргет цели на ваквите напади се високотехнолошките индустрии кои се од големо значење за државата, тука спаѓаат индустриите за нафта и гас, телекомуникациската област, фармацевската индустрија, области со природни ресурси, како и образовните области кои се занимаваат со истражување и развој.

Нападите кои на еден начин се спонзорирани од државните структури добиените информации ги употребуваат за да им дадат конкурентска предност на домашните фирми. Државните актери кои користат сајбер-напади познато е дека користејќи го овој механизам, е начин за да предизвикаат нестабилност во политичките и економските активности како инструмент за влијание врз владините одлуки. Заканите сајбер-саботажа, сајбер-операции, сајбер-шпиунажа и

други типови закани се сериозен предизвик во поширока смисла врз економијата и останатите клучни сектори од критичната инфраструктура.⁷¹

Криминалните дејствувања врз критичната инфраструктура се делат на внатрешни и надворешни. Внатрешните закани се манифестираат внатре во секоја организација и се неминовен дел од истата. Во целост, вработениот злоупотребувајќи ја својата позиција ги извршува саботажите и шпионажата против својот работодавец. Овие намерни дејства можат да се манифестираат и како кражби или суптилни начини на саботажа или насилство на работното место. Инсајдерите своите закани ги остваруваат преку злоупотреба на ИТ-мрежата, која често предизвикува конфузија поврзана со сериозноста на заканата.⁷²

Надворешните закани делумно ги опишавме и се манифестираат преку различни начини на инфилтрирање во системот, физички или користејќи ги информациските технологии, а мотивот за ваквиот тип на закана секогаш зависи од поводот на напаѓачот.

Физичките напади претставуваат обид за присвојување на опрема или придобивање на битни информации преку директна соработка со вработените во фирмите или преку одреден начин на изнуда или интрига. Со ваквиот однос на напади, се почести и посериозни упади се случуваат во сајбер просторот. Ваквите типови на напади врз критичната инфраструктура се случуваат секојдневно на глобално ниво и од овој аспект трендот на нападите се зголемува. Овој вид на опасност по сајбер-просторот и критичната инфраструктура е предизвик за безбедносните структури. Ги носи во подлабоки размислувања на кој начин најсоодветно да ги заштитат виталните делови од критичната инфраструктура од надворешните упади.

Ваквата силна поврзаност помеѓу критичната инфраструктура и интернетот доаѓа да на цена на зголемена сложеност и како последица од ваквите закани да се зголеми и ризикот од случајни грешки.

⁷¹ Canadian Security Intelligence Service (2017) Cybersecurity and Critical Infrastructure Protection, <https://www.csis.gc.ca/ththrtvnmnt/nfrmtn/index-en.php>, (цитирано 20мај 2021).

⁷² Thomas Noonan and Edmund Archuleta (2008) The Insider Threat to Critical Infrastructures, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, (цитирано 20мај 2021).

Закани предизвикани од асиметрични закани

И покрај минатите достигнувања во решавањето на конфликтите, се појавуваат брзи технолошки достигнувања кои можат значително да ги надминат способностите на утврдените општествени вредности, норми, закони и институции за намалување или дури и контрола на насилниот судир. Џ. Клапер, поранешниот директор на Националното разузнавање на САД во своето сведочење пред Комитетот за вооружени служби на Сенатот за проценка на заканите низ целиот свет, истакнал како технолошкиот напредок може да ги доведе во опасност основните елементи на нашето општество, како што се сајбер инфраструктура, финансиски услуги, здравствени системи, системи за транспорт, итн. и повеќе меѓусебно поврзани и исто така зависни од разузнавачки уреди кои се потенцијално „подложни на низа нарушувачки и измамнички тактики што може тешко да се предвидат или брзо да се разберат“.⁷³

Заедно, технолошкиот напредок во компјутерската и информатичката технологија рапидно го зголемува потенцијалното влијание на сајбер тероризмот и војувањето на начини што не се очекуваат, целосно разбрани или подготвени од меѓународната заедница, националните држави, корпоративните субјекти или поединци.

Технолошкиот напредок во, како што се нарекуваат технологии со двојна употреба, може да им овозможи на помалку технолошки напредните народи, па дури и на малите поддржавни групи потенцијално да му нанесат голема штета на општеството во иднина. На пример, во областа на биолошкото оружје, Џ. Клапер вели дека со оглед на широката дистрибуција, ниската цена и забрзаното темпо на развој на технологијата со двојна употреба, нејзината намерна или ненамерна злоупотреба може да доведе до далекусежни економски и национални безбедносни импликации. Во областа на биолошкото оружје, намалувањето на

⁷³ Clapper, J.R.: Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee (2016 February 9), p.1-6

трошоците за моќните технологии со двојна употреба се одвива со речиси незамисливи стапки.⁷⁴

Технологијата исто така може значително да го зголеми ендогениот ефект на насилството врз општествените одлуки. Денешните комуникациски технологии имаат способност драматично да ги засилуваат и сензационализираат актите на насилство кои за возврат можат драстично да ги менуваат политичките дијалози и политиката и често произведуваат непредвидени и непризнаени исходи. Така, иако општеството обично се фокусира на тоа како да се контролира насилството, релативно помалку се фокусира на тоа како и насилните настани со мало влијание можат да влијаат врз политичките и општествените избори.

Двојната употреба и другите технологии претставуваат закана за општеството, кое во моментот ги нема системите за ефикасно реагирање на ваквите закани. Клучната поента е дека овие технолошки достигнувања претставуваат ризици од многу тешки последици со непозната, но потенцијално многу голема веројатност да се појават. За жал, тие исто така претставуваат развој на настаните што општеството започна да ги проценува и развива институционалните стандарди и норми за нивно контролирање. Само неодамна, претседателот на Мајкрософт предложи свикување на Женевската конвенција за сајбер војна.⁷⁵

Другите екстерни влијанија можат да ја нарушат моменталната способност да се справиме со насилството. Сепак, и покрај напредокот во контролирањето на насилството, општеството сега се соочува со уште една рунда предизвици за кои ќе бидат потребни дополнителни применливи фокусни точки. Овие несомнено ќе бараат посилна меѓународна координација и регулација, нешто што станува сè помалку популарно кај голем број развиени нации.

⁷⁴ Clapper, J.R.: Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee (2016 February 9), p.1-6

⁷⁵ Weise, E.: Microsoft calls for 'digital Geneva Convention'. USA Today

Помеѓу крајот на Втората светска војна и осумдесеттите години, светот бил сведок на историски економски придобивки од страна на Соединетите држави, проследено со Европа, Јапонија, а подоцна и со разни нации од Југоисточна Азија, вклучувајќи ги Кореја, Сингапур, Кина (Хонг Конг) и Малезија. Во двете децении по осумдесеттите години на минатиот век се забележани драматични намалувања на екстремната сиромаштија кај земјите во развој низ поголемиот дел од светот и драматичен раст на приходите на ниво на средна класа кај избраните југоисточни азиски нации, особено Кина и во помала мера Индија.⁷⁶ Сепак, во текот на истиот овој период голем дел од светот доживеле значителни економски предизвици кои негативно влијаеле на стабилноста на многу земји и на благосостојбата на нивните граѓани на непредвидени начини.

Овој период е доказ на зголемена нестабилност и зголемување на нееднаквоста на избраните пазари на труд, зголемување на економската несигурност кај граѓаните со предност во развиените нации и продолжување на екстремната сиромаштија низ голем број народи. Нееднаквоста се зголемила на неочекувани начини и во рамките на нациите и меѓу нациите. Исто така, се чини дека се зголемила регионално во некои нации. Во последните децении, приходите во развиените нации драматично се зголемени за најголемиот процент од нивните граѓани, но стагнирале или опаднале за многу од нивните граѓани од средната класа и значително се намалиле за помалку образованите членови на нивните општества.

