

6. A biztonsági vezető tevékenysége nagyvállalati környezetben

Csikós Gellért

Jelen fejezet célja, hogy gyakorlatias iránymutatást adjon a nagyvállalati biztonsági területen elhelyezkedő vezetőknek. Minden élethelyzetre megfelelő általános, instant megoldások nem állnak rendelkezésre, de jelen fejezet tanulmányozása segítséget nyújthat a célravezető gondolkodásmód, szemlélet elsajátításában.

6.1. A nagyvállalati biztonság jellemzője, rendezőelvek

A nagyvállalati biztonság a kreativitásnak, önmegvalósításnak teret adó közeg. Nincsenek olyan kötött előírások, mint például a rendvédelmi szerveknél, amelyek jogszabályi előírás alapján kötelező erővel határozzák meg a feladatokat, a felelősségeket. Ezen a területen inkább ajánlások, bevált gyakorlatok vannak, amelyeket alakítani lehet és kell is. Az alkalmazott módszert befolyásolhatja a vállalati kultúra, az első számú vezető személyes tapasztalata vagy a meghatározó vezetők személyisége, kommunikációja, a szervezet pénzügyi eredményei, rendkívüli események (a továbbiakban: RES), piaci helyzet változásai.¹

Nagyvállalati környezetben a biztonsági vezető tevékenysége nem az általa képviselt szervezet egyéni szabályozói, továbbá egyéb utasítások, határozatok, jogszabályok betartása és betartatása alapján lehet eredményes. A vezető személyes elkötelezettsége, az üzleti élet kommunikációjának megértése is hozzájárul az eredményességhez (megtérüléskalkuláció).

6.2. Biztonsági pillérek és a kontroll

A sikeres és fenntartható biztonsági működés megvalósításában a biztonsági vezető támogatására a „kontroll”, valamint a „befolyásolás” körébe tartozó szempontrendszerek állnak rendelkezésre. A „kontroll” megvalósításáért, vagyis a helyes működésért, annak fenntartásáért egy személyben a biztonsági vezető a felelős. A „kontroll” szempontrendszerbe nem tartozó egyéb feladatok a „befolyásolás” körébe tartoznak. Ezen feladatok végrehajtása és a végrehajtási feltételek biztosítása az egyenrangú (mellérendelt vagy oldalági) azonos beosztásban lévő vezetőkön múlik, vagyis akkor valósulnak meg, ha a regnáló biztonsági

¹ AMIR Mohtarami (2015): *Enterprise Security Architecture: Approaches and a Framework*. Paris, International Conference on Information Systems Security on May 18–19.

vezetőnek jó a befolyásolási, kapcsolatteremtési képessége, és eléri, hogy a vele egyenrangú vezetők elismerjék kompetenciáját, figyeljenek rá.

Az egyenrangú (mellérendelt vagy oldalági) vezetők között szervezeten belül nincs függőségi kapcsolat. Ezen vezetők támogathatják egymás munkáját, vagy érdekütközés esetén (objektív szempontrendszer figyelembevételével) akár hátráltathatják is.

Valaki vagy segít, vagy semleges marad, persze érdekütközés esetén, vagy ha a vezetők közötti jó összhang nem működik, az akár még hátráltathatja is a megoldást. A harmadik az „aggodalom” köre, ide azok a feladatok kerülnek, amelyeket nem tudunk megoldani, és a vezetőkhöz kell vele fordulni. A sikeres vezetők önjárók, hiba nélkül működtetik a kontroll körét, és eredményesek a befolyásolás körében, az aggodalom körébe minimális problémát visznek csak be.

6.2.1. A biztonsági vezető helyzete a vezetési struktúrában

Egy vállalat működésének biztonságában meghatározó kérdés, hogy a struktúrában hol helyezkedik el a biztonság. Erről a korábbi fejezetben már részletesen szóltak, így csak emlékeztetőül néhány gondolat.

A legtöbb nagyvállalat a felső vezetők közé sorolja a biztonsági igazgatót, aki az első számú vezetőnek jelent. Ennek a megoldásnak az előnye, hogy kialakulhat egy személyes kapcsolat az első számú vezető és a biztonsági igazgató között, minden vállalati működés, személyzeti kérdés vonatkozásában közvetlenül tudnak találkozni. További üzenete ennek a megoldásnak, hogy a vezető fontosnak tartja ezt a beosztást, személyesen is elkötelezett a biztonságos működtetés érdekében, és minden felső vezető biztonsági tudatossága megfelelően alakítható. A biztonsági igazgató képes stratégiai szinten működni, véleményezi a döntés-előkészítéseket, és első kézből szerez tudomást a változásokról.

Vannak azonban olyan vállalatok, ahol a biztonsági vezető eggyel alacsonyabb szintre van sorolva, például biztonsági osztályvezetőnek, és közvetlenül a pénzügyi, személyzeti vagy jogi igazgatónak jelent. Ennek a besorolásnak az üzenete, hogy a biztonsági vezető operatív szinten képes működni, sérülhet a felső vezetők biztonsági tudatosságának fejlesztése, és az első számú vezetőhöz csak szűrt információ jut el. Több esetben tapasztaltuk, hogy komolyabb veszteségek vagy rendkívüli események bekövetkezésekor a vállalati reakció az volt, hogy „minőségi cserét” hajtottak végre, és magasabb szintű biztonsági vezetőt vettek fel, aki már az első számú vezetőnek jelentett.²

A biztonsági vezetőnek 360 fokban kell gondolkodnia, azaz a vállalat teljes működését monitoroznia kell, ha a biztonsági tudatosságot és a védelmi intézkedéseket, különösen pedig a költségvetést időben be szeretné terveztetni. Törekednie kell arra, hogy a tervekről értesüljön, mert akkor lesz lehetősége a biztonsági koncepciót minden új vagy változó folyamatba beépíteni. Ellenkező esetben csak az utolsók között értesül a változásokról, amikor már késő biztonsági koncepcióról, szükséges költségvetésről beszélni.

