M Ű E G Y E T E M **1 7 8 2**

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék

BIZTONSÁG MENEDZSMENT KUTATÓ CSOPORT

VASVÁRI GYÖRGY CISM tiszteleti egyetemi docens (témavezető)
LENGYEL CSABA a KELER Rt. biztonsági vezetője
VALÁDI ZOLTÁN a GIRO Bankkártya Rt. informatikai biztonsági vezetője

A BIZTONSÁGSZERVEZÉS ÉS AZ EGYÉNI ÉRDEKEK ÜTKÖZÉSE

1.7

2006

Észrevételeket, javaslatokat tettek a vitára bocsátott anyaghoz:
Erdősi Péter CISA,
Sántha Péter szakértő
a Kutató Csoport tagjai.

TARTALOMJEGYZÉK

1. Bevezetés 4
1.1. A munkavállaló egyéni érdekei 4
1.2. A munkavállaló személyiség jegyei 5
1.2.1. A munkakörből fakadó érdekek. 5
1.3. A biztonság szervezés és az egyéni érdekek ütközése 5
2. A biztonságszervezés hatása a vállalat munkatársaira. 6
2.1. A biztonsági infrastruktúra függetlensége 7
2.2. A biztonsági alrendszerek átfedése az egyenszilárdság elve értelmében. 8
2.3. A „szükséges tudás elvének követelménye a hozzáférési jogosultságok meghatározásánál. 8
2.4. A biztonsági kiadások, és a költségeik 9
2.5. A biztonsági követelmények érvényesítése a nem biztonsági intézkedéseknél. 9
2.5.1.Szabályozásoknál 9
UTASÍTÁSOK 10
SZABÁLYZATOK 10
ELJÁRÁS RENDEK 10
3. Javaslatok az ellenérdekeltség kockázatának csökkentésére. 11
3.1. A biztonsági tudatosság erősítése 11
3.2. A kompenzálás. 11
3.3. Anyagi érdekeltté tétel. 12
4. A szociálpszichológiai megközelítés 12
4.1. Elemzés 12
4.2. Teendők 16
5.Csökkenthető-e az érdek ütközések kockázata? 18

1. Bevezetés

A gyakorlati biztonságszervezési tapasztalatok számtalan példát szolgáltattak arra, hogy a biztonsági átvilágítás során az egyes veszélyforrások feltárása konfliktus helyzetet teremt a biztonságszervező és az átvilágított vállalat egy vagy több munkatársa között. Hasonló tapasztalatok jelentkeztek a biztonságszervező védelmi intézkedési javaslatainak a megrendelő munkatársai részéről megnyilvánuló fogadó készségénél.

Érdekes módon a konfliktusok közül egyesek a szakmai indokok ismertetésével feloldhatóak voltak, míg más esetekben érezhetően a konfliktus nem oldódott fel, csak egy felszínes alkalmazkodás volt észlelhető a vállalat által elfogadott javaslattal szemben.

A konfliktus okait keresve az a következtetés adódik, hogy a munkavállalók egyéni érdekei sérültek, sérülhetnek a megállapítások és javaslatok felvetése, még inkább a vállalat részéről történő elfogadása esetén.

Felmerül a kérdés, vajon egy vállalat üzleti érdekei halmazának részben vagy egészben eleme-e a munkavállalók egyéni érdekeinek halmaza? A továbbiakban arra fogunk rámutatni, hogy csak részben eleme.

1.1. A munkavállaló egyéni érdekei

A vállalatok azért alkalmaznak munkavállalókat, hogy azok a vállalat erőforrásait felhasználva, hatékonyan és eredményesen megvalósítsák a vállalat küldetését. Természetesen a munkavállalóktól elvárják, hogy tevékenységüket az üzleti cél irányítsa, és azt teljesen tegyék magukévá. Ennek érdekében az anyagi érdekeltté tételtől kezdve, az oktatáson, meggyőzésen keresztül, valamint a munkaszerződés megkötésekor, illetve a munkavállaló feladatainak a meghatározásakor, a munkaköri leírásának átadásakor (módosításakor), vagy a teljesítménykövetés módszerének alkalmazásával, a vállalatok legkülönbözőbb eszközöket veszik igénybe. Mindez arra mutat, hogy a munkavállaló egyéni érdekei nem azonosulnak automatikusan a vállalat üzleti érdekeivel. A munkavállalással együtt a munkavállaló nem feltétlenül ismeri meg és fogadja el a vállalat érdekeit, tehát az érdekütközés eredhet tudatlanságból is. A vállalat eszközei ennek a tudatlanságnak a felszámolására is kell, hogy irányuljanak.