Покрај тоа, технологијата и глобализацијата, исто така, произведуваат она што може да се нарече структура за добивање на сите награди преку индустриите, во рамките на претпријатијата и низ различни региони и земји. На ниво на работник, технологијата создава феномен на стабилни работни места каде единицата на трудот на една личност може да се продаде повеќе пати без никаков дополнителен напор. Исто така, компаниите за информатичка технологија го зголемуваат своето обезбедување на централно управување и безбедносни услуги

⁷⁶Milanovic, B.: Global Inequality: A New Approach for the Age of Globalization. The Belknap Press of Harvard University, Cambridge, MA. (2016)

базирани на облак (cloud) на деловните претпријатија. Деловните субјекти што купуваат такви услуги, тогаш можат да ги заменат своите работници во или да ги пренаменат на порутинска и пониско платена работа. Ова создава ситуација кога многу мали разлики во индивидуалниот талент, обука или среќа можат да доведат до многу големи разлики во приходите меѓу работниците. Оваа динамика се чини дека создава многу голема диференција во платите и произведува намалување на вкупниот број на работници потребни во дадена професија.

Во текот на последните 70 години, нашите сегашни економски системи и технологии произведоа невиден економски раст, извадија голем број луѓе од сиромаштија и создадоа нов и растечки среден начин на живот во земјите во развој. Во исто време, постојан напредок воопшто не е загарантиран. Глобалниот карактер на економиите и финансиските индустрии заедно со брзите технолошки промени создаваат растечка еднаквост и високи нивоа на стрес, вознемиреност и во некои случаи гнев кај оние кои станаа неповолни од економските и социјалните промени. Општо, денешните економски и финансиски системи се склони кон потенцијални сериозни нестабилности на прилично непредвидливи начини. Конечно, нашиот економски систем и ориентацијата на нашите финансиски системи се акумулираат што претставува огромни еколошки долгови што мора да се платат за опстанокот на општеството.

Решавањето на предизвиците презентирани од нашите економски и технолошки системи несомнено ќе бара посилна меѓународна координација и регулација, нешто што може да одговори на зголемен отпор од зголемувањето на национализмот во некои земји

V ГЛАВА

БЕЗБЕДНОСТ НА КОРПОРАЦИИТЕ

БЕЗБЕДНОСТ НА КОРПОРАЦИИТЕ

Справување со потенцијални закани

Денес, не можеме да се обидеме да ја сфатиме целата сложеност на денешниот свет, појавите и процесите што се случуваат во него, сложеноста на системите што ги создал човекот, видот и бројот на информациите кои кружат низ него, а притоа да не се соочиме со потребата од нивни разбирања и планирања. Почетоците и динамиката на развојот на планирањето како научна дисциплина се во економијата, каде што и перманентно се бараат методи и начини за реално планирање и намалување на трошоците на сметка на зголемување на профитот. Според теоријата на системите која е доминантно развиена во последните децении на минатиот век, нереалноста на планирањето доведува до пропаст на системите. Затоа е развиена и кибернетиката како наука за управување на сложените системи кајшто најважна фаза е планирањето, а основни методи со кои се служи се моделирањето и системската анализа. Практично во голема за висност се теоријата на системите, моделирањето, планирањето и кибернетиката, бидејќи ги обединува иста цел, а тоа е подобрување на функционалноста и ефикасноста на сложените управувани системи.⁷⁷

Планирањето се извршува секојдневно од речиси секој човек. Во личниот живот се размислува за определени работи кои треба да се извршат наредниот ден, наредната недела или наредниот месец. Личните активности многу често се планираат на неформален начин. Меѓутоа, инситуционалното планирање е посложено, формализирано и поодговорно. Основната намера на планирањето е да развие тек акции за остварување на целите, односно тоа е процес на одлучување или антиципативно одлучување.⁷⁸

⁷⁷ Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација

⁷⁸ Шуклев, Б., (2002), Деловно планирање, Економски факултет, Скопје

Планирањето претставува многу тешка и комплексна активност што значи дека неговиот предмет го чинат сите облици на општествена активност, дејност и живот насочен кон постојан развој.⁷⁹

Планирањето како активност во време на динамични услови за живот и работа добива се поголемо значење, а тоа го наметнуваат брзите техничко-технолошки промени, економските состојби, политичката ситуација и други фактори. Во вакви околности кајшто се изразени очекувањата и се соочуваме со непредвидливоста, комплексноста итн, планирањето претставува начин како да се држат очите отворени, како да се унапреди состојбата, како да се донесат подобри одлуки, како да се изберат најдобрите алтернативи и како да се создаде реален пристап кон остварување на задачите во иднина.⁸⁰

Планирањето е фаза на процесот на управување и претставува континуиран процес на донесување плански одлуки и на избор на најповолни цели, политики, стратегии, програми и планови. Со планирањето се одредуваат целите, силите и средствата и се претвораат во плански задачи на одредени лица, органи и организациски единици. Исто така, планирањето претставува целосно размислување однапред со кое се подобрува одлучувањето. Планирањето не се ограничува само на донесување плански одлуки, туку тоа е настојување тие одлуки да се реализираат. Всушност, планирањето е процес на одлучување што и како нешто треба да се направи пред да се преземе акцијата, што значи со тоа да се влијае на работниот процес во целина или на неговите делови. Тоа укажува дека планирањето не е чин, туку процес што нема крајна точка. Тоа значи дека се приближува кон решението, но никогаш во потполност не стигнува до него, што е првенствено врзано за фактот дека во текот на планскиот процес се доаѓа до примена на системи за кои се планира во неговото опкружување.⁸¹

⁷⁹ Argenti, J., (1989): Practical Corporate Planning, UNWIN- Paperbacks, London.

⁸⁰ William, A., (1987), Forecasting. An appraisal for Policy - Makers and Planners, The Johns Hopkins Press, London

⁸¹ Стаменковски, А., (1996), Планирање на одбраната, Ѓурѓа, Скопје

Во литературата постојат голем број дефиниции кои поимот планирање го објаснуваат како функција, како процес, содржина, активност насочена кон перманентен развој.⁸²

Според Хикс, планирањето е умствена работа која што вклучува примена на логичко и корисно размислување за решавање некој проблем, а успехот на организацијата зависи од успехот со којшто функцијата на планирањето е извршена на секое организациско ниво и доколку активностите не се планираат тие ќе бидат нерационални, неостварливи, случајни и нема да бидат ориентирани кон целите. Исто така, авторот посочува дека планирањето води кон повисок степен на рационалност и тоа ги координира активностите во институцијата кон дефинираните на целите. Алтернатива на планирањето е однесувањето препуштено на случајност.

Британскиот економист Л. Робинс истакнува дека да се планира значи да се избере и да се дејствува кон определена цел, а изборот е суштината на економската активност и аналогно на тоа сиот живот вклучува планирање. Понатаму, овој автор посочува дека постоењето на повеќе од едно планирање (еден план) може да предизвика неусогласеност на различните планови. Во отсуство на координација еден план може да го оневозможи другиот. Во оваа насока шведскиот економист Ј.Свенилсон смета дека планирањето е координирање на акциите во различни идни периоди со користење на еден план.⁸³

Дармер смета дека планирањето му помага на менаџментот да ја антиципира иднината и да размислува за систем на меѓуодносите во кои тој дејствува. Со планирањето, менаџментот може да развие конзистентна ориентација кон непредвидливото опкружување на иднината на која се дејствува. Така, планирањето е средство на мислење на менаџментот за остварување на тоа што е сакано и како тоа треба да биде остварено. Конкретно, како умствена

⁸² Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик: (во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување.

