СЪВРЕМЕННОТО УПРАВЛЕНИЕ НА СИГУРНОСТТА – ЧАСТ ОТ ИНТЕГРИРАНО УПРАВЛЕНИЕ НА БИЗНЕСА

доктор Пламен СОФРОНИЕВ,
Нов български университет,
мениджър „Сигурност“ в „Ди Ейч Ел Експрес България“ ЕООД

Plamen SOFRONIEV, PhD,
New Bulgarian University,
Security manager in “DHL Express Bulgaria” LTD

Резюме: Съвременното управление на сигурността може да се разглежда като пряко отражение на управлението на бизнеса. Казано с други думи, сигурността следва да има съответстващи на бизнеса, който защитава визия, мисия и цели. Ето защо през последните години интегрираните системи за управление, включително и управлението на сигурността, набират все по-широка популярност. От гледна точка на практиката, използването на структуриран и стандартизиран подход при управлението на сигурността е гарант за ефективно и ефикасно управление и в същото време защита на активите на бизнеса. Въпреки актуалността на информационната сигурност и кибер атаките, защитата на физическите активи остава с ключов фактор при управлението на сигурността.

Ключови думи: сигурност, управление, активи, бизнес, стандарт.

Summary: Modern security management can be seen as a direct reflection of business management. In other words, safety should be consistent with the business, which protect vision, mission and goals. That is why in recent years, integrated management systems are rapidly gaining in popularity, including security management. In terms of practice, the use of structured and standardized approach to security management is a guarantor for effective and efficient management while protecting the assets of the business. Despite the timeliness of information security and cyber-attacks, protection of natural assets remains a key factor in security management.

Keywords: security, management, assets, business, standard.

Сигурността на движимите или физическите активи е една от областите, които набират все по-широка популярност при управлението на сигурността. Свидетели сме на свят, в който технологиите и икономиката се развиват изключително бързо, тласкани от потребителското мислене и консуматорското общество. Пазарите придобиват нови измерения – от конвенционална към онлайн търговия, производствата се ре-локират в различни точки на света, в зависимост от икономическите интереси на компаниите.

Въпреки необходимостта от високо ниво на сигурност във веригите от доставки, в съвременните динамични условия и конкурентна среда, за икономическите субекти е по-важно да разполагат със система за сигурност, която да е достатъчно гъвкава. От една страна по отношение на предизвикателствата и посрещането на новите рискове и заплахи пред сектора и от друга страна в състояние да спомага за реализирането на

икономически интереси на субектите. Тази комплексна обстановка изисква бързи и адекватни решения във всеки един момент. Ето защо, днес компаниите разчитат изключително много на най-ценния си актив – персоналът и по-специално на обучения и подготвен персонал, защото именно качествените и добре подготвени експерти по сигурността са в състояние да посрещнат адекватно предизвикателствата на нашия век. Ефективното управление, обаче далеч не започва с експертите по сигурността. Всяка една компания има *Визия, Мисия и Цели.* Това са основните характеристики на печелившия бизнес и успешните икономически отношение. Да имаш визия за своя бизнес и неговото развитие означава най-общо да имаш поглед в бъдещето. Казано с други думи, къде би следвало да бъде една компания в дългосрочен план. Когато разглеждаме мисията, съвсем естествено следва да навлезем в детайлите на една икономическа дейност или конкретен бизнес. Какви би трябвало да са продуктите или услугите, които компанията предлага, на какви стандарти за качество би следвало да отговарят и не на последно място, към кои целеви групи от клиенти са насочени тези продукти и услуги. Днес гласът на клиента е по-важен от всякога, защото компаниите от сектора на стоките и услугите, преживели не една или две икономически кризи, са осъзнали че лоялността на клиентите се постига трудно. Един от начините е именно този – да се вслушаш в гласа на клиента. Това съвсем естествено се е превърнало в една от постоянните стратегически цели на съвременните компании. А целите следва да са един от най-конкретните елементи при планирането и управлението на бизнеса. В съвременното управление и практика е широко разпространен акронимът *SMART*[1] цели. Той идва първите букви на английското значение на понятията Специфични, Измерими, Постижими, Реалистични и Времеви, използвани по отношение на целите и целеполагането. Формирането и реализирането на такива цели е един от гарантите за постигането на мисията и реализиране на визията на една компания.