1.2. A munkavállaló személyiség jegyei

Az egyéni érdekeket alapvetően a munkavállaló személyiségjegyei alakítják ki. Az adott téma szempontjából ezek közül ki kell emelnünk az érvényesülés (beosztás, szakmai karrier) iránti vágyat, a foglalkoztatása biztonságának igényét, a nehezen nélkülözhető munkatársként kezelés iránti igényt. Továbbá van olyan munkavállaló, akinek „a kis feladat, kis felelősség, biztos fizetés" az elfogadható.

Ezek a személyiségjegyek az egyéni érdekekben jutnak többek között kifejezésre, amelyeknek azonban a vállalat üzleti érdekeinek elméletben nem szabad ellentmondaniuk. A személyiségjegyek az egyes munkavállalóknál nem azonosak, vagy nem azonos mértékben vannak jelen, ennek következtében a személyiségjegyekből fakadó érdekek érvényesítése iránti elszántság, törekvés sem azonos mindenkinél. Természetesen egyes munkakörökben eltérő személyiségjegyek lehetnek kívánatosak, tehát ez nem azt jelenti, hogy létezik abszolút megfelelő személyiségjegyű optimális munkavállaló.

1.2.1. A munkakörből fakadó érdekek

A munkakörnek, azaz a munkavállaló feladat és felelősségi körének, hatáskörének összhangban kell lennie mind a munkavállaló egyéni érdekeivel, mind pedig a vállalat érdekeivel.

A fentiekben megfogalmazott érdekeket még a témánk szempontjából a következők egészítik ki (nem preferencia sorrend):

- a tevékenysége elfogadottságának igénye (ide értve a munkaköri tevékenység hozzájárulását a vállalati célok eléréséhez),
- az anyagi elismerés iránti igény,
- az egyedi hatáskör iránti igény,
- a vállalat ügyeiről a jól értesültség igénye.

1.3. A biztonság szervezés és az egyéni érdekek ütközése

A biztonságszervezés gyakran olyan megállapításokat tesz, illetve olyan intézkedéseket javasol, amelyek a munkavállaló tényleges vagy vélt egyéni érdekeivel ütköznek.

Ezek közül tipikusak a munkavállaló

- önállóságát (hatáskörét) csorbító,
- a fennálló alárendeltségi viszonyát megváltoztató,

- a megfelelni akarásának lehetőségeit, a lojalitási képét rontó,
- az anyagi érdekeit sértő

biztonságszervezési intézkedések.

Ez a helyzet biztonsági szempontból veszélyforrást képezhet az adott munkavállaló érdekérvényesítési törekvései függvényében, és tiltakozáshoz vagy a védelmi intézkedések nem rendeltetésszerű végrehajtásához vezethet, azaz részben vagy egészben nem kényszeríti ki az üzleti érdekeket realizálni hivatott biztonsági követelményeket.

Az érdekütközés olyan munkatársaknál jöhet létre, akik valamilyen felelősséget viselnek a biztonságért. Így a vállalat gazdasági szervezetének biztonságért egy személyben felelős első vezetője és az alá közvetlenül tartozó biztonsági szervezet tagjai között. Továbbá az új szereplők között, ha a vállalatirányításon belül a biztonság irányításért felelősök kibővülnek a biztonsági stratégiáért felelős bizottsággal, a humán politikai és munkaügyi szervezet tagjaival, a gazdasági és adott esetben egyes pénzügyi számviteli munkatársakkal. Ezek és a vagyon, illetve az informatikai biztonsági intézkedések érintettjei, a felhasználók lehetnek azok, akik valamilyen módon biztonsági ügyekben illetékességgel bírnak. Kulcskérdés, hogy a biztonsági tudatosságuk, a veszélyérzetük megfelelő színvonalú-e. Természetesen az adott szituáció, amely szervezetenként igen változatos lehet, és ez módosíthatja az esetleg érintettek körét. Ebből viszont az következik, hogy a biztonság iránti fogadókészség általános vállalati színvonala eldöntheti, hogy ki az, aki érdekütközés helyzetébe kerül.

2. A biztonságszervezés hatása a vállalat munkatársaira

A biztonságszervezés egy ismert folyamat, amelynek során meghatározásra kerülnek

- a veszélyforrások,
- kockázatok,

majd ezek alapján

- a védelmi intézkedések,
- a biztonsági dokumentumok.