⁸³ Hicks, H., (1972), The Management of Organizations, McGraw- Hill Books Company, Inc., New York

активност, планирањето охрабрува иновација, овозможува да има растегнување на умот и е истражување на повеќе алтернативи.⁸⁴

Друкер планирањето го дефинира од аспект на неговата содржина и тоа како формулирање цели, политики, програми и постапки за нивно остварување или планирање кое опфаќа дефинирање на целите на организацијата, изработка на стратегијата за остварување на тие цели и развивање сеопфатна хиерархија на планови која треба да ги активира и да ги координира активностите. Планирањето е масовна активност која му помага на човекот, односно му овозможува да го постигне тоа што го сака со предвидување.⁸⁵

Ланданер планирањето го дефинира како водење стопански активности од страна на некој орган на заедницата, врз основа на некоја програма што ги опишува квантитативно и квалитативно потребните производствени процеси во некој иден период. Месие смета дека планирањето е процес преку кој се гледа во иднината и се откриваат нови алтернативни правци на акција.⁸⁶

За Шуклев, планирањето е дел од процесот на менаџментот и претставува прва фаза од процесот на управување и е примарна фаза на управувањето, која во себе ги опфаќа активностите поврзани со истражувањето, предвидувањето и донесувањето одлуки за основните цели, политиката, стратегијата и тактиката и поединечните планови со кои треба да се обезбеди остварувањето на зацртаните цели и политики.⁸⁷

Според Чепујноски, планирањето по својата суштина претставува инструмент на свесна организација и управување со општествено економскиот развој во сообразност со научното спознание на економските законитости.

⁸⁴ Darmer J., (1977) Management Planning and Control Systems, Advanced Concepts and Cases, (Richard D) Inc., Homewood, Illinois.

⁸⁵ Drucker P., (1997) Management, Pan books Ltd., London.

⁸⁶ Landaner C., (1947), Theory of National Economic Planning, Berkeley and Los Angeles, University of California Press

⁸⁷ Шуклев, Б., (2002), Деловно планирање, Економски факултет, Скопје

Стаменковски, пак, планирањето го дефинира како процес на одлучување што да се прави и како да се направи, пред да се преземат определени акции, односно планирањето е селектирање на можни одлуки од многубројни алтернативи.⁸⁸

Stejner, американски автор, планирањето го дефинира најкомплексно истакнувајќи четири перспективи важни за разбирање на суштината на планирањето:

1. Планирањето како иднина на сегашни одлуки;
2. Планирањето како процес;
3. Планирањето како филозофија;
4. Планирањето како структура.⁸⁹

Планирањето како иднина на сегашните одлуки ја изразува комплексноста на планирањето во организационите нивоа и прави да се согледаат причините но и ефектите од актуелните одлуки, како и нивните реперкусии во одредено време. Планирањето се однесува на развојот на експлицитните алтернативни цели и се фокусира на обликување на посакуваната иднина.⁹⁰

Планирањето како процес започнува со осознавање на целите и задачите кои се основен концепт и посакувана состојба што организацијата сака да ги оствари, потоа дефинирање на стратегијата и политиките, како и изработка на детални планови за постигнување на целта со кои се специфицираат неопходните алокации на ресурси за достигнување на саканите цели.⁹¹

⁸⁸ Чепујноски Ѓ., Косев С., (2005), Економско планирање, Економски факултет, Скопје

⁸⁹ Stejner G., (1997), Strategic Planning, New York, London, Toronto, Sidney, Singapore, Free Press Paperbacks, Published by Simon Schuster

⁹⁰ Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување(стр-18)

⁹¹ Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување(стр-18)

Планирањето како филозофија ја опишува потребата да се планира што е рационална претпоставка за определување на начинот на живеење. Планирањето симболизира легитимитет за континуирано спознавање на иднината.⁹²

Планирањето како структура опфаќа повеќе видови планови со кои се дефинираат организациските активности и алокации на ресурсите во вид на луѓе, способности, простор за финансиски ресурси, итн.⁹³

Оттука, можеме да заклучиме дека планирањето како научна дисциплина тешко се дефинира.

Планирањето е системска подготовка и темел на решавачките цели за реализирање на плановите во иднина и како процес на апстракција на тие цели во основа е насочено кон селектирање од инфинитивната група можни варијабли и врски, и тоа оние што најдобро ја карактеризираат активноста, а исто така, ги специфицира и резултатите остварени за одредено време. Според оваа традиционална секвенца за решавање на проблемите, планирањето е општо процес што вклучува неколку планирачки активности како што се политичка формулација, стратегиска детерминација, продукција и друго.⁹⁴

За значењето на планирањето треба да се истакнат следните укажувања:⁹⁵

⁹² Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување(стр-19)

⁹³ Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување(стр-19)

⁹⁴ Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување(стр -19) “Значење на планирањето“

⁹⁵ Стаменковски, А., (1996), Планирање на одбраната, Ѓурѓа, Скопје,(стр-388) [http://periodica.fzf.ukim.edu.mk/godzb/GZ64\(2011\)/GZ64.29.%20%D0%91%D0%B0%D0%BA%D1%80%D0%B5%D1%81%D0%BA%D0%B8,%20%D0%9E.%20-%20%D0%9F%D0%BB%D0%B0%D0%BD%D0%BE%D1%82%20%D0%B7%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%20%D0%BA%D0%B0%D0%BA%D0%BE%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%20%D0%BD%D0%B0%20%D0%BF%D0%B%D0%B0%D0%BD%D0%B8%D1%80%D0%B0%D1%9A%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%D1%82%D0%B0%20%D0%BD%D0%B0%20%D0%A0%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%20%D0%9C%D0%B0%D0%BA%D0%B5%D0%B4%D0%BE%D0%BD%D0%B8%D1%98%D0%B0.pdf](http://periodica.fzf.ukim.edu.mk/godzb/GZ64(2011)/GZ64.29.%20%D0%91%D0%B0%D0%BA%D1%80%D0%B5%D1%81%D0%BA%D0%B8,%20%D0%9E.%20-%20%D0%9F%D0%BB%D0%B0%D0%BD%D0%BE%D1%82%20%D0%B7%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%20%D0%BA%D0%B0%D0%BA%D0%BE%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%20%D0%BD%D0%B0%20%D0%BF%D0%B%D0%B0%D0%BD%D0%B8%D1%80%D0%B0%D1%9A%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%D1%82%D0%B0%20%D0%BD%D0%B0%20%D0%A0%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%20%D0%9C%D0%B0%D0%BA%D0%B5%D0%B4%D0%BE%D0%BD%D0%B8%D1%98%D0%B0.pdf)

- 1) Идната неизвесност и промените го прават планирањето потребно и во случаи кога постои извесна иднина, односно планирањето е потребно за правење избор на оптимална алтернатива од повеќе алтернативи;
- 2) Со планирањето се утврдуваат целите;
- 3) Со планирањето се зголемува координацијата на активностите со кои се остваруваат целите;
- 4) Со планирањето се зголемува ефикасноста.

Покрај ова, значењето на планирањето се гледа и во следното:

- 1) Со него се оневозможува парцијално одлучување;
- 2) Се придонесува полесно да се совладаат промените;
- 3) Претставува канал на комуникација;
- 4) Придонесува во унапредување на управувањето и раководењето;
- 5) Со негова помош се овозможува да се донесат оптимални плански одлуки засновани врз претходно анализирање и предвидување;
- 6) Се создаваат претпоставки за стабилен развој и друго.⁹⁶

Кога планирањето се карактеризира со секоја акција на донесувачите на одлуки, значењето на планирањето се гледа во извршувањето на следните работи:

- Тоа би водело кон подобра позиција или положба во институцијата. Планирањето не е само по себе крај, туку тоа е средство за остварување на крај.

