BANK TIZIMLARIDA AXBOROT XAVFSIZLIGINI BOSHQARISHNING TEXNIK-TASHKILIY ASOSLARI

Zumrad Zarifova
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Sirojiddin Salimov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Annotatsiya. *Internet va kompyuter texnologiyalarining takomillashuvi xar bir sohada bo‘lgani kabi, moliya va bank sohasida xam ko‘plab yangiliklarni olib keldi. Biroq, texnologik rivojlanishlar ko‘plab afzalliklar bilan bir qatorda xavfsizlik nuqtai nazaridan ko‘plab muammolarni xam keltirib chiqarmoqda. Korxona va tashkilotlarda ularga qarshi qaratilgan ichki va tashqi hujumlar global miqyosida olib qaraydigan bo‘lsak, yiliga trillonlab dollar yo‘qotilishlarga olib kelmoqda. Shu sababli, bank tizimlarida axborot xavfsizligini tartibga soluvchi tizim zarurligi qatiy belgilanmoqda. Ushbu maqolada axborot aktivlari va bank tizimlari uchun potensial tahdidlar, va axborot xavfsizligini boshqarish bo‘yicha keng tarqalgan tizimlar, standartlar va eng yaxshi ishlanmalar keltirib o‘tiladi.*

Kalit so‘zlar: *Axborot xavfsizligini boshqarish, bank korporativ boshqaruvi, axborot xavfsizligini boshqarish asoslari.*

Kirish.

So‘nggi o‘n yilliklarda axborot texnologiyalarining jadal rivojlanishi natijasida, kompyuterlar hayotimizning barcha jabhalarida xususan, biznes, hukumat, ta’lim, moliya, aerokosmik tadqiqotlar, sog‘liqni saqlash sohalaridan tortib mudofaa tizimlarigacha keng qo‘llanilmoqda. Jamiyatning axborot texnologiyalariga qaramligi ortib borayotganligi sababli, kiber jinoyatchilik tahdidi ham ortib bormoqda. Xavfsizlikga tahdidlar va zararli dasturlar global kompaniyalar va tashkilotlarga yiliga trillionlab dollar zararlar keltirmoqda.

Fishing xostingi - kiberjinoyatchilarga soxta veb-saytlarni boshqarish imkonini beruvchi xavfsiz va bardoshli infratuzilma Ushbu saytlar qonuniy platformalarning

sinchkovlik bilan ishlab chiqilgan nusxalari bo‘lib, shubhasiz foydalanuvchilarni parollar yoki moliyaviy ma’lumotlar kabi o‘ta shaxsiy ma’lumotlarni almashish uchun aldashga qaratilgan faoliyat. Jinoiy faoliyat uchun o‘q o‘tkazmaydigan markazni taqdim etgan holda, fishing hosting muvaffaqiyatli fishing hujumlarini osonlashtirishda muhim rol o‘ynaydi.[1]

Axborot tizimlari bugungi kunda butun dunyoda zamonaviy bank faoliyatining yuragi hisoblanib, axborot insayderlar[1], begonalar va raqobatchilardan himoyalanadigan eng qimmatli aktivga aylandi. Mijozlar maxfiylik va shaxsiy ma’lumotlarning daxlsizligiga alohida urg‘u berishadi. Biznes hamkorlar, ta’minotchilar va sotuvchilar o‘zaro aloqada ma’lumotlarning ishonchliligi va xavfsizligini eng yuqori talab deb hisoblashadi. Banklarning muvaffaqiyatlari yangiliklarni o‘zlashtirishi, yangi imkoniyatlar taqdim etishi, qulay va xavfsiz xizmatlarini taqdim etish qobiliyatiga bog‘liq. Axborot xavfsizligini taminlash bozor ulushini va foydani oshiradi. Banklar xodimlar va mijozlar ma’lumotlarning xavfsizligiga javobgar bo‘ladi. Shu sababli, banklar tarmoq orqali sodir etilgan firibgarlik faoliyati uchun ham javobgar bo‘lishlari kerak. Banklar aksar hollarda mijozlarga yo‘qotishlarni qoplashlari kerak, garchi mijoz o‘z hisob ma’lumotlarini o‘zi buzgan bo‘lsa ham. Bugungi kunga kelib ma’lumotlar xavfsizlikni boshqarish bo‘yicha ba’zi tizimlar mavjud bo‘lib, ular Yevropa ittifoqi mamlakatlari va Amerika Qo‘shma Shtatlari kabi rivojlangan mamlakatlarda ishlab chiqilgan va keng qo‘llanilgan, ammo ularning har biri o‘zining afzalliklari va zaif tomonlariga ega (Kengash III, 2006). Odatda, u tashkilot tuzilmasi atrof-muhitga mos ravishda moslashtirilishi kerak (Axmad Syaxroz, 2003). Shunday qilib, bu maqola ushbu tadqiqot bo‘shlig‘ini to‘ldirishga harakat qiladi.