Az érdekütközés fellépése a kockázatkezelés melléktermék. Célszerű ezért elsősorban azokkal foglalkozni, amelyek egyértelműen felvethetik az érdekütközés kockázatát. Ezek azok a veszélyforrások, illetve

védelmi intézkedések, amelyek közvetlen kapcsolatban állnak a humán erőforrásokkal. Az alábbiakban a védelmi intézkedésekből vizsgálunk néhányat, amelyeket természetesen megelőzött az azonos témákban feltárt gyengeségek és veszélyforrások a vállalat munkatársaival való megvitatása.

2.1. A biztonsági infrastruktúra függetlensége

A biztonsági szervezetnek a vállalat minden más szervezetétől függetlennek kell lennie. Ezt mondja ki a feladat szétválasztás elve (segregation of duty). A megfelelő biztonsági követelmény szerint (lásd például COBIT 3) a biztonsági és egyéb informatikai vagy üzleti feladatokat, munkaköröket azonos személy nem tölthet be.

Ennek alkalmazása esetén

- a biztonsági szervezet (vagyon, üzem, illetve informatikai biztonsági) egy biztonsági vezető alá, és annak közvetlenül a vállalat első vezetőjének alárendeltségébe kell, hogy tartozzon,
- nem lehetne biztonsági feladata például az információ rendszerekben oly fontos rendszergazdáknak.

A fenti esetekben érdekütközés kockázata áll fenn, mivel eredendően a vállalati szervezetekben külön szervezetbe tartoztak a vagyon és az informatikai biztonsági szervezetek. Ezen belül is tipikus a rendészeti feladatokat ellátók (kékgallérosok) és az informatikusok (fehérgallérosok), ezen belül is az informatikai biztonsággal foglalkozók ellentéte, illetve a biztonsággal foglalkozók általános lenézettsége.

A korszerű követelményeknek eleget tevő biztonsági szervezet létrehozása együtt jár azzal, hogy integrált biztonsági szervezetre van szükség, amely a korábbi vezetők érdekeit sértheti.

Az információ rendszerben például a rendszergazdák feladatainak a biztonsági feladatokkal történő csökkentése a hatáskörüket egy fontos tevékenységben, a beleszólási lehetőségükben csökkenti.

Megjegyzés: a biztonsági feladatok rendszergazdákról történő leválasztása sokszor csak korlátozott mértékben valósítható meg, ezért ilyen esetekben különösen nagy gondot kell fordítani az audit naplók működtetésére, így biztosítva a rendszergazdai tevékenységek nyomonkövethetőségét.

2.2. A biztonsági alrendszerek átfedése az egyenszilárdság elve értelmében

A vagyonbiztonsági rendszerben a fizikai biztonsági berendezéseket, az épület automatikát, a videó-, hang- és adattávközlést egy információ rendszer fogja össze egy intelligens épületben, míg az információ rendszer környezetében a belépés és mozgás ellenőrzés fizikai biztonsági eszközökkel történik. A vagyonbiztonsági és az informatikai rendszerek tehát átfedik egymást, azaz a vagyonbiztonsági rendszerrel foglalkozók az informatikai biztonság területén, míg az informatikai biztonsággal foglalkozók a vagyonbiztonság területén kell, hogy hatáskörrel, feladatokkal rendelkezzenek az egyenszilárdság elve és a meg nem kerülhetőség érvényesítése mellett. Ez a gyakorlatban azt jelenti, hogy a két szervezet munkatársai mind a két területen jelen vannak, és kölcsönösen hatáskörrel intézkedhetnek, amennyiben a megfelelő szakértelem rendelkezésükre áll.

- A leírt esetben hatáskört, illetve feladatkört vesznek el és adnak is a vagyonbiztonsági és informatikai biztonsági vezetőknek, ezáltal az üzleti rendszer és az információ rendszer vezetői és munkatársai érintettek lehetnek. Ez jelentősen sértheti az érdekeiket.

  Megállapíthatjuk tehát, hogy a feladatszétválasztás elvének érvényesítése elsősorban a hatáskörök csökkenéséhez vezet, azaz hatalmi pozíciókat zavarhat meg, és a biztonságszervezés megvalósulása számukra eddig természetesen hozzáférhető biztonsági események ismereteinek korlátozását eredményezheti.