⁹⁶ Стаменковски, А., (1996), Планирање на одбраната, Ѓурѓа, Скопје, (стр-387) [http://periodica.fzf.ukim.edu.mk/godzb/GZ64\(2011\)/GZ64.29.%20%D0%91%D0%B0%D0%BA%D1%80%D0%B5%D1%81%D0%BA%D0%B8,%20%D0%9E.%20-%20%D0%9F%D0%BB%D0%B0%D0%BD%D0%BE%D1%82%20%D0%B7%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%20%D0%BA%D0%B0%D0%BA%D0%BE%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%20%D0%BD%D0%B0%20%D0%BF%D0%B5%D0%B0%D0%BD%D0%B8%D1%80%D0%B0%D1%9A%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%D1%82%D0%B0%20%D0%BD%D0%B0%20%D0%A0%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%20%D0%9C%D0%B0%D0%BA%D0%B5%D0%B4%D0%BE%D0%BD%D0%B8%D1%98%D0%B0](http://periodica.fzf.ukim.edu.mk/godzb/GZ64(2011)/GZ64.29.%20%D0%91%D0%B0%D0%BA%D1%80%D0%B5%D1%81%D0%BA%D0%B8,%20%D0%9E.%20-%20%D0%9F%D0%BB%D0%B0%D0%BD%D0%BE%D1%82%20%D0%B7%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%20%D0%BA%D0%B0%D0%BA%D0%BE%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%20%D0%BD%D0%B0%20%D0%BF%D0%B5%D0%B0%D0%BD%D0%B8%D1%80%D0%B0%D1%9A%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0%D1%82%D0%B0%20%D0%BD%D0%B0%20%D0%A0%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%20%D0%9C%D0%B0%D0%BA%D0%B5%D0%B4%D0%BE%D0%BD%D0%B8%D1%98%D0%B0)

- Тоа би и помогнало на организацијата во развојот на начин на кој нејзиниот менаџмент размислува најкомплетно.
- Тоа му помага на секое раководно лице да размислува, да одлучува и да постапува поефикасно за остварување на саканата цел.
- Тоа помага да се одржи флексибилноста на организацијата.
- Планирањето стимулира интегративен и ентузијастички приод кон организационите проблеми. Постои природна тенденција во најголем број организации вниманието да се концентрира на моменталните проблеми, изолирајќи ги нив од другите проблеми.
- Тоа му укажува на раководниот тим како да го оценува и да го проверува прогресот кон планските цели.
- Планирањето би водело кон општествени и корисни резултати.

Генерално, идентификувани се повеќе причини од потребата за планирање. Прво тоа е процес на комуникација и како таков ја унапредува координацијата. Второ, тоа мотивира што значи активно влијаение на доброто планирање. Трето, планирањето води кон подобро одлучување, односно планирањето вклучува повеќе фактори во размислувањето затоа што од донесувачите на одлуки се очекува да ги оценат идните импликации од сите донесени одлуки.⁹⁷

Исто така, планирањето е потребно до степен до кој една организација мора да ги антиципира промените од опкружувањето и да го намали временското заостанување содржано во процесот на приспособување; раководниот тим во институцијата мора да бара општи рамки за да ги интегрира одлуките и целите; комуникацијата мора да биде потпомогната, конфликтите разрешени, а координацијата и соработката остварени.⁹⁸

Потребата од планирање станува се понагласена во услови на брзи промени на техничкото, технолошкото, економското, социолошкото, политичкото и

⁹⁷ Шуклев, Б., (2002), Деловно планирање, Економски факултет, Скопје

⁹⁸ Darmer J., (1977) Management Planning and Control Systems, Advanced Concepts and Cases, (Richard D) Inc., Homewood, Illinois.

безбедносно опкружување, бидејќи со него се градат инструменти за осознавање на неизвесната иднина и за приспособување кон неа.⁹⁹

Целите може да се дефинираат како одредена специфична состојба, ситуација или резултат, која организацијата посакува да ја оствари. Целите се поставени во насока што ја дава исходноста на акцијата која треба да се преземе, односно целите служат за насочување и за координација на сите активности, организациони делови и поединци. Кога еднаш ќе се формулираат, тие претставуваат критериуми за донесување рационални одлуки во изборот на алтернативните правци на акција, како и стандардна контрола за ефикасно и ефективно дејствување.¹⁰⁰

Целите на планирањето ја исполнуваат кога се мерливи, јасно дефинирани, кога се усогласени, кога се предизвикувачки и реални и кога се временски детерминирани. Мерливоста на целите се изразува преку големата мотивациска сила за самите субјекти додека дефинирањето на клучните цели е особено важно затоа што тоа овозможува да се прецизираат до ситни детали сите аспекти на однесување на субјектот во соодветната организација. Предизвикувачките цели секогаш не значи дека се и реални. Ако целите не се реални тие негативно влијаат на човекот и на неговиот морал. Исто така, целите треба да се временски одредени, за да се знае во кој временски период треба да бидат реализирани.¹⁰¹

Во однос на одбраната, целите на планирањето се во корелација со утврдените развојни интереси и тие може да се категоризираат како цели на стратешко, на оперативно и на тактичко ниво.¹⁰²

⁹⁹ Стаменковски, А., (1996), Планирање на одбраната, Ѓурѓа, Скопје

¹⁰⁰ Milosavljevic M.m Todorovic J., (1987), Poslovna i razvojna politika samoupravnog preduzeca, Sovremena administracija, Beograd.

¹⁰¹ Станковиќ Т., (2004) Планирање, Факултет за цивилна одбрана, Белград

¹⁰² Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување

Стратегиските цели на планирањето на одбраната се утврдуваат на ниво на држава и врз нивна основа се насочуваат развојните активности на сите делови на системот на националната одбрана односно на сите носители и учесници во планирањето. Во рамките на овие цели се утврдени општите, посебните и поединечните цели на развојот на одбраната, а кој се внесуваат во плановите за развој и во плановите на одбранбените активности.

Општите цели на стратегиски нивоа, имајќи ја предвид организациската и хиерарихиска поставеност на системот за одбрана се единствени за целиот систем и неговите подсистеми. Со нив се насочува организацијата, подготвеноста и функционирањето на системот и неговите основни компоненти. Посебните цели на стратегиското ниво произлегуваат од општите цели, а се однесуваат на развојот на потсистемите и нивните основни елементи додека поединечните цели на стратегиско ниво претставуваат конкретизација на општите и посебните цели, врз чијашто основа се утврдуваат конкретните задачи.¹⁰³

На оперативно ниво, целите на планирањето се во функција на насочување на задачите, потребите и можностите за развој, на елементите на потсистемите на одбраната, односно на посебно организираниите сили за одбрана на оперативно ниво. Оперативните цели мора да се усогласени со стратегиските, како и во нив да се содржи насоката, односно идејата за целите на тактичко ниво.¹⁰⁴

На тактичко ниво, целите на планирањето служат за конкретизација на развојот на одбранбениот систем и подготовките на извршителите во планирањето на одбраната и на силите и на средствата на посебно организираниите сили за одбрана на тактичко ниво. Истите цели задолжително мора да се во согласност со повисоките (оперативни цели) и тие можат да бидат општи, посебни и поединечни.¹⁰⁵

¹⁰³ Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација

¹⁰⁴ Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација

¹⁰⁵ Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација

Задачите на планирањето произлегуваат од утврдените цели и претставуваат нивна конкретизација. Тие конкретно се однесуваат на *кој, каде, што, како* и *кои* активности и акции треба да се преземат за да се остварат поставените цели.¹⁰⁶

Планирањето има повеќе задачи кои можат да се претстават преку неколку елементи, и тоа:

- Релативизација на конфликтноста на развојните цели во општеството во целина;
- Намалување на неизвесноста во остварувањето на поставените цели на развојот;
- Максимизирање на позитивните разлики од екстерните фактори и слично.¹⁰⁷

Од аспект на безбедноста, важно е да се напомене дека задачите на планирањето се утврдуваат и се спроведуваат со низа детерминирачки претпоставки кои понатаму укажуваат на комплексното опкружување и влијание на одредени фактори кои се важни за реализирање на безбедносните цели.