Maqola beshta bo‘limga bo‘lingan. Birinchi bo‘lim o‘rganish va tadqiqot jarayonini tushuntiradi. Ikkinchi bo‘limda bank sohasida axborot xavfsizligini boshqarish bo‘yicha adabiyotlar tahlili tasvirlangan. Uchinchi bo‘limda axborot xavfsizligini boshqarish bo‘yicha tez-tez qo‘llaniladigan tizimlar va ularning farqlari muhokama qilinadi. To‘rtinchi bo‘limda bank tizimi uchun taklif qilingan ISG (Information Security Governance) asoslari muhokama qilinadi. Nihoyat, maqola xulosa bilan yakunlanadi.

Bank va moliya institutlari uchun eng keng tarqalgan texnologik xavf yoki tahdid bu **fishing hujumi**dir (Tubin, 2005). Odatiy fishing hujumi ijtimoiy muhandislikka asoslangan bo‘lib, kompyuter jinoyatchilari mijozlar va xodimlarni o‘z akkauntlarining foydalanuvchi nomlari va parollari kabi maxfiy ma’lumotlardan foydalanish uchun ishlatadigan taktikadir. Ushbu maxfiy ma’lumotlar bilan firibgarlar tarmoqlarga kirib, mablag‘larni o‘tkazib yuborishi va hisoblarni egallashi mumkin. Hujumning boshqa

shakllari, masalan, josuslik dasturlari, troyan otlari[2] va keylogger[3]lar, foydalanuvchining turli xil ma'lumotlarini yig'ish maqsadida ishlab chiqilgan zararli dasturlardir. Bunda foydalanuvchi o'zi bilmagan holda yuklab olgan dastur, jinoyatchining qarmog'iga tushishga olib kelishi mumkin. Bu esa ko'proq uchraydigan fishing hujumlari bilan bog'liq. Hisobni ko'zdan kechirish hisobni egallab olishdan ancha shubxali harakatdir. 2007-yildagi yana bir voqeada Shimoliy Karolina politsiyasi uchta kiber o'g'rini shahar Milliy bankidagi shahar bank hisob raqamidan 450 000 AQSh dollarini o'g'irlaganlikda aybladi. Gumon qilinayotgan o'g'rilar shaharning bank hisob raqamiga kirish va pul o'tkazmalarini amalga oshirish uchun haqiqiy identifikatsiya ma'lumotlaridan foydalangan. Voqea bo'yicha sud-tibbiyot ekspertizasi tekshiruvi shahar bank hisob raqami identifikatsiya ma'lumotlari kompaniya foydalanuvidagi ishchi noutbukda o'rnatilgan josuslik dasturlari orqali o'g'irlanganligini aniqladi (Vijayan, 2010). Nyu-Jersi shtatida bank xodimlari tomonidan 500 000 ta bank hisob raqamlari va shaxsiy ma'lumotlarni o'g'irlash bo'yicha jinoyat ishi ochildi. Bu ish keng qamrovli sxema bo'lib, jinoiy guruh bu ma'lumotlarni kollektorlarga sotish niyatida bo'lgan (MSNBC, 2010).

Bank ishida axborot xavfsizligini boshqarish

Adabiyotlarda axborot xavfsizligini boshqarish bo'yicha bir nechta ta'riflar mavjud, ammo akademiklar va tadqiqotchilar kelishilgan holatda bir xil ta'riflar berishmagan. Moulton and Cole (2003) "Axborot xavfsizligini boshqarish - axborot va uni qo'llab-quvvatlovchi jarayonlar va tizimlarning maxfiyligi, yaxlitligi va mavjudligi bilan bog'liq xavflarni boshqarish uchun nazorat muhitini yaratish va qo'llab-quvvatlashdir", deb ta'riflagan. Xarris (2006) "Axborot xavfsizligini boshqarish barcha vositalar, xodimlar va biznes jarayonlari xavfsizligini ta'minlash uchun tashkilotning o'ziga xos ehtiyojlari", deb xulosa qildi. U tashkiliy tuzilmani, boshqaruv va mas'uliyatni, samaradorlikni, belgilangan vazifalarni va nazorat mexanizmlarini talab qiladi. IT boshqaruv instituti (2006) xulosasiga ko'ra," Axborot xavfsizligini boshqarish - strategik yo'nalishni ta'minlash, xavflarni to'g'ri boshqarish va korxona resurslaridan mas'uliyat bilan foydalanishni tekshirish maqsadida boshqaruv kengashi tomonidan amalga oshiriladigan mas'uliyat va amaliyotlar majmuidir" deya ma'lumot bergan. (Qingxiong Ma, 2004) Axborot xavfsizligini boshqarish atamasining ushbu ta'rifi tadqiqot uchun kengroq va mos bo'lganligi uchun ushbu maqolada havola sifatida foydalaniladi.