2.3. A „szükséges tudás elvének követelménye a hozzáférési jogosultságok meghatározásánál

Az információs rendszerben, hagyományosan a logikai hozzáférési jogosultságok megadásánál, a hierarchia szerinti jogosultság elvét alkalmazták, amikor is a betöltött munkakör, pozíció minnél magasabban volt a szervezetben, annál nagyobb betekintési, módosítási stb. jogosultságot kapott az illető vezető. Ez azonban nem felel meg annak a ma vallott bizalmasságra vonatkozó alapelvnek, hogy valamiről csak az tudhat, akinek arra a munkája ellátásához szüksége van, ami természetesen a hozzáférési jogosultságok kemény korlátozásával érhető csak el. A „szükséges tudás elve” kimondja, hogy arra kell jogosultságot adni, ami valakinek a feladatkörébe tartozik, és a jogosultság a munkája elvégzése érdekében szükséges. Így a logikai hozzáférés-védelem érdekében a hozzáférési jogosultságot egy meghatározott tevékenység elvégzésére az kaphatja meg, akinek az a

munkaköri leírásából következően feladatai ellátáshoz szükséges. Természetesen ehhez napra kész munkaköri leírások szükségesek. Egy biztonság érzékeny adatokkal, alkalmazásokkal dolgozó cégnél az eljárás ennél szigorúbb. Az adatok és az alkalmazások, valamint a hozzáférési jogosultsággal rendelkezők és a hozzáférés során végezhető tevékenységeik osztályozva vannak biztonság érzékenységük szerint. A hozzáférés, majd egy tevékenység elvégzése csak akkor lehetséges, ha a hozzáférési jogosultsággal rendelkezők biztonság érzékenysége legalább egyező, illetve nagyobb, mint az adatok és az alkalmazások biztonsági érzékenysége.

- Természetesen a munkatársak hatáskörét, elfogadottságukról, fontosságukról alkotott képüket, jól értesültségük iránti igényüket sértheti, sérti ez a hozzáférési jogosultságaikat korlátozó biztonsági követelmény (természetesen a fizikai hozzáféréseknél, például a biztonság érzékenységük szerint osztályozott helyiségekbe történő belépési jogot is korlátozni kell).

2.4. A biztonsági kiadások és költségek

A biztonság megteremtésének, fenntartásának a költségei, a kiadások az általában költségérzékeny vezetőkkel és a gazdasági terület munkatársaival szemben okozhatnak ütközést, különösen, ha a biztonságért felelős első számú vezető döntése nem az ő „szájízük" szerint való. Döntő tehát az, hogy például a tulajdonosok, az őket képviselő igazgatóság, felügyelő bizottság és a felső vezetők mennyire elkötelezettek a biztonság irányában. Egyértelművé kell tenni, hogy egy gazdasági kérdésben, amennyiben az a biztonságot érinti, a költséget igénylő biztonsági intézkedés megtétele, vagy elutasítása, milyen kockázatokkal járhat. Tudomásul kell vetetni, hogy a kis költségek eleve nagyobb kockázatokat jelentenek. Tehát a döntéshozónak, elutasítás esetén, a kockázatot is vállalnia kell.

2.5. A biztonsági követelmények érvényesítése a nem biztonsági intézkedéseknél.

2.5.1. Szabályozásoknál

A gazdasági szervezeteknél alkalmazott szabályozások jelentős része biztonságérzékeny (a biztonságérzékenység azonban nem a dokumentumok hozzáférhetőségének korlátozását, hanem az adott szabályozás biztonsági összefüggéseit jelenti). Ezek közül kiemeljük a következőket:

UTASÍTÁSOK

Humán Politika
Titokvédelmi Utasítás
Iratkezelési Utasítás
Selejtezési Utasítás
Tűzvédelmi Utasítás
Munkavédelmi Utasítás
Outsourcing Utasítás

SZABÁLYZATOK

Adatvédelmi és Adatbiztonsági Szabályzat
Biztonsági Szabályzat (Politika)
Üzletmenet Folytonossági Terv
Működési Szabályzat
Fejlesztési Szabályzat
Beszerzési Szabályzat
Vírusvédelmi Szabályzat

ELJÁRÁS RENDEK

Üzemeltetési Eljárás Rend
Jelszó és Jogosultság Kezelés Rendje
Alkalmazások Eljárás Rendjei (mentési és újraindítási rend beleértve)
Szoftver Verzió váltások Eljárás Rend
Help Desk Eljárás Rend
Hardver és Szoftver Nyilvántartási Rend
Szoftver Licensz Nyilvántartási Rend
Program Változás Kezelés Rendje
Hálózat Üzemeltetés Eljárás Rend
Levelek Elektronikus aláírásának és Titkosításának Rendje
Internet Hozzáférés Rend
Védelmi Intézkedések Nyilvántartási Rendje
Konfiguráció Kezelési Rend
Átadás/átvételi Eljárási Rend