Со процесот на планирање во одредена институција, се поставуваат основните определби за насоките и идентификуваните потреби. Процесот на планирање условно се состои од пет елементи, и тоа:¹⁰⁸

- I. Поставување примарни цели и меѓуцели. Личниот придонес на раководните луѓе влијае врз примарните цели. Поставувањето цели, на пример, во безбедносниот сектор се прави од страна на носителите на раководни функции во овој сектор. Меѓуцелите помагаат да се разјаснат

¹⁰⁶ Станковиќ Т., (2004) Планирање, Факултет за цивилна одбрана, Белград

¹⁰⁷ Т. Гоцевски, О. Бакрески, С. Славески, ЕУ низ призмата на европската безбедност, Филозофски факултет, 2007

¹⁰⁸ Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување.

примарните цели и најчесто се поставувани од пониските нивоа на управување.

- II. Истражување можности. Истражувачкиот елемент е насочен кон собирање податоци и се фокусира кон откривање на можностите што ги нуди средината, а генерално се примарни за спроведување на понатамошните активности.

Проценка на ризик е израз што се користи за да се опише целокупниот процес или метод што вклучува идентификување, евалуација и утврдување на сите закани (ризици) и нејзините предизвикувачки фактори и изнаоѓање на решение за отстранување на тие закани пред да се предизвикаат катастрофалните резултати.¹⁰⁹ Како една од процедурите за корпоративна безбедност, проценката на ризикот вклучува пет термини.

а) Идентификација на ризици: тоа вклучува процес на наоѓање, наведување и карактеризирање ризици / закани и неговите предизвикувачки фактори пред појавата на катастрофален резултат.

б) Анализа на ризик: Тоа вклучува процес за разбирање на природата на ризиците / заканите и утврдување на нивото на ризик. Анализата на ризикот дава основа за проценка на ризикот и одлуките за контрола на ризик. Информациите можат да вклучуваат тековни и историски податоци, теоретска анализа, информирани мислења и загриженост на засегнатите страни. Анализа на ризик вклучува проценка на ризик.

в) Евалуација на ризик: Процес на споредување на проценет ризик со дадени критериуми на ризик за да се утврди значењето на ризикот.

г) Контрола на ризик: Тоа вклучува активности што ги спроведуваат одлуките за проценка на ризик. Контролата на ризик може исто така да вклучуваат следење, преоценување и усогласеност со одлуките.

¹⁰⁹ Rausand M 'Risk Assessment: Theory methods and Applications'(2013) John Wiley & Sons

Улога на проценка на ризик врз безбедноста на компанијата

Проценките на ризиците се многу важни бидејќи тие претставуваат составен дел од безбедносната политика на корпорациите. Создаваат свесност за ризикот, идентификуваат кој може да биде изложен на ризик (на пример, вработени, чистачи, посетители, изведувачи, јавност и сл.), утврдуваат дали е потребна програма за контрола за посебен ризик/закана, утврдуваат дали постојните контролни мерки се соодветни или треба да има повеќе направено особено кога е направено во фазата на дизајнирање или планирање, да се даде приоритет на мерките за ризик и контрола и да ги исполнуваат законските барања каде што е применливо. Целта на процесот на проценка на ризикот е да се процени ризикот, потоа да се отстрани тој ризик или да се минимизира нивото на ризикот со додавање на контролни мерки, по потреба. За да се постигне целта, односно правилна проценка на ризикот обидете се да одговорите на следниве прашања:

- што може да се случи и под кои околности?
- кои се можните последици ?
- како веројатно се појавуваат можни последици ?
- дали ризикот се контролира ефикасно или и понатаму се бара акција?

Планирање на проценка и анализа на ризик

Проценката на ризикот треба да се направи пред да бидат утврдени какви било безбедносни политики или мерки. Проценката на ризик обезбедува како треба да се фокусира безбедносната политика и кои се безбедносните мерки соодветно да се применат за да се спречи и заштити секоја закана. Планирањето за проценка на ризик воопшто, е утврдување кој ќе биде опсегот на проценка на ризик, на пр., спецификација на област, обезбедена услуга, големината на персоналот и посетителите, физичката област каде што се одвива работната активност, или видови на ризик, како ризик на свршеник, измама, кражба итн., потребните ресурси (на пример, обука А) тим на поединци за извршување на проценката, видовите на извори на информации, безбедноста мерки итн.), каков

вид мерки за анализа на ризик ќе се користат (на пример, колку е точна скалата или дали параметрите треба да бидат со цел да се обезбеди најрелевантна проценка), кои заинтересирани страни се вклучени (на пример, менаџер, супервизор, работници, претставници на работници, добавувачи, итн.), кои се релевантни закони, регулативи, кодови или стандарди може да важат во вашата пресуда или проценка, како и организациони политики и процедури.

Доставување проценка и анализа на ризик

Менаџерот за корпоративна безбедност треба да биде надлежен за проценка на ризикот и да направи научна анализа на ваквите ризици. Менаџерот за безбедност мора да ја знае природата на бизнисот во рамките на субјектот пред да ја достави проценката. Природата на бизнисот го одредува бројот на ризик во рамките на компанијата, на пример, ризикот во банкарскиот бизнис е прилично различен од ризикот во деловниот субјект на осигурување или деловните компании во трговијата на мало.¹¹⁰

Така, службеникот за безбедност има должност да спроведе темелно истражување на деловната активност на компанијата за да му овозможи идентификување, проценка и утврдување на какви било закани по безбедноста. Важно е да се запамети дека проценката мора да ја земе предвид не само моменталната состојба во компанијата, туку и при какви било потенцијални ситуации исто така. Со утврдување на нивото на ризик поврзано со ризикот, на работодавачот, менаџментот и тимот за безбедност (каде што е соодветно), можат да одлучат дали контролната програма е потребна и на кое ниво.

Извори на процедури за проценка и анализа на ризик

Како би требало да се проценат и анализираат ризиците, зависи од законодавството на државата и регулативите, меѓународните безбедносни стандарди и упатства и практики во рамките на компанијата субјект. Должност е

¹¹⁰ Rausand M 'Risk Assessment: Theory methods and Applications'(2013) John Wiley & Sons

службеникот за безбедност и неговиот тим да ја истражат природата на бизнисот и тогаш да направат усогласување на ваквите наоди од истражувањето во рамките на регулаторните, меѓународните стандарди и упатства за проценка и анализа на ризиците.

Современи пристапи во справување со заканите

Кога станува збор за иднината во развојот во корпоративната безбедност треба да има превид трансформацијата низ која поминуваат современите корпорации. Како резултат на најновите техничко технолошки достигнувања светската економија, а со тоа и корпорациите се менуваат, односно трансформираат. Ако средствата на компаниите ги поделиме во две групи: видливи (tangible) и невидливи (intangible) и на првime временска анализа тогаш се забележува промена во нивната улога во производствените и услужните процеси на микро ниво.