1-"Insayder" - bu ochiq aksiyadorlik jamiyatining direktori yoki yuqori mansabdor shaxs[2].
2-Troyan oti virusi - bu qonuniy dastur sifatida yashiringan kompyuterga yuklab olinadigan zararli dastur.[3]
3-Keylogger-klaviatura bosish yozuvchisi yoki klaviaturani yozib olish deb ataladigan keylogger ma'lum bir kompyuterda har bir tugmani kuzatish va yozib olish uchun ishlatiladigan kuzatuv texnologiyasining bir turidir.[4]

Axborot xavfsizligini boshqarishni amalga oshirishning asosiy maqsadi tashkilotning eng qimmatli aktivini himoya qilishdir.

Kompaniyaning axborot aktivlarini aniqlash kompaniyalarda axborot xavfsizligini samarali amalga oshirish uchun muhim omilidir (IT boshqaruv instituti, 2001; Deloitte Touche Tohmatsu, 2003).

Kurt va Tentra (2004) bank sohasida himoya qilinishi kerak bo‘lgan axborot aktivlarini to‘rtta qismga ajratadilar:

•Ichki ma’lumotlar: bozorda noqonuniy ustunlik beruvchi va ichki operatsiyalarini boshqarish uchun mos bo‘lgan ma’lumotlar (masalan: direktorlar kengashining yig‘ilish bayonnomalari, kapital bozori ma’lumotlari va kompaniyaning ichki moliyaviy ma’lumotlari).

•Mijoz haqida ma’lumot: mijozning shaxsini aniqlashga imkon beruvchi ma’lumotlar (masalan: ismi, manzili, tug‘ilgan sanasi), shu jumladan uning bank ma’lumotlari (hisob raqami, depozit raqami).

•Mijozning hisob raqam ma’lumotlari: Iqtisodiy benefitsiar, raqamlangan yoki xayoliy hisob egalarining ma’lumotlari.

• Balans haqida ma’lumot: Bank va mijozlar o‘rtasidagi tijorat da’volarini ifodalovchi ma’lumotlar yoki biznes hamkorlar to‘g‘risidagi ma’lumotlar (masalan: bank hisobi, bank depoziti, nostro hisob raqamidagi ma’lumotlar).

•Tranzaksiyalar haqida ma’lumot: Bank, mijozlar yoki biznes hamkorlar o‘rtasidagi tijorat da’volarini o‘zgarishiga olib keladigan ma’lumotlar (masalan: hisob raqamlar va depozitlar harakati, savdodagi hodisalari).

Axborot xavfsizligini boshqarish amaliyotining yo‘qligi sababli bank tizimiga birinchi navbatdagi tahdidlarni quyidagicha tasniflash mumkin:

1) Binolarni, infratuzilmani va ma’lumotlarni tabiy yoki qastdan jismoniy yo‘q qilish. Favqulotda vaziyatga tayyorgarlikning yo‘qligi, bankning yopilishiga olib kelishi mumkin (Kurt va Tentra, 2004).

2) Asbob uskunalarning yaroqliligi, xodimlarning malakasi, ish yuki, ish odob-axloq normalari va kompaniya qadiriyatlari kabi ko‘plab omillarga e’tibor bermaslik tufayli tizimlar va ma’lumotlarning qasddan yo‘q qilinishi yoki shikastlanishiga sabab bo‘lishi (Kurt va Tentra, 2004; Siregar, 2008).

3) Bank xodimlari yoki agentlari tomonidan maxfiy ma’lumotlar bilan ishlashda ishonchni suiste’mol qilish: masalan, mijoz ma’lumotlari yoki biznes sirlarini o‘zlashtirish, bank va mijozlar to‘g‘risidagi maxfiy ma’lumotlarni soxtalashtirish yo‘li bilan zarar yetkazilishi (Kurt va Tentra, 2004; MSNBC, 2010).