A független biztonsági szervezetnek el kell érnie, hogy a gazdasági szervezet a fenti utasításokat, szabályzatokat, eljárásrendeket elfogadja, amelyekkel szemben természetesen hatályba léptetésük előtt a gazdasági szervezetnek hozzászólási és vétó joga van. Látni kell, hogy itt a vállalat biztonsági követelményeinek érvényesítéséről van szó,

feltételezve azt, hogy ezek a dokumentumok figyelembe veszik az üzleti érdekeket. Ugyanis, amennyiben ellentmondanak az üzleti érdekeknek, a szervezet felső vezetőjének joga és felelőssége, hogy döntsön a biztonsági követelmények figyelembe nem vételéről, vagy azok más, gyengébb formában való érvényesítéséről. Ebben az esetben arról van szó, hogy a felső vezető vállalja a döntésével járó felelősséget.

Ez a téma, mint az előbbiek is, egyaránt szól mind a két biztonsági alrendszerről.

- A gazdasági szervezet érvényesíthető véleményezési joga sértheti, sérti egyrészt a szabályzatok készítőinek egyedi hatáskör iránti érdekeltségét, másrészt különböző módokon a szabályzatok végrehajtóinak, alkalmazóinak, érdekeit is (lásd 2.5.1.).

3. Javaslatok az ellenérdekeltség kockázatának csökkentésére

3.1. A biztonsági tudatosság erősítése

Alapvető intézkedés a biztonsági tudatosság megteremtése, erősítése, amely nélkül minden további intézkedés céltalan. Ugyanis a veszélyforrások felismerése (a veszélyérzet), a védelmi intézkedések elfogadása még abban az esetben is alapvető kérdés, ha az ütközik az adott munkatárs tényleges vagy vélt érdekeivel. Ettől függ, hogy az adott munkatárs érdekei érvényesítése céljából tesz-e valamit, illetve mit tesz. Az érdekérvényesítés kockázatot jelent tehát a vállalat biztonsága szempontjából, amelyet például maga a munkatárs is mérsékelhet a biztonsági tudatossága hatására. Ide tartozik az is, hogy a munkavállalóval adott esetben a saját védelmét szolgáló védelmi intézkedések elfogadtatása is feladatot, problémát jelenthet. E tekintetben tehát alapvető a biztonság általános tudatosításának a színvonala, a védelmi intézkedések indokoltságának a megértése, konkrétan például a feladat szétválasztás, vagy a szükséges tudás elve, aminek az elfogadását széleskörű oktatás segítheti elő.

3.2. A kompenzálás

Az 1.2 pontban megadott érdekek vélt vagy tényleges sérelmét, kompenzáló intézkedéssel lehet csökkenteni. Azaz elvont hatáskör esetén más, nem biztonsági hatáskör adása, vagy az adott munkatárs szakmai, vezetői elfogadottságának bizonyítása a menedzsment részéről (például vezetők esetében valamely, a vállat irányításával foglalkozó bizottságba történő bevonás) elegendő lehet a munkatárs számára.

3.3. Anyagi érdekeltté tétel.

Adott esetben, amennyiben az érdeksérelmet az anyagi érdekeltség a munkatársnál „felül írja”, a jutalmazás a biztonsági intézkedések sikeres végrehajtáshoz kötve, eredményes lehet.

4. A szociálpszichológiai megközelítés

4.1. Keresztösszefüggés

A gazdasági szervezetek üzleti céljaikat, az üzleti követelményeket az üzleti és informatikai folyamatokkal kívánják hatékonyan és eredményesen megvalósítani. Ezeknek a folyamatoknak egyik erőforrása az ember. Ebből következik, hogy a humánpolitikai folyamatok átfedik az üzleti és informatikai folyamatokat. Keresztösszefüggések alakulnak ki. Témánk tehát szükségessé teszi a biztonsági, védelmi intézkedések humánpolitikai megközelítést is. Mindebből következik, hogy szociálpszichológiai megközelítés szükséges az érdekütközések hátterének, okainak elemzéséhez, a teendők meghatározásához.

4.2. Elemzés

Az érintettek a biztonsági intézkedéseket a privát szférájukba való behatolásként értelmezik, sokan mások, pedig személyes sértésnek veszik. Az alábbi felsorolást tartalmazza az alapvető emberi típusokat:

- notórius szabálykerülő - "Nekem senki ne mondja meg, hol gyújtsak rá!"
- tesztelő - "Biztos csak ijesztgetnek azokkal a füstérzékelőkkel."
- nemtörődöm - "És akkor mi lesz, ha rágyújtok?"
- a rácsodálkozó - "De hát nekem senki nem mondta, hogy itt nem lehet."