Настануваат промени во нивното учество во креирањето новосоздадена вредност и тоа во насока на експоницијален раст на учеството на т.н. невидливи средства (знаење и умеење, патенти, авторски права, информации, информативни мрежи, софвери, интеграции на оперативните процеси). Значи вредноста на т.н. невидливи средства расте побрзо од вредноста на видливите средства на корпорациите. Ова природно предизвикува промени во потребата и значењето на нивната заштита, а со тоа во концептите и формите на корпоративната безбедност, односно заштитата на т.н. невидливи средства станува се позначајна.

Заштитата на корпоративните средства веќе не е доминантна како облик на физичката заштита на средствата во сопственост на корпорацијата, туку позначајна станува заштитата и безбедноста на информатичките мрежи, податоците кои се движат низ овие мрежи, податоците кои се чуваат во складишта за податоци, интелектуалната сопственост, know-how, авторските права и сл. Компаниите од услужната дејност заедно со индустриските компании од т.н. индустрија 4.0 имаат потреба од еден сосема нов вид на корпоративна безбедност.

До пред половина век, поимот шпиунажа главно се однесуваше на шпиунажа меѓу државите. Имајќи ја предвид структурата на современата економија, треба да се промени името од „индустриска“ во „деловна“ шпиунажа, бидејќи предмет на шпиунажа не се само деловните тајни во индустријата, туку и во услужниот сектор.

Денеска деловната шпиунажа е и пораспостранета меѓу државите. За разлика од оддавањето на државни тајни кое се санкционира со кривични закони и е кривично дело, корпорациите многу тешко можат да користат законски мерки против неовластеното оддавање на деловни тајни. Ова ја прави заштитата од деловна шпиунажа уште посложена и потешка.

Потребата за квалитет на заштитата кај деловната шпиунажа станува сè поголема. Заради ова компаниите се приморани да изнаоѓаат и имплементираат нови креативни солүции кои ќе обезбедат нивна заштита од т.н. индустриска шпионажа.

Најранливи за вакви дејствија се истражувачките единици на корпорациите. Тука треба да се додаде уште еден многу значен момент за современите компании, но и за корпоративната безбедност, а тоа е обезбедување на континуитет на производството, односно операциите на компанијата, елиминирање или субстантивно намалување на застоите на операциите. Ова е посебно значајно заради поврзаноста на производствените процеси, односно функционирањето на т.н. *supply chains*. Со цел да не врзуваат голем капитал во репроматеријали и други компоненти потребни за производство, корпорациите чуваат минимални залихи и очекуваат навремено да бидат снабдени со потребните инпути.

Континуитетот на снабдување со репроматеријали и полупроизводи, стоки и давање на услуги во услови кога економијата функционира во модул на *just on time supply chain* е особено значајно. Способноста на компанијата навремено и во континуитет да ги снабдува своите клиенти е поеднакво важно како и цената и квалитетот на сировините, полупроизводите што се продаваат, односно услугите што се даваат. Заради ова компаниите покрај добрата заштита на видливите и невидливите средства, неопходно е да имаат добро разработени планови за превенција, но и планови за постапување доколку се случи настан кој го нарушува

континуитетот на бизнис операциите без оглед дали е резултат на природата или пак на човечки фактор. Нарушување на континуитетот покрај директните финансиски штети, може да ја наруши и репутацијата на компанијата.

Заклучок

Врз основа на претходните истражувања дојдов до следниве заклучоци:

Во одредена форма, безбедноста постоела уште од почетокот на животот, заедно со инстинктот да се заштити истата. Со создавањето на заедниците, инстинктот полека се губел и бил заменет со логика. Иако претежно можеме само да претпоставиме, бидејќи всушност не знаеме толку многу за античките заедници, безбедноста сигурно била една од примарните грижи на нашите далечни предци. Во основа, безбедноста постепено стана клучен комунален процес кој бил мотивиран од заемен интерес и се изведувал со користење на седумте основни столба на безбедносниот процес: луѓе, физички елементи, технологија, процедури, информации, координација и комуникација. Иако во доста апримитивна, но ефективна форма, нашите предци ги применувале сите основни елементи на безбедноста што до денес се сметаат (но не секогаш практично се користат) за основни столбови на безбедносниот систем.

Безбедноста во суштина е главна компонента во развојот на државата затоа што преку остварувањата на потребното ниво на безбедност се остварува потребната заштита на граѓаните за нивниот имот, личната заштита, заштитата на работните места и итн. Безбедноста е севкупен феномен кој ги детерминира вкупните состојби од аспект на остварувањето на заштитата на државата и граѓаните од различни видови на загрозување затоа безбедноста претставува иманентен дел на општеството затоа што ја обезбедува и структуралната позиција и функционалната позиција и дејност на општеството.

Во современата теорија на безбедноста има бројно широко прифатени концепти кои ги означуваат современите права на безбедноста. Секако, покрај концептите за национална безбедност важен е концептот на корпоративна безбедност.

Корпоративната безбедност е посебно важна за корпорациите, компаниите, организациите и денес клучното прашање не е дали е потребна корпоративната безбедност туку да се гради корпоративна безбедност.

Едноставно кажано, корпоративната безбедност е мултидисциплинарна и повеќеслојна функција чија одговорност е да ги координира целокупните напори за безбедност на комерцијална организација. Во теорија, таа тесно соработува со деловниот менаџмент и сите функции што се однесуваат на безбедноста, деловниот континуитет и усогласеноста за зачувување на деловните интереси, луѓето, профитот и угледот и ублажувањето на ризиците.

Во истражувањето се потврди хипотезата дека корпоративната безбедност преку дејноста која ја остварува влијае на целокупниот развој на корпорацијата во организациска смисла и во функционална смисла и во безбедносна смисла.

Корпоративната безбедност е исто така одговорна за насочување на сите вработени во извршувањето на своето учество во безбедносниот систем на една организација преку нивните секојдневни постапки и пресуди.

Анализата потврди дека корпоративната безбедност е важен дел на корпоративната структура и како таква е основен предуслов за остварување на потребното ниво на заштита на компаниите од различни предизвици со кои се соочуваат во поширокиот општествен контекст.

Корпоративната безбедност е задолжена за проценка, мерење и квантифицирање на ризиците; измислување, планирање, спроведување и контрола на безбедносните мерки кои имаат за цел да ги предвидат и забележат трендовите, да спречат и да запрат инциденти и да ја разберат нивната корелација во различни делови на корпорацијата и во различни фази на деловните процеси; анализирање на перформансите и успехот на безбедносните мерки и нивно соодветно прилагодување при добивање поддршка од организацијата, како од аспект на мандатот, така и од финансирањето.

Аналицата супституционално потврди дека во корпоративната безбедност предуслов за остварување за потребното ниво за безбедност во компаниите е спроведување на функциите во целост.

Глобализацијата ја смени структурата и темпото на живот на компаниите; заситеноста на традиционалните пазари ги носи компаниите на поризични места; поместувањето кон економија на знаење ја нарушува важноста на „местото“ во деловниот свет; нови деловни практики, како што се компаниите со предизвик да

управуваат на далечина; и новите форми на отчетност, како што се корпоративното управување и општествената одговорност на претпријатијата, извршуваат дополнителен притисок врз компаниите да ги поклопат своите зборови со дела, каде и да работат. Во истражувањето се потврди меѓузависноста помеѓу корпоративната безбедност и современите предизвици бидејќи тоа се клучни елементи со кои се придонесуваат на одредено ниво на остварување на целите на корпорацијата.

Во исто време, безбедносните ризици станаа посложени, исто така. Многу од заканите, како што се тероризмот, организираниот криминал и безбедноста на информациите, се асиметрични и мрежни, што го отежнува управувањето со нив. Во рамките на истражувањето се потврди хипотезата за непосредната корелација помеѓу суштинските потреби на корпорациите наспроти реалните предуслови за остварување на потребните задачи.