Когато разглеждаме Визията, Мисията и Целите, сигурността на един бизнес и в частност нейното управление, също не прави изключение. За големите международни компании с изградени структури за сигурност това не е новост, а по-скоро дългогодишна практика, превърнала се в култура, в която се развиват и възпитават следващите поколения експерти и мениджъри по сигурността. Ето защо в структурите за сигурност на съвременните компании, формирането на визия, мисия и цели по сигурността е основен елемент при изграждането на стратегията за сигурност. Използването на SMART цели и в частност създаване на числово измерими показатели на сигурността поставя нейното управление наравно с останалите функции в компанията (финанси, бизнес развитие, продажби, операции). Казано с други думи, управлението на сигурността може да се разглежда като един структуриран и стандартизиран процес, не по-различен от останалите, протичащи в една компания. Това разбира се не лишава сигурността от нейните специфични функции, предмет на дейност, цели и задачи, а по-скоро извежда на преден план прозрачността при управлението и приносът на структурите за сигурност към постигането на целите на компанията и законните бизнес интереси.

---

[1] *SMART (Specific, Measurable, Attainable, Realistic, Time-related) https://www.projectsmart.co.uk/brief-history-of-smart-goals.php - посетен на 30.04.2016 г.*

Както беше отбелязано и по-горе, управлението на сигурността не би следвало да се различава от общото управление на една компания. В частност, визията, мисията и целите на структурата или отдела за сигурност не би следвало да се отличават по своята същност от тези на компанията.

Днес много от компаниите се управляват посредством интегрирани системи за управление – ИСУ. Тези системи по същество наследяват системите за управление на качеството, околната среда, безопасността, непрекъсваемостта на процесите и сигурността от близкото минало. Разликата на пръв поглед е незабележима, но при по-задълбочен анализ могат да се открояят някой основни преимущества на интегрираните системи за управление. На първо място това е ролята на ръководството, която в интегрираните системи за управление ИСУ е изведена на преден план не само чрез ангажимента в политиките и контрола на компанията. В ИСУ към отговорностите на ръководството е добавен и ангажимента за разработване, внедряване и контрол на собствена методология за оценка, управление и апетит за риск. Това за голяма част от компаниите не е ново. В банковия сектор например, методологията и инструментариума за управление на риска са въведени от години. Ситуацията в сектора на застраховането не е по-различна. В авиацията и по-специално в управлението на авиационната сигурност това също не е новост. В сектора на транспорта, съответните стандарти за сигурност на транспортираните активи приложиха методологията за управление на риска в края на 2014 година. В миналото са правени опити, добрите модели от други бизнес сектори да бъдат въведени в сферата на корпоративната сигурност, но като цяло и до момента той не разчита на стандартизиран подход по отношение на управлението на сигурността и по специално по отношение на защитата на физическите активи.

Какво всъщност представлява съвременното управление на сигурността и как би могло да се разглежда? От една страна би могло да се разглежда изцяло от гледна точка на мениджмънта и под формата на система за управление, както описахме по-горе, с нейните особености и характеристики като част от ИСУ. От друга страна може да се разглежда и чисто експертно, от гледна точка на постигането на сигурност на една компания с изцяло експертен подход. Този подход включва анализ и оценка на активите, рисковете и заплахите и тяхното евентуално влияние, при настъпване на събитие с вредоносен резултат. Тук е мястото и на подбора на инструментариум за оценка на защитата и подбор на мерки за сигурност, които да гарантират, че откритите при анализа уязвимости няма да бъдат експлоатирани, както и компенсаторни мерки (в случай на провал на мерките за сигурност).