A problémák az emberek társadalmi és szociális természetéből fakadnak, abból az alapigazságból, hogy a biztonság érdekeket sért.

A biztonsági szabályzások és eljárások nem csak arra vannak hatással, hogy az emberek mit tesznek, hanem arra is, hogyan látják magukat, a kollégáikat, a világot.

Mindezek ellenére a biztonsággal foglalkozók egyáltalán nem, vagy csak kevés figyelmet fordítanak arra, amit mindannyian olyan jól ismerünk, a szociálpszichológiára.

A társadalmi viselkedés szabályainak ismerete sok segítséget nyújt a biztonsági eljárások bevezetése során. Sok esetben a biztonság inkább az emberen múlik, nem a technológián. Ezért az alkalmazottak sokkal nagyobb veszélyt jelentenek a vállalatra nézve, mint a szervezeten kívüliek.

A szociálpszichológiai megfigyelésekből következik, hogy a biztonság növelése szükségszerűen magában foglalja a viselkedési formák, meggyőződések, attitűdök megváltoztatását mind az egyénekre, mind a csoportokra vonatkozóan.

A szociálpszichológia segítséget tud nyújtani abban, hogyan kezeljük az emberi részrehajlást, hajlamot céljaink elérése érdekében:

- A kutatások arra fókuszálnak, hogy az emberek hogyan alakítják a valóságról alkotott képüket. Ismerve ezeket az elveket, nagyobb hatással lehetünk ügyfeleinkre és munkatársainkra. Figyeljünk másokra!

- Ha a meggyőződések és álláspontok formálásán dolgozunk, hatékonyabban tudjuk rávenni az egyéneket, hogy kooperáljanak a cél elérése érdekében
  Kommunikáljunk!

- Olyan környezetet kell kialakítani, hogy a munkatársak a vállalati információt akaratlagosan, meggyőződésből óvják.
  Motiváljunk!

- Csoportokkal foglalkozni sokkal eredményesebb, mint az egyének ellenállását áttörni.
  Rendszerszemlélet - ISMS!

Az informatikai biztonsági eljárások sokszor erős érzelmi viharokat korbácsolhatnak. Az emberek könnyen mérgessé válnak, ha úgy érzik fölöslegesen felforgatják a jól bevált, megszokott munkamódszereiket. Ez odáig is vezethet, hogy a szabályok módszeres megkerülésével aláássák a biztonságot.

A már meglévő, kikényszeríttet vagy új biztonsági szabályokkal - és nem utolsó sorban az ezeket betartatni igyekvő kollégákkal - szemben paranoiás ellenállás alakulhat ki.

Ezeket a konfliktusokat az addig elfogadott magatartási normák, megváltozása szüli. Nem a biztonsági szabályokat kell ezekhez igazítani,

hanem az elfogadott normákat kell úgy megváltoztatni, hogy összhangba kerüljenek a biztonsági elvárásokkal.

Ezek a képek, sémák alakítják ki a valóságról alkotott elképzeléseket. Ezek segítenek abban, mi fontos, és mi irreleváns. Ezek a sémák teszik lehetővé, hogy tudjuk, miként kell viselkedni egy adott szituációban. Sajnálatos módon a biztonsági szabályozások és eljárások konfliktust okoznak a legtöbb ember fentiekhez hasonló, kialakult viselkedésformáival. A biztonságot a vállalati kultúra szerves részévé kell tenni! A szervezeteken belüli kooperációt leginkább akadályozó tényező az interperszonális konfliktus. A legtöbb konfliktus gyökere a személyiség jegyek, eltéréséből adódik. Az alábbi széleskörűen használt kategóriák (személyiség típusok) segíthetnek a személyiségek ábrázolásában, ahol a magas és az alacsony azt jelenti, hogy a személyiség típusok mennyire erőteljesen (nagyon, kevéssé) jellemzik az illető személyt.