Анализата потврди дека постојат бројни предизвици со кој се соочуваат корпорациите но особено од аспект на безбедоста значајни се тероризмот, сајбер криминал, организираниот криминал, државните непријатели и итн.

Исто така, постои поголема ценење на меѓузависноста помеѓу портфолиото на ризици на компанијата и начинот на деловното работење: одредени видови на однесување може да ја подобрат или поткопаат „лиценцата за работа“ на една организација, а во некои случаи тоа може да генерира ризици кои инаку не би постоеле.

Нема дилема дека корпорацијата за да се справи со потенцијалните предизвици мора да им довери на менаџерите по корпоративна безбедност целосна доверба која се заснова на професионализам и треба да се базира на реалната ситуација помеѓу она што значи корпоративна добивка и корпоративен ризик.

Во истражувањата се потврди изработката на соодветна анализа и проценка во компанијата придонесува да се објективизираат состојбите.

Ефикасното справување со ризикот подразбира и придржување кон принципите дадени во корпорацијата како составен дел од организациските процеси. Управувањето со ризикот е севкупна одговорност на менаџментот од сите проекти и процеси кои се во согласност со плановите на корпорацијата. Управувањето со ризикот на менаџерите им помага во поставување на приоритетни цели при избор на алтернативни правци во нивното дејствување. Анализата потврди дека управувањето со ризик секогаш се заснова на најдобрите добиени информации како и прогнозата и експертските размислувања.

Анализата на светско ниво потврди дека не постои ниту една компанија комплетно заштитена од опасности и ризици, исто така не постои работно место без опасност и ризик од настанување на повреди. Целта на проценката на ризикот е секогаш насочена кон намалување на ризиците од можните опасности и ризици, односно отстранување на штетните влијанија при работниот процес.

Опасноста се потврди дека може да претставува се она што не опкружува без да правиме разлика помеѓу материјалите, опремата, работните методи, надворешните или внатрешните закани кои имаат висок потенцијал да предизвикаат застој или повреда. Како краен исход од опасноста следува да ја процениме истата.

Повеќето истражувања во корпорациите потврдија дека за успешно остварување на деловните резултати е значајно доброто раководење и управување со човечките ресурси. Тоа е секако можно да се достигне со ефикасен менаџмент на човечки ресурси. Менаџментот на човечки ресурси допринесува во проучувањето на сите аспекти на вработените во корпорациите, а воедно менаџментот за човечки ресурси зазема управувачка функција во корпорациите, која во изминативе години е изложена на многубројни предизвици кои ги носат глобалните, технолошките промени и промените во демографската структура.

Менаџментот на човечки ресурси има голема одговорност за човечкиот капитал во организацијата. Одговорен е секогаш да најде компетентни личности, како и да организира соодветна обука за работното ангажирање кое допринесува

со висок учинок и ефикасност за одржување на продуктивната алка на организацијата.

Каков и да е резултатот од опасностите и ризиците, безбедноста денес има поголем профил во корпоративниот свет отколку пред пет години. Компаниите бараат нови начини за управување со ризиците и опасностите, додека портфолиото на одделот за безбедност се проширува и вклучува заедничка одговорност за работи како што се углед, корпоративно управување и регулирање, општествена одговорност на компаниите и осигурување на информации.

Користена литература

Alruwaili, A., & Brooks, D. J. (2008). Organisational security: a propositional study to map expert knowledge. Proceeding of the 1st Australian Security and Intelligence Conference pp. 4-11). Perth.

ASIS International.(2002). Proceedings of the 2002 academic/practitioner symposium. The University of Cincinnati, Ohio: ASIS International

ASIS International.(2003). Proceedings of the 2003 academic/practitioner symposium. The University of Maryland, Maryland: ASIS International.

ASIS International.(2005). Career opportunities in security. Alexandria: ASIS International.

ASIS International. (2009). Security body of knowledge (BoK): Substantive considerations. Unpublished

ASIS International Academic/Practitioner Symposium 2009, ASIS International.

Argenti, J., (1989): Practical Corporate Planning, UNWIN- Paperbacks, London.

Australian Security Industry Association.(2008). Security industry overview. Retrieved 2 September, 2008, from <http://www.asial.com.au/default.asp?page0%2Fconsumer+information%2Fsecurity+industry+overview>

BAJAGIĆ, Mladen, Osnovi bezbednosti, Policijska akademija, Beograd, 2007, str. 57.

Bazzina, M. (2006). Security standards and support systems report: A collaborative project between the Commonwealth Attorney-General's Department and Standards Australia. Sydney: Standards Australia International Ltd.

Borg, I., & Groenen, P. J. (2005). Modern multidimensional scaling: theory and applications (2nd ed.). New York: Springer. 100 Asian Criminology (2013) 8:89–101

Boskovic, M., Osnovni detektivskog delatnosti, Novi Sad, 2006

Bradley, T., & Sedgwick, C. (2009). Policing beyond the police: A "first cut" study of private security in New Zealand. Policing and Society, 19(4), 468–492.

Brooks, D. J. (2008). Defining the science of security through knowledge categorisation. Acta Criminologica, CRIMSA Conference Special Edition 2008, 1, 12-23.

Brooks, D. J. (2009a). Key concepts in security risk management: A psychometric concept map approach to understanding. Saarbrücken: VDM Verlag.

Brooks, D. J. (2009b). What is security: Definition through knowledge categorisation. Security Journal. doi:10.1057/sj.2008.18,1-15.

Calder, J. D. (2007). Been there but going where? assessing old and new agendas in security research and study. Security Journal, 20, 3–8.

Buckland, B., Winkler, T. (2011), Javno-privatna saradnja: izazovi i mogucnosti upravljanja bezbjednoscu,. Beograd, forum za bezbednost i demokratiju

Business Security Survey 2004, MORI, IPSOS and the Confederation of British Industry (CBI) in association with QinetiQ.

Cheng, C. C. (2004). Statistical approaches on discriminating spatial variation of species diversity. Botanical Bulletin of Academia Sinica, 45, 339–346.

Clapper, J.R.: Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee (2016 February 9) p.1-6

Cohen, L., Manion, L., & Morrison, K. (2002). Research methods in education (5th ed.). London: RoutledgeFalmer.

Cox, T. F., & Cox, M. A. A. (2000). Multidimensional scaling: Monographs on statistics and applied probability (2nd ed., Vol. 88). Boca Raton: Chapman & Hall/CRC.

Darmer J., (1977) Management Planning and Control Systems, Advanced Concepts and Cases, (Richard D) Inc., Homewood, Illinois.

Drucker P., (1997) Management, Pan books ltd., London.

Fischer, R. J., & Green, G. (2004). Introduction to security (7th ed.). Boston: Butterworth Heinemann.

Fortna, V. P.: Does Peacekeeping Work? Shaping Belligerents' Choices after Civil War. Princeton University Press, Princeton, NJ (2008)

Giever, D. (2007). Security education - past, present and the future. Security Journal, 20, 23–25.

Gill, M. (2007). The challenges for the security sector: thinking about security research. Security Journal, 20, 27–29.

Gligoroska, M., (2017), Корпоративна безбедност и државниот безбедносен систем. Факултет за детективи и криминалистика, Европски универзитет - Република Македонија

Т. Гоцевски, О. Бакрески, С. Славески, ЕУ низ призмата на европската безбедност, Филозофски факултет, 2007

Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација

Hesse, L., & Smith, C. L. (2001). Core curriculum in security science. Proceedings of the 5th Australian Security Research Symposium pp. 87-104). Perth, Western Australia.