4) Bandlik siyosati, biznes-jarayonlari, tizim ruxsatnomalari, ijtimoiy nazoratning yo‘qligi, bitim yoki valyuta kursi to‘g‘risidagi ma’lumotlarni o‘zlashtirish yoki

soxtalashtirish, bank xodimlari yoki agentlarini bank yoki mijozlar hisobidan boyishi, kompaniya qoidalariga bo‘ysunmaslik (Kurt va Tentra, 2004; Siregar, 2008; MSNBC, 2010).

5) Bankning axborot tizimiga xakerlar va viruslar kabi tashqi hujumlar axborotning yo‘qolishi, ma’lumotlarni soxtalashtirilishi, ma’lumotlarning maxfiyligi buzilishi, biznes jarayonlarining buzilishi; (Kurt va Tentra, 2004; Vijayan, 2010).

6) Ma’lumotlarni, telekommunikatsiya tarmoqlari faoliyatini, o‘g‘irlangan asbob-uskunalarni tahlil qilish yo‘li bilan xorijiy razvedka xizmatlari tomonidan ma’lumotlarning tizimli to‘planishi va bunday harakatlar mijoz ma’lumotlarining daxlsizligiga tahdid solishi(Kurt va Tentra, 2004; Biznesni boshqarish, 2010).

7) Ijtimoiy muhandislik yondashuvi tizimda jabrlanuvchining shaxsini tasdiqlovchi ma’lumotlarni berish yoki tizim haqida ma’lumot olish, shu jumladan parollarni o‘zgartirish kabi omillar bankning ma’suliyatiga misol bo‘la oladi. (Biznesni boshqarish, 2010).

Axborot aktivlari va bank faoliyatidagi potentsial tahdidlarni tasniflagandan so‘ng, keyingi bo‘limda axborot xavfsizligini boshqarish bo‘yicha tez-tez qo‘llaniladigan tizimlar va standartlar, eng yaxshi amaliyot va yo‘riqnomalar muhokama qilinadi.

Axborot doirasi xavfsizlik boshqaruvi

Ma’lumot uchun, Rastogi va Von Solms (2006) axborot xavfsizligini boshqarish tizimlari, munosabatlar va jarayonlardan iborat ekanligini ta’riflaydi; axborot xavfsizligini boshqarishni amalga oshirish uchun asoslarni ta’minlovchi yo‘riqnoma mavjud. Asosan axborot xavfsizligini boshqarish bo‘yicha mas’uliyatni tashkiliy ierarxiya bilan taqqoslash orqali amalga oshiriladi. Holmquist (2008) ma’lumotlar xavfsizligi standarti bank sanoati uchun qo‘llaniladigan axborot xavfsizligini boshqarish tizimlarining bir nechta tanlovini taklif qiladi. Ushbu taklifga asoslanib, biz yuqorida aytib o‘tilgan axborot xavfsizligini boshqarish tizimini batafsil ko‘rib chiqamiz. Axborot xavfsizligini boshqarishda keng qo‘llaniladigan turli xil tizimlar mavjud, bular:

FFIEC

Federal Moliya Institutlarini Ekspertiza Kengashi (FFIEC-the Federal Financial Institutions Examination council) 1979 yil Moliyaviy institutlarni tartibga solish va foiz stavkalarini nazorat qilish to‘g‘risidagi (FIRA-Financial Institutions Regulatory and Interest Rate Control Act), 95-630-sonli davlat qonunining X sarlavhasiga muvofiq tashkil etilgan.

1-Xayoliy hisoblar-pulni to‘g‘ri va samarali ishlatish uchun o‘tkaziladiga mashg‘ulot qatnashchilari.[5]

2-Nostro hisobvaraq deganda bankning boshqa bankda chet el valyutasida saqlaydigan hisob qaydnomasi tushuniladi.[6]

1989-yilda Moliya institutlarini isloh qilish, qayta tiklash va qo‘llash to‘g‘risidagi XI sarlavhasida Imtihon Kengashi tarkibida Baholash quyi qo‘mitasini (ASC-The Appraisal Subcommittee) tashkil etdi.

Federal rezerv boshqaruv kengashi (FRB-Federal Reserve System), Federal Depozitlarni Sug‘urtalash Korporatsiyasi (FDIC- Federal Deposit Insurance Corporation), Milliy moliya institutlari tomonidan moliya institutlarini federal ekspertizadan o‘tkazish uchun yagona tamoyillar, standartlar va hisobot shakllarini belgilash vakolatiga ega bo‘lgan rasmiy idoralararo organdir. Davlat va federal nazorat organlari tomonidan yagona imtihon tamoyillari va standartlarini qo‘llashni rag‘batlantirish uchun Kengash nizom talablariga muvofiq, davlat nazorati organlarining besh nafar vakilidan iborat davlat aloqa qo‘mitasini tashkil etadi.