Kifelé fordulás (extrovertizmus)

Magas (pozitív): aktív, energikus, beszédes, öntudatos, társaságkedvelő
Alacsony (negatív): csendes, visszahúzódó, félénk, zárkózott

Kedvesség

Magas: rokonszenves, megnyerő, lágyszívű, méltányos, szeretetteljes
Alacsony: hideg, keményszívű, barátságtalan, civakodó, kötözködő

Lelkiismeretesség

Magas: szervezett, tervszerű, hatékony, felelős, alapos
Alacsony: frivol, felelőtlen, figyelmetlen, fegyelmezetlen, hanyag

Érzelmi stabilitás

Magas: stabil, higgadt, elégedett, szenvedélymentes
Alacsony: aggódó, ideges, gondterhelt, görcsös

Nyitottság és kulturáltság

Magas: intelligens, eredeti, érdeklődő, ötletes
Alacsony: közhelyes, unintelligens, szűklátókörű, felszínes

A jellemvonásokhoz tartozó jelzők a "magas" oldalon pozitivizmust, az "alacsony" oldalon, pedig negatívizmust sugallnak. A "magas" és "alacsony" karakterek közötti interferencia hat zavarólag a kollégák

közötti kommunikációban. Bemutatjuk például, hogy az "alacsony" személyiségjegyű ember hogyan, látja a fent felsorolt kategóriák jellemzőit:

Kifelé fordulás (extrovertizmus)

Magas: ideges, agresszív, nyomuló, ingerlékeny, pletykás
Alacsony: tisztelettudó, méltóságteljes, önálló, figyelmes

Kedvesség

Magas: kritikátlan, ragaszkodó, érzelgős, tökkelütött
Alacsony: analitikus, racionális, méltóságteljes, elvekkel bíró

Lelkiismeretesség

Magas: megrögzött, kényszeredett, alázatos, fontoskodó
Alacsony: szabad, spontán, kreatív, fiatalos, vicces

Érzelmi stabilitás

Magas: fagyos, unalmas, ambíció nélküli
Alacsony: vibráló, romantikus, erős, ésszerű

Nyitottság és kulturáltság

Magas: teoretikus, dilettáns, komplikált
Alacsony: anyagias, okos, praktikus, fókuszált, alapos

A konfliktusok a fenti a kategóriák értelmezésének felfogásbeli különbözőségéből adódnak. Az ellentét a személyiségbeli stílusok különbségéből eredeztethető, nem pedig a problémák megértésének eltéréséből. Nem mindenki konfrontálódik azonnal ilyen helyzetekben. Megoldás lehet, ha egy problémával a humán felelőshöz lehet fordulni.

Általában a szabályozások mögötti háttér megismerése, a dolgok miértjének és mikéntjének megfelelő kommunikálása segít a viselkedésmód megváltoztatásában. A reakciók megfigyelése mindig kifizetődőbb a parancsnoklásnál!

Az emberek általában a másik viselkedését két független dimenzió mentén ítélik meg: **Kifelé forduló** (extrovertált) - **befelé forduló** (introvertált) **Stabil** – **ingatag**. Példaként néhány jellemzés, hogy "Katika" miért felejtette bejelentkezve a gépét már negyedszer a héten:

- Befelé forduló, stabil - "Ő már csak ilyen, soha nem figyel a szabályokra."
- Befelé forduló, ingatag - "Nagyon feszült mostanában, mert a gyereke beteg, ezért felejthette úgy a gépet."
- Kifelé forduló, stabil - "A rendszer nem válaszol a kilépés funkcióra."
- Kifelé forduló, ingatag - "A héten a rendszer nem válaszolt megfelelően a kilépés parancsra."

Minden emberi viselkedésnek (magatartásformának) megvan az indoka, és erre a szociálpszichológia ad választ.

4.3. Teendők

Egy hatékony biztonsági program szociálpszichológiai elemei:

- a cégújság, intranet adta lehetőségeket kell kihasználni - információ biztonsági rovat
- küldjön rendszeresen biztonsági figyelmeztetéseket
- minden kiadott új eljárást kommentáljon - Miért szükséges? Mit érint? Milyen hatása lehet?

Egy biztonsági menedzsernek értelmeznie kell a körülötte zajló eseményeket, értenie kell azok hátterét, és ennek érdekében érdemes pszichológiai ismeretekkel is felvérteznie magát.