Az „üzleti partner” jellegű biztonsági vezetőnek rendelkeznie kell a hatékony időgazdálkodás és kommunikáció, konfliktuskezelés, delegálás, helyzetfüggő vezetés

² RITCHOT, Brian (2013): An Enterprise Security Program and Architecture to Support Business Drivers. *Technology Innovation Management Review*, Vol. 7. 25–33.

képességével, hogy a vállalat működését lássa magasabb perspektívából is, és ne vesszen el a részletekben. Lehet, hogy csak kis létszámú közvetlen csapata van, de az általa generált biztonsági tudatosság – az elkötelezettség elnyerésén keresztül – minden osztályban jelen van, így nagyobb csapattal dolgozhat, mint ahogy azt sokan elsőre felismerik. Azt érje el, hogy ne a jelenléte, hanem az elvárásai, ajánlásai működtessék a biztonsági szemléletet.

Sokáig dilemmát okozhat, ha nemcsak egy, hanem kettő vezető van a biztonsági főnök felett, és nem tisztázott, hogy kinek mikor mit jelentsen, kit miről tájékoztasson. Főként külföldi nagyvállalatokra jellemző ez a kettős vezetés.

A közvetlen (line) vezető általában a magyarországi vezérigazgató, aki a biztonsági vezető teljesítményértékelését készíti, aki meghatározta a fizetés mértékét, annak emelését. Ők az adott országban való működésért voltak a felelősek, és közvetlenül irányították a teljes magyar vezetőséget.

A szakmai (dotted line) vezető általában a régiószintű vagy az európai biztonsági vezető, akinek a felelősségi körébe tartozott a kijelölt országokban működő biztonsági igazgatók munkájának koordinálása.

Fontos egyeztetni, hogy kinek mi a fontos, és mit hova jelentsen a biztonsági vezető, ha az nincs a belső szabályokban rögzítve. Megoldás lehet az is, hogy minden eseményről mindkét vezetőt tájékoztatni kell, akár személyes megbeszéléseken, vagy ha levelet kell küldeni, akkor mindkettőt megjelölni címzettként. Idővel kialakulhat, hogy kivel miről kell részletesebben egyeztetni, de az is előfordulhat, hogy ők egymásra is támaszkodnak, tehát ha a szakmai vezetővel már átbeszél egy témát a biztonsági vezető, akkor a vezérigazgatónak csak rövid összefoglalóra van szüksége.

Egyes helyzetekben kialakulhat érdekellentét a vezetők között, amikor az országos vezető nem szeretné, ha a probléma az európai vezető elé kerülne, tehát országon belül akarja azt tartani. Ezekben a helyzetekben is az a megoldás, hogy egyeztetni kell velük, mit szeretnének, és mit engednek meg a biztonsági szakma szabályai. A legrosszabb helyzet talán az, ha a biztonsági vezető beszorul a két vezető közé, taktikáznia kell, amiből könnyen gond lehet.

6.2.2. Biztonsági alkalmazottak

A belső biztonsági munkatársak kiválasztása, képzése kritikus fontosságú. Erről is részletesen olvashattunk a megelőző fejezetben. A legtöbb, legújabb képzést érdemes számukra biztosítani, hogy naprakészek és hitelesek legyenek a társosztályok munkatársai előtt, és magabiztosak az ügyintézéseikben. Ők az igazi, operatív „nagykövetei” a biztonsági operációnak. Viselkedésük, megjelenésük eleve meghatározza a biztonsági vezető minőségét, ha a csapatuk nem képviseli ugyanazt a vonalat, máris veszítenek értékükből.

Legyen mindenkinek munkaköri leírása, célkitűzése, teljesítményértékelése, valamint személyes és csoportos megbeszélésekre lehetősége. Inkább a beosztottak hozzák a problémákat és azzal együtt a javaslatukat, mint hogy a vezető tartson előadást, eligazítást, ami meglátásom szerint nem a hosszú távon működő modell ebben a környezetben.

Vezetőként javaslom a biztonsági operáció éves munkatervének létrehozását, amely hetekre, hónapokra, negyedévekre van felosztva, és áttekinthetővé, jól tervezhetővé teszi az osztály leterheltségét. Ezen belül a feladatokat érdemes személyekhez kötni, így, ha ezt

a beosztottakra szűrjük, máris rendelkezésre áll az egyéni munkaterv. Ez sokat segít munkatársaink számára a prioritások megtartásában, hogy ne vesszenek el a részletekben, és valóban meg is oldódnak a feladatok. Ezzel meg is teremtettük egyéni teljesítmény-értékelésük alapját.

6.2.3. Biztonsági beszállító menedzsment

Hiszem, hogy akkor járunk el helyesen, ha üzleti partnerként kezeljük az élőerős és biztonságtechnikai szolgáltatókat, ők meg akarnak felelni az elvárásoknak. Segíteni akarnak, és részesei akarnak lenni egy sikeres együttműködésnek. Rendszeresen találkozunk velük közösen, vagy külön-külön is, és hathavonta, évente, amikor értékelhetjük az elmúlt időszak közös munkáját. Bátran mutassuk meg nekik az üzleti és fejlesztési elképzeléseinket, de nyíltan beszéljünk a problémáinkról is, körvonalazva, hogy miben várunk segítséget tőlük. Ha felvetnek valamit, vegyük komolyan, nézzünk utána, és válaszoljuk meg nekik, ezáltal is elnyerve magasabb szintű elkötelezettségüket. Az üzleties fellépésű szolgáltató nemcsak a vagyontörést vagy a kamerákat biztosítja, hanem közösen gondolkodik a megbízóval, segíteni akar a biztonságos ügymenetben. Könnyen felismerhető azonban az a szolgáltató is, ahol a menedzsment kiválóan felkészült, hatékonyan kommunikál, azonban a középvezetői réteg és a végrehajtó állomány már messze nem képviseli a vezetők által beígért működést.