Съвременното управление на сигурността в една компания, която развива бизнес в частна полза и чиято крайна цел е постигане на печалба и законни бизнес интереси, започва с отговорността и ангажимента на ръководството. Когато управлението на сигурността е част от ИСУ, отговорността и ангажимента включват един основен документ – Политиката за сигурност. Аналогия с други стандарти за управление от една интегрирана система, веднага ще покаже, че в този документ висшето ръководство на една компания следва да заяви кои са неговите приоритети (по отношение на сигурността) и с какво се ангажира, следвайки тези приоритети. Освен приоритизирането, политиката за сигурност трябва да е ясна и разбираема за цялата

компания и да бъде комуникирана, познавана и спазвана от всички служители. Именно това е документа, върху който се основава управлението на сигурността. Върху него следва да се изгради системата за сигурност и според него ще се управлява сигурността и защитата на активите в компанията. В повече детайли, политиката за сигурност трябва на първо място да отразява волята на ръководството да предотвратява и ограничава вероятността от настъпването на събития с вредоносен резултат, както и да гарантира сигурността на компанията. В допълнение политиката за сигурност може да се насочена към безопасността на обществото и околната среда. Друг важен момент, който следва да отразява политиката за сигурност е съответствието с визията, мисията и целите на компанията. По този начин целеполагането на отдела по сигурността ще гарантира, че целите и задачите, които се поставени или се възлагат на експертите по сигурността ще са насочени към постигането не само на целите по сигурността, но и целите на компанията.

След като компанията разполага с политика за сигурност, следващата стандартизирана стъпка е свързана с отговорността. Това се постига като се назначи ръководител, който да е отговорен за системата за сигурност, в това число и за отдела за сигурност. В негово лице висшето ръководство ще търси ръководната функция, която ще следи за внедряването, поддръжката и оценката на системата за управление на сигурността, съгласно собствената си политика. В практиката, често пъти мениджъра или ръководителя по сигурността е част от висшето ръководство, което по никакъв начин не следва да влияе на субординацията в компанията, а напротив. Подобна практика и отношение към сигурността само показват ангажираността на една компания към опазването на нейните активи.

Както всяка една организационна политика, така и политиката за сигурност следва да бъде комуникирана и сведена до знанието на целия персонал на компанията. Важно е в комуникацията да се подчертае важността на политиката за сигурност, нейния задължителен характер, както и стремежа към постоянно подобрение, който е характерен за ИСУ. Един от основните моменти, които също следва да се отбележат при съвременното управление на сигурността е ресурсното осигуряване. Назад във времето, немалко компании смятаха, че сигурността е въпрос единствено на организационни мерки и фирмена култура и пренасочваха значителни човешки и времеви ресурси за внедряване на технически мерки за сигурност и обучения по сигурността, фокусирани предимно към персонала. Тази политика на управление на сигурността дава своите положителни резултати, но отразява управлението на сигурността едностранно и в недостатъчна степен. Когато говорим за съвременното управление на сигурността и неговия стандартизиран подход, ресурсите с които следва да разполага съответния ръководител могат да бъдат обобщени както следва:

- хора, притежаващи необходимите знание, умения и квалификация;
- оборудване, отговарящо на потребностите на компанията и активите, които следва да се защитават;
- вътрешна инфраструктура, която да подпомага отдела по сигурността;
- технологии за защита на активите и превенция;
- информация;

•процеси;

•бюджет.