- Az előzetesen kapott információk befolyásolják az emberek reakcióit a később kapott ismeretekre vonatkozóan. A biztonságtudatosság növelésének előkészítéseként mutassunk be megtörtént eseteket, történeteket. Ezek befolyásolják a kollégák hozzáállását a biztonsági követelményekhez.
- Figyeljünk arra, hogy ezeket a példákat a legszélesebb körből vegyük. Életszerűbb, ha nem egy vállalatra, üzleti szegmensre koncentrálunk. Mutassuk be, hogy ezzel a problémával ki mindenki kerül szembe, ezáltal csökkenthetjük az ellenállást.
- Vigyázzunk a szavakkal! Ha kockázatokról és veszélyforrásokról beszélünk, akkor próbáljuk meg ezeket pozitív környezetben feltüntetni. Emeljük ki a veszélyforrások elkerüléséből adódó pozitív végeredményeket. Az emberek a tényszerű információt nem mindig racionálisan fogadják be. Építsünk a kollégák érzéseire és fantáziájára. Ez nem is olyan nehéz.

A kérdőívek használata nagy segítséget nyújt az ismeretanyag megszerzéséhez. A kérdőívek kiértékelésével csoportokat lehet meghatározni, így hatékonyabban lehet kommunikálni a különböző hozzáállású kollégák felé is.

Az attitűd megváltoztatására vonatkozó legfontosabb motiváló tényezők a jutalom és a büntetés. Sok szervezet a biztonságpolitika megerősítéséhez teljes mértékben a büntetésre és szankcionálásra hagyatkozik, annak ellenére, hogy a pszichológia mai állása szerint a magatartás megváltoztatásának jóval hatékonyabb eszköze a jutalmazás.

Mi történik itt, ha büntetéssel, és mi, ha jutalmazással próbálunk ezen változtatni?

Az egyik osztályon a felelős végigjárta a gépeket és figyelmeztető cetlit hagyott a monitorokon a közvetlen felettes értesítésének kilátásba helyezésével. Egy másik osztályon az ellenőrzéssel megbízott a szabályszerűen kilépett munkaállomások billentyűzetére kis csokit rakott.

Egy hónap után a büntetéssel "motivált" osztályon az arány 50%-ra kúszott fel, míg a "csokis" osztályon 80%-ra!

Fontos a pozitív tónus az üzenetekben. Egy egyszerűen körülírható személyiségtípus kifejezetten gátja lehet a biztonsági eljárások sikerének: a tekintélyelvű, ellentmondást nem tűrő személyiség.

Célokat helyezni egy javaslat elé és ellenérveket is felhozni sokkal hatékonyabb, mint egyoldalú, heves kirohanásokat tenni. Ez a "nem éri meg a kockázatot" technika. Ezen üzenetek mérsékelt ismétlése is pozitívabb válaszokat generálhat kollégáink irányából.

A célközönséggel folytatott kommunikációnak nagy szerepe van a hozzáállás megváltoztatásában. A modern szervezetek esetében a legelterjedtebb eszköz a csapatépítő összejövetelek.

A szemtől szembeni meggyőzés, természetesen nagy szervezetnél kivitelezhetetlen. A döntéshozók legtöbb esetben mindenképpen preferálják.

Nincs annál nagyobb veszély, mint a cég biztonságpolitikáját csoportosan megvitatni a döntéshozókkal. Ismerős lehet mindenkinek az a tapasztalat, hogy az egyik vezető csak azért ellenzi a kérdést, mert egy másik támogatja.

Másfelől a kérdéseket is a megfelelő módon kell feltenni: "Elfogadható számunkra az információ rendszerünk ellen való külső támadás?" Ezek a retorikai kérdések viszont csak akkor hatásosak, ha a mögöttes érvek is erősek. Ellenkező esetben visszafelé sülhetnek el a dolgok. Retorikai kérdés feltevése veszélyes addig, amíg meg nem bizonyosodtunk róla,

A fentiek hozzájárulhatnak, hogy lassan, szinte észrevétlenül átalakuljon a munkatársak attitűdje a biztonsággal kapcsolatban. Hosszan sorolhatnánk, hogy melyek azok a berögzült dolgok, amelyeket érdemes megváltoztatni, hogy nagyobb biztonságban, tudjuk az értékeinket A biztonság tudatosság megalapozása és elmélyítése csak hosszú távú munka eredménye lehet!

5. Csökkenthető-e az érdekütközések kockázata?

Meggyőződésünk, hogy a vállalatvezetés biztonsági tudatossága, érdekeltsége esetén az egyéni érdekeket sértő biztonsági intézkedések is sikerrel vezethetők be. Az előbbiekben javasolt intézkedésekkel (lásd 3. és 4. pontok), annak felismerésével, hogy interdiszciplináris problémáról van szó, a vezetés elérheti az érdek ütközések kockázatainak csökkenését. Ezzel kimondtuk, hogy ez a feladat a vállalatvezetésé, és az érdekütközést a vállaltvezetés oldhatja fel.