Minden leendő vagy regnáló biztonsági vezetőt arra biztatok, hogy mindig adjanak a szolgáltatóiknak őszinte visszajelzést. Köszönjük meg, ha valamit jól oldottak meg, de azt is mondjuk el, ha valami nem sikerült.

6.3. Biztonságtechnika, biztonsági folyamatok

Rendelkezzünk technikai specifikációkkal, rendszeres karbantartási szerződéssel, „hozom-viszem” szolgáltatással, ha meghibásodik egy-egy kiemelt jelentőségű technikai eszköz, és a karbantartó cég máris hozza a működőképes csereeszközt, amit a javítás vagy pótlás idejére felhelyez. A technikai helyiségek takarítása nagyon fontos, de ne feledjük soha azok biztonsági vonatkozásait sem, fontos még a körletsztenderdek naprakészen tartása is.

Sok esetben a technikai eszközöket a biztonsági beosztottakon kívül más személy is használja, így szükséges számukra az egyszerű, nem technikai nyelvezetű oktatási anyag és minőségi oktatás.

6.4. Bűnügyikockázat-elemzés

Biztonsági kockázati felmérést az adott objektumra nézve mindenképp célszerű elvégezni, már akkor, amikor a telket kiválasztották, és az építési engedélyezési eljárások elindultak.

A bűnügyikockázat-elemzés egy szükséges felmérése az adott objektumnak, amely során a helyi bűnözési adatokat hasonlítjuk az országos arányokhoz. Igaz, hogy ez csak statisztika, de tapasztalatok szerint elfogadható módon mutatja meg a valós képet.

Több áruházláncnál is készült 100–200 boltszám közötti, boltonkénti elemzés, és a kapott eredményt elfogadhatónak találtuk a területet jól ismerő kereskedelmi vezetéssel.

Ide tartoznak többek között a helyi bűnözési adatok, mint a személy és vagyon elleni, erőszakos bűncselekmények aránya, jellemző elkövetési módok, kereskedelmi és ipari objektumok elleni betörések, gépjárműfeltörések, lopások, lakosság összetétele, munkanélküliség mértéke, jellemző foglalkoztatási formák stb. Ezeket az információkat a helyi rendőrség és önkormányzati látogatás során lehet beszerezni. Célszerű előre jelezni, mire is vagyunk kíváncsiak, hogy a hatóság fel tudjon készülni az adatokból. Tapasztalatom szerint inkább találkoztam segítőkészséggel a hatóságok részéről, tekintve, hogy kialakul a közös bűnmegelőzési érdek és az esetleges későbbi egymásrautaltság.³

Statisztikai alapon jól lehet látni, hogy a tízezer lakosra jutó bűncselekmények aránya helyi szinten hogyan aránylik az országos átlaghoz. Ebből a terület fertőzöttségére lehet következtetni. Ezeket az adatokat a [Police.hu](https://www.police.hu) oldalon, a bűnmegelőzési térkép formázásával lehet bűncselekményi kategóriára, országos területrészekre, városokra alakítani. A kapott információ, ha tájékoztató jellegű is, de támaszkodásra mindenképp megfelelő lehet.

Milyen bűncselekmények, rendkívüli események fordulhatnak elő egy nagyvállalatnál? Szinte minden, akár személy és vagyon elleni bűncselekmény, de lehet sztrájk, fegyveres rablás, ATM megrongálása, bankfiók kirablása, fenyegetés, kényszerítés, zsarolás, vesztegetés, szándékos tűzokozás, termékmérgezés, közveszéllyel fenyegetés, kábítószerrel kapcsolatos cselekmények, számviteli, adózási visszaélések, tehát a főtevékenységhez kapcsolódó cselekmények.

Katasztrófavédelem esetén fontos tudnunk, milyen jellegű létesítmények milyen távol vannak az objektumunktól. Például: katonai objektumok, vegyi üzemek, ipari létesítmények stb., de ebben a katasztrófavédelem ma már naprakész információkkal tud szolgálni.

Az objektumokat – felmérésünk alapján – célszerű három kategóriába sorolni: alacsony, közepes, magas kockázatnak megfelelően, ideértve a specifikációk (technikai meghatározások, műszaki és funkcionális leírások) változtatását is.

Az alacsony kategória tartalmazza a minimális biztonsági elvárásokat, a minimális költségvetéssel együtt, a közepes szint már emeltebb biztonsági elvárásokat és az alapköltségvetéshez képest körülbelül 15–20%-kal magasabb költségtervet, a magas kockázati besorolás pedig az alacsony kategóriához képest körülbelül 20–30%-kal magasabb költségvetést tartalmazhat.

6.5. Oktatási rendszer

Az oktatási piramist tudatosan kell felépíteni, amely lefedi a teljes munkát végző állományt.