Hicks, H., (1972), The Management of Organizations, McGraw- Hill Books Company, Inc., New York

https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Priracnik_mak_final.pdf

(36-38) Скопје, 2017, Марина Митревска

Hough, P.: Understanding Global Security, 3rd Edition. Routledge, New York (2013)

Huntington, S. Why International Primacy Matters, International Security, 1993

Institut za standardizacija na Srbija, *Drustvena bezbednost- Usluge privatnog obezbedjenja- Zahtevi i upastva za ocenjivanje usaglasenosti*, prvo izdanje, Beograd, 2008, str. 3

Ivetic, S., Pavlovic G. Uporedni modeli privatnog obezbjedjenja licnosti i objekata, Monografija, OEBS, Misija u BiH, Sarajevo, 2015.

Jay, C. (2005). Big debacles help shape a new science. The Australian Financial Review, 17 March 2005, 2.

Keković, Zoran i dr., Procena rizika u zaštiti lica, imovine i poslovanja, Centar za analizu rizika i upravljanje krizama, Beograd 2011, strana 105.

Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. Journal of Criminal Justice Education, 19(2), 290–307.

Kozarev A., Privatna bezbednost u Republici Makedoniji - aktuelno stanje i perspektive, Zbornik radova - Prvi međunarodni naučni skup: Privatna bezbednost - stanje i perspektive, USEE, Novi Sad, 2008 godina, str.177

Козарев А., Блажески В., Страторски А., Приватната безбедност во Република Македонија - теоретски и институционален дизајн, Зборник од втора меѓународна научна и стручна конференција во организација на Асоцијацијата за корпоративна безбедност, Скопје, 2016 година, стр. 14-17.

Krzalic, A., Stanje privatne sigurnosti u Bosni i Hercegovini, Sarajevo, 2009

Кековиќ З., Бакрески О., Стефаноски С., Павловиќ С., (2016), Планирање и процена на ризик:(во функција на заштита на лица, имот и работење). Скопје: Комора на РМ за приватно обезбедување.

Landaner C., (1947), Theory of National Economic Planning, Berkeley and Los Angeles, University of California Press

Manunta, G. (1996). The case against: Private security is not a profession. International Journal of Risk, Security and Crime Prevention, 1(3), 233–240.

Martinez-Torres, M. R., Garcia, F. J. B., Marin, S. L. T., & Vazquez, S. G. (2005).A digital signal processing teaching methodology using concept-mapping techniques.IEEE Transactions on Education, 48(3), 422– 429.

Milanovic, B.: Global Inequality: A New Approach for the Age of Globalization. The Belknap Press of Harvard University, Cambridge, MA. (2016)

Milosavljevic M.m Todorovic J., (1987), Poslovna i razvojna politika samoupravnog preduzeca, Sovremena administracija, Beograd.

Nalla, M. K. (2001). Designing an introductory survey course in private security. *Journal of Criminal Justice Education*, 12(1), 35–52.

Pennebaker, J. W., Francis, M. E., & Booth, R. J. (2001). *Linguistic inquiry and word count (LIWC2001)*. Mahwah: Erlbaum.

Pinker, S.: *The Better Angels of our Nature: Why Violence has Declined*. Penguin, New York, NY (2011)

Prenzler, T., Earle, K., Sarre, R. (2009). Private security in Australia: Trends and key characteristics. *Trends and Issues in Crime and Criminal Justice*, no. 374 [Electronic Version]. Retrieved 11 August 2010, from <http://www.aic.gov.au/publications/tandi/tandi374.html>

Prenzler, T., Martin, K., & Sarre, R. (2010). Tertiary education in security and policing in Australia. *Asian Journal of Criminology*, 5, 1–10. doi:10.1007/s11417-009-9074-7.

Sarre, R. (2005). Researching private policing: Challenges and agendas for researchers. *Security Journal*, 18(3), 57–70.

Schulz, S., Yeung, C., *Private Military and Security Companies and Gender*, DCAF, Geneva, 2005

Schreier F., Caparini, M. (2005), *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, Geneva, DCAF

Simonsen, C. E. (1996). The case for: Security management is a profession. *International Journal of Risk, Security and Crime Prevention*, 1(3), 229–232.

Singer, P. (2003), *Corporate Warriors: The Rise of the Privatized Military Industry*, Ithaca, Cornell University Press

Smith, C. L. (2001a). Security science as an applied science? Australian Science Teachers Journal, 47(2), 32–36.

Smith, C. L. (2001b). Security science: An emerging applied science. Journal of the Science Teachers Association of Western Australia, 37(2), 8–10.

Stejner G., (1997), Strategic Planning, New York, London, Toronto, Sidney, Singapore, Free Press Paperbacks, Published by Simon Schuster

Стаменковски, А., (1996), Планирање на одбраната, Ѓурѓа, Скопје

Станковиќ Т., (2004) Планирање, Факултет за цивилна одбрана, Белград

Talbot, J., & Jakeman, M. (2008). SRMBOK: security risk management body of knowledge. Carlton South: Risk Management Institution of Australasia.

Tate, P. W. (1997). Report on the security industry training: Case study of an emerging industry. Perth: Western Australian Department of Training. Western Australian Government Publishing.

Trochim, W. M. K. (2005b). Concept mapping. Retrieved 28 July 2009

Toyne Sewell Patrick, Private Security Companies: The Reasons Why, Military Technology, Vol. 31, Issue 3, Monch Publishing Group, Bonn, 2007, pp. 60-61

Trivan D., Detektivska delatnost, Beograd, 2014 godina, str. 65.

Trochim, W. M., Cook, J. A., & Setze, R. J. (1994). Using concept mapping to develop a conceptual framework of staff's views of a supported employment program for individuals with severe mental illness. Journal of Consulting and Clinical Psychology, 62(4), 766–775.

Turner, P. (2002). Multidimensional scaling analysis of techniques used by physiotherapists in Southeast Australia: A cross-national replication. *The Australian Journal of Physiotherapy*, 48, 123–130.

ULB, UNI-Europa and CoESS, Preventing occupational hazards in the private security sector (manned guarding and surveillance services), Bruxelles, 2004

Vejnovic, D., i dr., Detektivska djelatnost, Banja Luka-Ljubljana, 2008

Wakefield, A. (2007). The study and practice of security: today and tomorrow. *Security Journal*, 20, 13–14.

Weise, E.: Microsoft calls for ‘digital Geneva Convention’. USA Today, <http://www.usatoday.com/story/tech/news/2017/02/14/microsoft-brad-smith-digitalgeneva-convention/97883896/>

William, A., (1987), Forecasting. An appraisal for Policy - Makers and Planners, The Johns Hopkins Press, London

Yates, A. (2007). The future of private security. Canberra: Australian Homeland Security Research Centre.

Young, L. J. (2007). Criminal intelligence and research: An untapped nexus. *The Journal of the Australian Institute of Professional Intelligence Officers*, 15(1), 75–88.

Zedner, L. (2009). Security: Keys ideas in criminology. London: Routledge.

Зоран Јолевски, Корпоративна безбедност во современата услужна економија и индустријата 4.0.ЗБОРНИК НА ТРУДОВИ ОД ЧЕТВРТАТА МЕЃУНАРОДНА НАУЧНА И СТРУЧНА КОНФЕРЕНЦИЈА. СКОПЈЕ, 2018

Rausand M 'Risk Assessment: Theory methods and Applications'(2013) John Wiley&sons

Šabović, Šerif, Upravljanje rizikom u uslovima krize, u Zborniku radova „Menadžment 2010“, Kruševac, 2010, strana 478.

Шуклев, Б., (2002), Деловно планирање, Економски факултет, Скопје

<http://www.pravdiko.mk/ovlastuvan-ata-na-litsata-koi-vrshat-privatno-obezbeduvanje/>