Както беше посочено по-горе една от основните разлики при съвременното управление на сигурността е отношението към управлението на риска. В тази връзка, след внедряването на политиката за сигурност, следва да се определят критериите по отношение на оценката и управлението на риска за сигурността като част от интегрираната система. Това от своя страна включва както конкретни критерии за рисковете както за сигурността, така и по отношение на активите, към които се прилагат мерки за сигурност. На този етап се оформя и концепцията за апетит за риск на съответната компания. Казано с други думи какви нива на риска би могла да си позволи да понесе компанията като запази пазарната си позиция и не позволи да бъде „извадена“ от бизнеса. За тази цел в компанията преди всичко трябва да има разработен и внедрен стандартизиран процес по планиране. Както беше описано по-горе, сигурността не би следвало да се възприема като област различна от останалите в бизнеса, ето защо действията на висшето ръководство по отношение на рисковете за сигурността логично следват утвърден, в останалите области на бизнеса, процес на планиране. Конкретно по отношение на рисковете за сигурността планирането би могло да започне „отвън-навътре“. В обратния случай би означавало, че компанията игнорира външната среда и нейните фактори, което от своя страна би довело до погрешно планиране, погрешно алокиране на ресурси и погрешни управленски решения. При планирането по отношение на риска за сигурността отвън-навътре, висшето ръководство може да започне с идентифицирането и проучването на всички нормативни изисквания, които могат да се отнесат и да се прилагат към компанията, нейната структура, активи, персонал и дейности. В този процес е необходимо да се обхванат изискванията към доставчици, клиенти и трети страни за да може в последствие да се изгради цялостна картина на рисковете за сигурността. След като нормативните изисквания са идентифицирани, тази информация трябва периодично да се обновява с цел недопускане на несъответствия поради промяна в законодателството. По отношение на рисковете за сигурността, съвременното управление чрез интегрирани системи предвижда стандартизиран подход. Той е базиран основно на ISO 31000:2009[2] методологията за управление на риска. Този подход предвижда няколко основни момента, които са релевантни, както спрямо общото управление на сигурността, така и спрямо защитата на физическите активи:

•Оценка на рисовете – където са включени:

-Идентифициране;

-Анализиране;

-Оценяване.

•Третиране на рисковете:

-Преглед на оценката и анализа;

-Избор на мерки за противодействие;

•Мониторинг.

[2] *ISO 31000:2009 - http://www.iso.org/iso/catalogue_detail?csnumber=43170 – посетен на 30.04.2016 г.*

По този начин следва да се разглеждат и оценяват рисковете за сигурността в компанията в основната им форма. В допълнение, ангажимент на мениджъра по сигурността е да представи пред висшето ръководство оценка на различните възможности спрямо рисковете за сигурността. Подобно на анализа и оценката на нормативната база, спрямо рисковете се предвижда същия подход. Редовния преглед на оценката на риска, като част от прегледа на ръководството на ИСУ би спомогнал за по-добро управление на сигурността в компанията. Както бе отбелязано по-горе стандартизирания подход, базиран на утвърдена методология следва да гарантира, че рисковете са адресирани и третирани съгласно визията на ръководството за гарантирането и управлението на сигурността, като част от интегрираната система за управление.

След разработването и внедряването на инструментариума за наблюдение и оценка на риска, фокусът на интегрираното управление на сигурността се насочва към активите на компанията и тяхната защита. Практиката показва, че когато става дума за информационни активи, компаниите предпочитат стандартизиран подход, който включва решение от край до край и обхваща всички процеси. Това са решения базирани на стандартите за информационна сигурност от групата на ISO/IEC 27001:2013[3]. По отношение на физическите активи има различни подходи за защита. Те са свързани с няколко аспекта, касаещи компанията – специфика на икономическите дейности, на процесите, на бюджета за сигурност и разбира се на оценката на риска за самите активи. В контекста на съвременното управление на сигурността е важно целите и задачите на отдела за сигурност да съответстват на целите на компанията. В това отношение, защитата на физическите активи също изисква стандартизиран подход, който да е основан на идентификацията на активите и оценката на риска за самите активи. При този подход, могат да се следват няколко основни момента, които да подпомогнат избора на ефективни мерки за сигурност на физическите активи:

- Създаване на програма за защита на физическите активи;
- Създаване на стандартни оперативни процедури за защита на активите като част от ИСУ;
- Създаване на програма за обучение и оценка на ефективността от обучението;
- Разработване на методология за целеполагане и оценка на представянето на отдела за сигурност.