Komoly felkészülést igényel a felső vezető biztonsági tudatosságának formálása, amely nem ér véget egy beszélgetéssel, azon folyamatosan dolgozni kell. Két különböző típusú vezetőt lehet megkülönböztetni. Van, aki személyiségéből adódóan érzékeny, nyitott

³ Kockázattertelési módszerek és lehetőségeik a fizikai védelem területén (2013). *Biztonságtechnikai szakportál*, 2013. 04. 21. Forrás: www.securinfo.hu/termekek/biztonsagi-szolgalat-az-eloero-eszkozei/978-kockazattertelési-módszerek-es-lehetosegeik-a-fizikai-vedelem-területén.html (A letöltés dátuma: 2018. 07. 21.)

és fogékony az általa irányított terület ellenőrzésére, és minden jelentősebb biztonsági jellegű képzés nélkül, tudatosan kontroll alatt tartja azt.

Van, aki inkább bíz a munkatársaiban, kevésbé ellenőrző típusú, nála lehetnek inkább meglepetésjellegű rendkívüli események.

Javaslom minden leendő biztonsági vezetőnek, hogy kifejezetten sok időt töltsön más üzleti vezetőkkel, legyen nyitott az üzleti felvetéseikre, és meg kell tudni válaszolni a miérteiket, esetleg egy-egy példával alátámasztva azok indokát. Az üzleti vezető mindent vitat – egyébként ez a dolga –, és csak azt fogja elfogadni, ami üzleties, okszerű, szükséges és pénzügyileg indokolt.

Beszélgetéseink során a vezetők elmondták, hogy ha tapasztalt vezetőként jöttek is a vállalathoz, előtte nem kaptak biztonsági képzést mástól. Hiszem, hogy akkor nyújtunk igazi segítséget a vezetőknek, ha nemcsak az elfogásokra figyelünk, hanem részesei vagyunk minden folyamatnak, kikérik a véleményünket még a döntéshozatal előtt. Ezért azonban keményen kell dolgozni. Sikeresen működhet a bemutatkozásoktatás. Amikor új vezető érkezik a vállalathoz, és a bevezető képzési programjában a biztonsági vezető is részt vesz, akkor program során találkozhatnak. Ezek a néhány órás beszélgetések a későbbiekben nagyon sokat kamatozhatnak. Átbeszélhetők egymás tapasztalatai, a másikkal szembeni elvárások, országos, helyi veszteségi, bűnözési trendek, és egyeztethető az elsődleges és másodlagos kontroll szerepe.

Nagyon sok múlik továbbá a középvezetői réteg biztonsági tudatosságán. Nagy hívás a közös vezetői értékrend megtartása és a következetes folyamatok megkövetelési igényének kialakítása, fenntartása. A veszteségi és rendkívüli események vizsgálatának általános tapasztalata szerint, ahol a középvezetői kör következtelen volt, vagy különböző vezetői elvárásokat fogalmaztak meg az alkalmazottak felé, annak nyoma észrevehetően látszott a területen, a leltáreredményen, valamint a visszaélések mértékén és minőségén.

Az alkalmazottak azonnal észreveszik, ha két osztályvezető eltérő igényeket támaszt, és kihasználják a vezetői gyengeséget. Nem teljesítenek vagy a saját hasznukat keresik. Az alkalmazottak mondták el, hogy ha választhatnának, inkább a szigorú, következetes vezetővel dolgoznának szívesen, mert bár nehezebb, de magasabb forgalomnál és kevesebb veszteségnél nincs létszámleépítés, megmaradnak a munkahelyek.

Általános szabály, hogy bevezető biztonsági képzést minden munkavégzőnek kell kapnia, s ezt meghatározott időközönként frissítő képzésnek kell követnie. Célszerű ezt összekötni a munka- és tűzvédelemmel, és megfelelő lehet, ha a tréningkoordinátor oktatja az általunk jóváhagyott oktatási anyagot.

Egy objektumban sokféle szolgáltató dolgozhat, és gyakran átlag feletti fluktuáció jellemzi őket, takarító, beszállító stb. Két fő megoldás lehetséges: szerződés részévé tenni, hogy ők kötelesek kiképezni minden – a képviselőtükben eljáró – személyt. A másik megoldás, hogy a képviselő első áruházi bejelentkezése során rövid oktatásban részesüljön, és azt írásban regisztrálják is. Mindkét megoldás lehetséges, az objektum működésének jellege dönti el, melyik a célszerűbb.

6.6. Lehetséges elemzési eszközök

6.6.1. Kockázatelemzés

Egy általános modellt mutatunk be, amely alkalmas többfajta kockázati értékelésre. Használok ezt a modellt több objektum vagy folyamat veszélyeztetettségi besorolására, segít a prioritások racionális kialakításában. Bőven olvashatunk róla részletes leírást, így itt csak a használhatóságára szeretnék példát mutatni.⁴

A kockázatelemzés lényege, hogy egyes kockázatok bekövetkezési valószínűségét és a pénzügyi eredményességre (profitra) gyakorolt hatását méri fel, ítéli meg – igaz, sok esetben szubjektív módon, pusztán üzleti tapasztalat vagy megbecsülés alapján. A szakirodalom ismer háromszor hármas vagy ötször ötös felosztású táblázatot, ahol magas, közepes és alacsony értékek mutatják a kockázat nagyságát. Ezek kombinációja pedig a kockázat végső besorolását, amely akár a prioritási sorrendet is jelentheti. Főként külföldi háttérű vállalatok gyakorlatában tapasztalható e modell használata.

Példaként szeretném megemlíteni azt a tevékenységet, amikor a biztonsági vezetőnek értékelnie kell az adott objektumot veszélyeztető bűncselekmények bekövetkezési valószínűségét és az üzletmenetre gyakorolt hatását, hogy a kockázati besorolás alapján megalapozza, alátámassza a védelmi tervét.

Vegyük alapul a lehetséges rendkívüli eseményeket, bűncselekményeket, amelyek bekövetkezése előfordult már, vagy nagy valószínűséggel előfordulhat a vállalat, a város, a megye vagy az ország vonatkozásában. A bekövetkezési valószínűségeket soroljuk be alacsony, közepes, magas kockázatba, majd az üzletmenetre gyakorolt hatásukat is rangsoroljuk. A magas-magas kockázati kombinációjú bűncselekmények megelőzésével érdemes foglalkozni a listánk élén. Példaként említeném az eladótéri lopást a kereskedelemben, amely bekövetkezési valószínűsége például közepes, de a profitra gyakorolt hatása alacsony, így a közepes-alacsony kombináció legfeljebb közepes szintű kockázatnak minősíthető. Ennek megfelelően kell a védelmi tervet elkészíteni, és a megvalósítását támogató költségvetést betervezni.

Ha egy zöldmezős beruházás részeként épülő, külterületi, felső küszöbértékű veszélyes ipari üzem működési biztonságát tervezzük, és ezen belül a kutatási-fejlesztési épület fizikai védelmét, beléptetőrendszerét, akkor számolnunk kell a tényleges vagy az intellektuális behatolás lehetőségével, amely eredményezhet közepes-magas vagy magas-magas kockázati besorolást.

6.6.2. A DMAIC-modell⁵

A Hat szigma (Six Sigma) módszere egy strukturált folyamatfejlesztő és problémamegoldó elméleti módszer, amely meglátásom szerint a gyakorlatban jól használható a nagyvállalati környezetben. Ez 5 fő lépésből áll, amelyek az azonosítás, a mérés, az elemzés, a fejlesztés

⁴ KINSEY, Vance A. (2010): *DMAIC: Hang Your Tools on a Solid Model*. Old Dominion University. 18–27.

⁵ *Define-Measure-Analyze-Improve-Control (DMAIC)* (é. n.). Elérhető: <https://cdn.ttgtmedia.com/searchSoftwareQuality/downloads/ect01TreasurechestSixSigma.pdf> (A letöltés dátuma: 2018. 07. 15.)

és az ellenőrzés szó angol megfelelőinek kezdőbetűjéből állnak össze: DMAIC, azaz Define, Measure, Analyze, Improve, Control.

Azért javaslom ezt a módszert, mert tapasztalatom szerint, ha egy problémával szembe-sülünk az üzleti életben, hajlamosak vagyunk azonnal a megoldást kitalálni, még azelőtt, hogy a probléma valós gyökerét, okát megállapítanánk. Könnyen álmegoldást hozunk létre, amely jól eladható, a gyorsaságnak fantasztikus „marketingértéke” van, de a valódi hasznossága sokszor igencsak csekély. Újra és újra találkozunk a problémával, ami pedig nem hatékony és nem gazdaságos.

A valódi okot csak alapos kutatás és elemzés után lehet meglegelni, legtöbbször szakértők, specialisták bevonásával, de semmiképpen nem az irodából. Itt valóban le kell menni a részletek szintjére.

6.7. Bűnmegelőzési együttműködés

Kiemelten fontosnak tartom a partneri együttműködés jelentőségét, és hiszem, hogy a modern biztonsági vezető nyitott a tudásmegosztás irányába. Kiváló hazai és nemzetközi magánbiztonsági szerveződések vannak. Egyre nívósabb biztonsági konferenciákkal és igazi inspirátorként indult el néhány éve az NKE RTK MÖR Tanszéke, amely a magánbiztonsági oktatás méltó zászlóshajója. A tudásmegosztás nem üzleti titkok kiadását jelenti, sokkal inkább veszteségi trendek, tendenciák, főbb védelmi lehetőségek megosztása egymással, esetlegesen felkészülés egy váratlan rendkívüli helyzet kezelésére.

Példaként egy kereskedelmi esetet szeretnék megemlíteni, amikor egy budapesti áruházban rendszeresen értünk tetten eladótéri lopáson fiatalokú személyeket. Csak írtuk a feljelentéseket, írtuk és írtuk, de elkövetési csökkenés nem történt. Elemezni kezdtük a környezetet, beszélgettünk a fiatalokkal, és megállapítottuk, hogy a közeli középiskola diákjai szinte virtusból jártak az áruházba lopni. Válaszként felkerestük az iskola igazgatóját, aki őszintén nyitott volt a megoldásra. Előbb a tantestületnek, majd vele együtt az összehívott, érintett évfolyamos diákoknak mondtuk el közösen a lehetséges következményeket, kérve őket, hogy ne tegyék ezt. Következő lépésben kezdeményeztünk egy önkormányzati szintű találkozót, ahova eljöttek más kereskedelmi cégek vezetői – nekik is volt gondjuk a fiatalokkal –, a rendőrség, a gyermekjóléti szolgálat és a polgárőrség képviselői, más iskolák biztonsági referensei. Kiderült, hogy a gyermekjóléti szolgálat nem értesült megfelelő módon az esetekről, és vállalták, hogy akár a családot is meglátogatják fiatalokú visszaélése esetén. Érezhetően csökkent a fiatalokúak által elkövetett virtuosos visszaélések száma. Mit tettünk? Csak beszélgettünk egymással, megosztottuk az információkat, és tisztáztuk, kinek mi lenne a szerepe. Egyedül talán senki nem tudta volna megoldani a helyzetet, de együtt működött.