Ефектът от всичко това е създаването на цялостна и работещата система за управление на сигурността и внедряване на ефикасни мерки за защитата на физическите активи. Като част от ИСУ, системата за сигурност не би следвало да се разглежда като изолирана системата. Тя е съвкупност от хора, процедури, оборудване и технологии, чиято цел е да защитава активите, съоръженията, процесите и имуществото като цяло. Целта и функционирането на тази система биха могли да се обобщят като възпиране настъпването на нежелано събитие, забавяне на злонамерени лица от постигане на целите им, засичане на потенциално събитие с вредоносен резултат или лице, което планира реализирането на такова събитие. При разработването и внедряването на система за сигурност и най-вече по отношение на защитата на

[3] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm - *посетен на 29.04.2016 г.*

физическите активи е важно мерките за защита да са разработени на различни равнища, които да включват като минимум:

- Планиране на средата (CPTED[4]);
- Физически бариери;
- Контрол на достъпа;
- Осветление;
- Охранителни системи;
- Видеонаблюдение;
- Защита на мрежовата инфраструктура;
- Персонал;
- Административни процедури и управление.

След разработването и внедряването на системата за сигурност, тя не следва да съществува и да се разглежда като фиксирана система основана на един документ. Когато управлението на сигурността е част от ИСУ, системата за сигурност се разглежда на равни интервали от време, разписани в системата за управление. Една от добрите практики в областта е използването на модела PDCA [5] или Планиране, Изпълнение, Проверка, Действие – съкращението идва от първите букви на английските понятия. Този модел гарантира постоянното и устойчиво развитие на системата за сигурност, както и нейното управление. Максимална полза за системата за сигурност може да се гарантира, когато този модел се използва още при внедряването. Тогава етапите от модела могат да изглеждат по следния начин:

- Планиране – базирано на оценката на риска и целите на организацията, определяне на мерките за противодействие и методите за контрол
- Изпълнение – внедряване на системата, оформяне на процесите, обучение и разпределяне на отговорности
- Проверка – избор на метод за оценка и оценяване ефективността на системата
- Действие – управление на промените и постоянно подобрение на системата.

Управлението чрез интегрирани системи е отражение на съвременните потребности на бизнеса от подход, който носи не само ефективност и ефикасност, но и най-голяма полза на самия бизнес. Чрез ИСУ компаниите и мениджърите могат да гарантират на своите акционери, клиенти и партньори, че бизнеса който управляват се развива в положителната посока и начинът на управление е прозрачен и стандартизиран. В резултат на това сигурността претърпява една своеобразна трансформация във формирането, целеполагането и управлението, която я превръща от чисто разходна област за компанията, в неделима част от общото управление и развитие на бизнеса. Тази трансформация видоизменя управлението на сигурността от чисто експертно и функционално, към интегрирано с всички принципи на управлението, характерни за съответния бизнес. По този начин планирането и развитието на сигурността е хомогенно и съобразено с особеностите и характеристиките на средата, променящите се заплахи и потребностите на бизнеса, който защитава.

---

[4] *Crime prevention through environmental design - http://www.cpted.net/ - посетен на 30.04.2016 г.*

[5] *Plan-Do-Check-Act - https://www.mindtools.com/pages/article/newPPM_89.htm - посетен на 30.04.2016 г.*

Използвана литература:

1. *ISO 31000:2009 - http://www.iso.org/iso/catalogue_detail?csnumber=43170*
2. *SMART (Specific, Measurable, Attainable, Realistic, Time-related) https://www.projectsmart.co.uk/brief-history-of-smart-goals.php*
3. *Crime prevention through environmental design - http://www.cpted.net/*
4. *Plan-Do-Check-Act - https://www.mindtools.com/pages/article/newPPM_89.htm*
5. *http://www.iso.org/iso/home/standards/management-standards/iso27001.htm*