6.8. Az ECR-modell⁶

A nagyvállalati magánbiztonsági környezetben sajnálatosan még kevés tanulmány áll a rendelkezésre, amely kutatási vagy hivatkozási alap lehet egy induló biztonsági vezetőnek. Korábbi jegyzetemben hivatkoztam erre a tanulmányra, amelyet érdekességgként szeretnék itt is megjeleníteni. Igaz, a kutatás a kereskedelem területéről készült, de gondolkodásmódjával irányadó lehet más biztonsági területek vezetőinek is. Magam is azt gondolom, a nagyvállalati biztonságban a veszteségek jelentős részét nem a külső fenyegetések okozzák, hanem a folyamathibák. Fontos alapelv, hogy csak olyan folyamatunk legyen, amelyik aktuális, oktatható és probléma esetében hivatkozható.

Az ECR- (Efficient Consumer Response) felmérést a Leicester Egyetem (University of Leicester) Kriminológiai Tanszéke végezte 2004-ben, amikor körülbelül 150 kereskedelmi nagyvállalatot kérdezett meg Európában, mi az oka kereskedelmi veszteségeiknek. A válaszok kiértékelése után elkészítettek egy összefoglaló tanulmányt, amelyben 4 fő lehetséges okot határoztak meg:

- Folyamathiba. A felmérés szerint általában a kereskedelmi veszteség 27%-át okozza, lehetséges előfordulásai: lejárt szavatosságú termék, pontatlan árfeltüntetés, termékazonosítási hiba, hibás készletszámolás, rongált termék, szkennelési hiba, hibás szállítás az elosztási központból (raktár), hiányos, többlet- vagy téves termék szállítása.
- Belső visszaélés. A kereskedelmi veszteség 28%-a. Nem megengedett módon termék vagy készpénz jut ki az áruházból, nappal vagy éjszaka, vállalati alkalmazott, szerződéses vagyonőr vagy karbantartást végző személy által. Ide értjük az alkalmazotti lopást, az alkalmazott és vásárló összejátszását, az alkalmazotti dézsmálást (tiltott termékfogyasztást), pénztárosi hiányt és a termékek árainak manipulálását is.
- Külső lopás. A kereskedelmi veszteség 38%-át teszi ki. Nem megengedett módon terméket vagy készpénzt juttatnak ki az áruházból, nappal vagy éjszaka, vásárló vagy nem alkalmazott által. Ide értjük a bolti lopást, a visszáruval kapcsolatos csalást, a betörést, a pénztárak kifosztását.
- Beszállítói csalás. A kereskedelmi veszteség 7%-a ez. Keletkezhet a beszállító vagy alvállalkozója által, ha kevesebb mennyiségű vagy gyengébb minőségű termékeket szállítanak, mint amit kiterhelnek (kiszámláznak) a kereskedőnek. Bérloői, beszállítói csalások tartoznak tehát ide. Kevesebb visszáru számláznak le, mint amit ténylegesen elszállítottak.

Ezt a modellt ma minden kereskedelembiztonsági vezetőnek ismernie kell, de hogy milyen mértékben használja, ez rajta múlik. Nagyon fontos a kereskedők előtti hitelesség szempontjából, hogy ne csak a bűnügyi elfogási statisztikákkal közlekedjünk, hanem elemezzük a kereskedelmi veszteséget, és ennek megfelelően állapítsuk meg kármegelőzési és biztonsági stratégiánkat.

A tanulmány arra is rámutat, hogy a kereskedők biztonsági költségeik 95%-át az eladótér védelmére költik, amely a lehetséges kereskedelmi veszteség csupán 38%-át okozza.

⁶ CSIKÓS Gellért – LÉVAI József (2007): *A létesítmények általános és speciális védelme. 5. témakör: Logisztikai központok, raktárak, ipari létesítmények védelme*. Budapest, Rendőrtisztí Főiskola. 39–40.

6.9. Üzleti pillérek – a befolyásolás köre

6.9.1. Költségvetés, megtérülésszámítás

A biztonsági költség tervezése elengedhetetlen a vezető számára. Hogy ki a költséghely felelőse, ebben lehet eltérés a vállalati hagyományoktól függően. Van olyan vállalat, ahol a biztonsági költség teljesen vagy részben a biztonsági funkcióhoz van rendelve, a tervezéstől a pénzügyi ellenőrzésig.

Van olyan vállalat, ahol másnál van a költséghely, erre példa, amikor a CCTV-rendszer karbantartási költségét az üzemeltetési osztály tervezi, persze egyeztetve a biztonsági területtel. Személy szerint azt tartom fontosnak, hogy a költségek ellenőrzésébe, a tendereztetésbe, a döntéshozatalokba vonjunk be más osztályt az átláthatóság jegyében, semmiképp ne legyen ez mind egy kézben. Lehetőség van együttműködni az eszközbeszerzéssel, az IT-vel vagy a pénzügygel, éljünk vele!

Amennyiben költségvetési megtakarítás a cél, mert a pénzügyi év például nem sikeres, vagy túlköltségek vannak egyes költséghelyeken, akkor a költséghely-tulajdonosok könnyen nyúlnak a biztonsági költségek – csak számszaki – csökkentéséhez, minden szakmaiság nélkül. Ekkor kell a biztonsági vezetőnek irányítani vagy inkább befolyásolni azt, hogy honnan mekkora százalékot csökkentsenek, és ebben segítenek a kockázatelemzések, a riportok. Fontos az, hogy a védelem belső aránya ne torzuljon el, aminek szakértő koordinátora a biztonsági vezető. A költségeket két fő részre bonthatjuk. Egyrészt a beruházási költségek, ide tartoznak a fejlesztési kiadások, másrészt a fenntartási költségek, mint a meglévő rendszerek karbantartási és javítási költségei, alkalmazottbér-költség és szerződéses vagyonőri költség.

A költségvetési év egyes vállalatoknál januártól decemberig tart, másoknál márciustól februárig. A tervezés és jóváhagyási folyamat június–augusztus hónapban aktuális, de erre már időben kell készülni. Segít a tervezésben, ha rendelkezésünkre állnak bűnügyi statisztikák, az előző évhez viszonyított árbevételi, veszteségi, költség-, betegség-, fluktuációs kimutatások. Ismernünk kell a vállalatüzleti változtatásokat, esetleges költségsökkentési kihívásokat, amelyekre szintén reagálnunk kell a tervezésnél.

Tapasztalatom szerint, ami gazdaságos számokkal, tendenciákkal, jövőképpel, kockázat–megtérülés-kalkulációval van alátámasztva, az üzleti élet azt komolyan veszi, és hajlandó invesztálni.

A biztonsági költségek mértékét, esetenként szükségességét mindenki vitatja, ez jellemzi a gazdasági környezetet. Minden üzleti vezetőnek lesz ötlete, valahol látott már egy megoldást, vagy nem látja a védelmi intézkedések értelmét. A biztonsági vezető akkor tudja irányítani, megvédeni az álláspontját, ha megfelelő indokokat sorakoztat fel, trendeket, tendenciákat mutat meg, esetleg konkurenciaérzékeny területen, a versenytársak védelmi szintjére is rámutat. Sokat lehet tanulni a gazdasági, pénzügyi vezetőktől, így javasolom, kérjünk tőlük bátran tanácsot.

Példaként szeretném megemlíteni, hogy egy vállalatnál elemeztük az éves logisztikai be-, ki- és átszállítások, valamint a felhasznált műanyag plombák mennyiségét, az erre fordított munkaidőt, annak bérben kifejezett értékét, a nyomtatványok előállítására fordított festékpátron költségét, a vagyonőri ellenőrzések költségét és a visszaszállított plombák ellenőrzésének, adminisztrációjának költségét. Alternatívaként jelent meg egy állandó

elektromos plomba felszerelése minden jármű minden ajtajára, amely egyszeri beruházás 1,4 év alatt megtérült, és a következő 8 évben sokmilliós költségmegtakarítást jelentett, nem beszélve az adminisztráció csökkentéséről és a hatékonyság fokozásáról.

Javaslom a biztonsági vezetőknek, hogy törekedjenek az üzleti döntések előkészítésénél, tervezésénél jelen lenni. Érték el, hogy állandó meghívottak legyenek ezeken a megbeszéléseken. Például. Az ingatlanok kiválasztási folyamatába állandó résztvevőnek meghívtak figyelembe vették az objektumokra szabott bűnügykockázat-értékelés alapú költségvetési tervet. Amikor tehát az ingatlant kibérelték vagy megvásárolták, már a biztonsági költségvetés is része volt az elfogadott üzleti tervnek.

6.9.2. Válságkezelés (crisis management – CRM); üzleti folytonosság (business continuity management – BCM)⁷

Saját megközelítésben, rövid fogalmakkal szeretném bemutatni a különbséget a két terület között, hangsúlyozva, hogy nagyban összefüggnek, jellegükből adódóan mégis eltérőek kissé:

- Vállalati válsághelyzet: egy váratlan eseményre való reakció, amely azonnal és jelentősen veszélyeztetheti az alkalmazottakat, a vásárlókat, a márkanevet, a vállalat megítélését, működését vagy a tulajdonát.
- Üzleti folytonosság: a vállalat működése szempontjából olyan meghatározó jelentőségű, időfüggő folyamatokra vonatkozik, amelyek a mindennapi működést biztosítják.

Az általam kutatott vállalatok mindössze 40%-a hallott az üzleti folytonosság (business continuity) és a válságkezelés (crisis management) tervezéséről, végezetül csak 25%-uk rendelkezik vállalati szintű stratégiai tervvel ezen a téren.

Ezt a témát érdemes gyakorlati szempontból megközelíteni, elgondolkodtatni, esetleg kapaszkodót adni az első lépések megtételéhez.

Az üzleti folytonossági irányítás nem más, mint a folyamatos vállalati működés biztosítására való felkészülés, hatáselemzés:

- Csökkenteni a rendkívüli események lehetőségét és/vagy hatását. Lásd korábbi fejezetben!
- Biztosítani, hogy a vállalat rendelkezzen egy előre meghatározott tervvel, ha bekövetkezik a rendkívüli esemény.

Miért van szükség az üzleti folytonossági tervre?

- A vállalat irányításának meghatározó része.
- Stratégiai kockázatként azonosítható a terv hiánya.
- Válsághelyzeteknek van reális előfordulási valószínűsége.
- Vállalati elkötelezettség a megrendelők, üzleti partnerek felé, hogy a folyamatos működés biztosított.

⁷ CSIKÓS–LÉVAI 2007, 9–13.

Nem látok megkötést arra nézve, hogy milyen típusú vállalatoknak van szüksége az üzleti folytonosság és a válságkezelés tervezésére, hiszen működési kockázattal számolhat az egyéni vállalkozó, a kis, a közép- és a nagyvállalat is. Hiszem azt, hogy az írásos tervezés azoknál a vállalatoknál célszerű, amelyek nagysága, struktúrája, tevékenységi köre ezt indokolja.

Megkülönböztethetünk belső és külső fenyegetéseket, mint emberi mulasztás, tűz, természeti katasztrófa, vegyi robbanás, baleset, bűncselekmény stb.

Szeretnék kiemelni azonban 3 területet, amelyet egyfajta összefoglalónak is tekinthetünk:

- objektum elvesztése;
- meghatározó beosztású személy elvesztése;
- informatikai rendszer elvesztése.

A terv elkészítésénél a következő „arany szabályok” figyelembevételét javaslom:

- ne bonyolítsuk túl a tervet;
- legyen könnyen megérthető;
- ne legyen túladminisztrált;
- a további, szükséges munkákat minimalizáljuk;
- a vállalat működése szempontjából globális megközelítés szükséges;
- biztosítani kell a terv fenntarthatóságát folyamatos frissítésekkel.

A tervet érdemes tesztelni, amelynek 4 lehetséges változatát jelölném meg:

1. Áttekintés: ez a terv egyszerű áttekintése, része lehet egy megbeszélésnek, tartalma 1 óra.
2. Részleges gyakorlat: ez a terv gyorsabb tesztelését jelenti, alaposabb előkészítést igényel, tartalma 2–4 óra.
3. Szimuláció: ez a gyakorlat mintázza a rendkívüli eseményt, hogy minden fontosabb folyamat a helyén legyen. Ez a tréning inkább tekinthető üzleti folytonossági, mint válságkezelési gyakorlatnak, tartalma 4–6 óra.
4. Teljes ellenőrzés: ez a gyakorlat bevon minden érintett csoportot, biztosítja, hogy minden folyamat a helyén legyen. Ez a tréning inkább tekinthető válságkezelési, mint üzleti folytonossági gyakorlatnak, tartalma 1 nap.

A vállalat vezetése részéről célszerű kijelölni elsődleges és másodlagos objektumokat mint irányítási pontokat, biztosítva ezekben az alapvető irányítási eszközöket, mint bútorzat, telefonok, fax, internetkapcsolat, számítógép, televízió, videó, térképek, tervrajzok stb.

Kihívást jelent a terv kivitelezésével és fenntartásával kapcsolatban:

- a vezetőség elkötelezettségének elnyerése;
- esetenként nehézkes az időpont egyeztetése;
- felelősök, helyettesek kijelölése;
- kétnyelvű kommunikáció a vállalati kultúrának megfelelően;
- személyi mozgások figyelemmel kísérése, a terv frissítése.

Összegzésképpen: az üzleti folytonosság és a válságkezelés tervezése akkor működik, ha az első számú vezető elkötelezett ezen a téren. Szükséges a projektvezető „MOTOR”

szerepe, a találkozók alapos előkészítése, hiszen ez a kérdés nem biztonsági, hanem alapvetően vállalati döntés és érdek.

6.9.3. Kapacitásterv

Ebben a metódusban, amely tulajdonképpen egy funkcionális tervezés, minden funkció teszi a maga dolgát, tervezi az éves cselekvési programját, tervezi ehhez a költségvetését, és egyeztet a vezérigazgatóval, esetenként anyaországbeli szakmai vezetőjével.

A nagyvállalatoknál komoly stratégiai tervezés tapasztalható, amikor a funkcióvezetők az elmúlt év pénzügyi eredményadatai és a jövő év költségvetési kihívásai alapján közösen meghatározzák a vállalati stratégiai irányokat. Sok esetben elvonulnak – akár többnapos – stratégiai tervezésre, külső helyszínre. Ennek rendelik alá saját funkcionális terveiket, ennek megfelelően tervezik a költségvetést, a létszámot.

A biztonsági vezetőnek fontos ismernie ezeket a stratégiai irányokat, újításokat, valamint az egyes területek időszakos leterheltségét, mert ezek ütközése nagyon sok probléma forrása lehet. Okozhatnak extra költségeket, túlfeszített osztályokat, ott pedig megnövekedett betegséget, fluktuációt, ami az elkötelezettség elvesztésének, gyengülésének a jele, és meg is érkeztünk a visszaélések lehetőségéhez. Ne felejtjük tehát el, hogy a nagy magasságokból időnként le kell szállni, hogy közelről is tudjuk szemlélni a működést, és néha hátra is léphetünk egyet, ha a folyamatok azt igénylik.

6.10. Riportok

A hatékony és modern biztonsági vezető részben elemző, analitikus típus is. Rendelkezik a működéséhez és a vállalati eredményesség megértéséhez szükséges riportokkal, adatokkal, statisztikákkal. Amennyiben rendelkezésre állnak, szerezzük be az európai országok összehasonlító adatait, és lehetőleg a nagyobb képből közelítsünk a kisebb felé.

Biztonsági területhez kapcsolódó riportok lehetnek: bűncselekményi adatok, biztonságtechnikai működés adatai, meghibásodások, karbantartási igények, költségek, vagyonőri szolgáltatás adatai, biztonsági ellenőrzések adatai.

Üzleti jellegű riport lehet – persze ezek nagyon eltérőek – a banki, ipari és kereskedelmi ágazatban: árbevétel, eredményesség, veszteségi adatok és ezek mély elemzése. Költségek árbevételhez viszonyított százalékos nagysága, mennyi például a bérjellegű kiadás, a logisztika költsége, és mennyi a kontroll költsége. Ha a kontroll, azaz a biztonsági működésre fordított teljes költség megfelel például az európai vagy az anyaországbeli százaléknak, az lehet jó, különösen akkor, ha a releváns veszteségi adatok kisebbek.

A gond akkor kezdődik, ha elkezd nőni a vállalat vesztesége, mert akkor mindenki a biztonsági vezetőre néz és akár mutogat is. Nehéz időszak ez, ekkor kell nagyon naprakészen ismerni a funkciók működését, éves tevékenységét, hivatalos és nem hivatalos működési megoldásait, a riportok adatait. A legjobb gyakorlat az, ha a biztonsági vezető képes reális képet adni a tényekről, prioritásokat állítani, és a többi vezetővel közösen kialakítani az akciótervet. Ezzel is részletesen foglalkozott az előző fejezet.