Kengash federal nazorat ostidagi moliya institutlari, ularning xolding kompaniyalari va ushbu institutlarning moliyaviy bo‘lmagan filiallari va xolding kompaniyalari uchun yagona hisobot tizimlarini ishlab chiqishga javobgardir. Kengashda vakili bo‘lgan besh federal a’zo agentlik tomonidan ishlaydigan imtihonchilar uchun semenar o‘tkazadi va bu semenar hisobotlarini moliya institutlarini nazorat qiluvchi davlat idoralari xodimlariga taqdim etadi. [7]

Bunda quyidagi ISG komponentalari kiritilgan:

- Axborot xavfsizligi strategiyasi;
- Yetakchilik va homiylik;
- Investitsiyalar bo‘yicha xavfsizlik daromadi;
- Xavsizlik ko‘rsatkichi va o‘lchovi;
- Xavfsizlik dasturi tashkiloti;
- Xavsizlik siyosati tartibi, eng yaxshi amaliyot standartlari va ko‘rsatmalari;
- Muvofiqlik;
- Monitoring va audit;
- Huquqiy tartibga soluvchi;
- Foydalanuvchi habardorligi, ta’lim va trening;
- Standartga muvofiq sertifikatlash;
- Risklarni boshqarish va baholash;
- Eng yaxshi amaliyotlarni ko‘rib chiqish;
- Aktivlar boshqaruvi;
- Jismoniy va ekologik nazorat qilish;
- Texnik operatsiyalar;
- Tizimni sotib olish , ishlab chiqish va texnik xizmat ko‘rsatish;
- Biznesning uzluksizligini rejalashtirish;

- Favqulotta vaziyatlarni tiklashni rejalashtirish
- Foydalanuvchi boshqaruvi
- Uzluksiz xizmat ko‘rsatishni ta’minlash

COBIT

Axborot va tegishli texnologiyalarni boshqarish maqsadlari (COBIT-Control Objectives for Information and related Technology) axborot tizimlari auditi va nazorati assotsiatsiyasi va jamg‘armasi tomonidan boshqaruv va biznes jarayonlari egalariga IT bilan bog‘liq xavflarni tushunish va boshqarishga yordam beradigan IT boshqaruv modelini taqdim etish uchun ishlab chiqilgan. COBIT to‘rtta asosiy komponentdan iborat: rejalashtirish va tashkil etish, sotib olish va amalga oshirish, yetkazib berish va qo‘llab-quvvatlash va nihoyat monitoring va baholash (IT boshqaruv instituti, 2007).[8]

1998-yilda ISACA tomonidan IT boshqaruvi va tegishli mavzular bo‘yicha asl tadqiqotlarga e’tibor qaratish maqsadida tashkil etilgan IT boshqaruv instituti (ITGI) IT boshqaruvi uchun asos bo‘lgan COBIT (ITGI, 2007) ni ishlab chiqdi. COBIT to‘rt domenga guruhlangan 34 ta jarayon to‘plamini taqdim etadi. Ushbu jarayonlarda har biri uchun nazorat maqsadlari, ko‘rsatkichlari, yetuklik modellari va boshqa boshqaruv yo‘riqnomalari batafsil bayon qilinadi. COBIT asosan IT boshqaruviga yo‘naltirilgan bo‘lsa-da, uning to‘rtta jarayoni ko‘proq ISG bilan bog‘liq, ya’ni:

- PO6 - Boshqaruv maqsadlari va yo‘nalishlarini bildiradi.
- PO9 - AT risklarini baholash va boshqarish
- DS4 - uzluksiz xizmat ko‘rsatishni ta’minlash
- DS5 - tizim xavfsizligini ta’minlash

COBIT atrofida uni asosiy doiradan tashqari to‘ldiradigan mahsulotlar guruhi mavjud (masalan, amalga oshirish bo‘yicha qo‘llanma, kafolat bo‘yicha qo‘llanma, IT investitsiyalarining qiymati va boshqalar).

- (ITGI, 2006b) ITGI ISG nima ekanligini va nima uchun muhimligini tavsiflaydi. Direktorlar kengashi va yuqori lavozimli rahbarlar nima qilishi kerakligi, uni qanday amalga oshirish mumkinligi va natijada nimaga erishish mumkinligi haqida batafsil ma’lumot beradi.
- Taklif (ITGI, 2008b) avvalgisida keltirilgan sabablarga asoslangan. U axborot xavfsizligi maqsadlari haqida, ularga erishish uchun ishlatilishi mumkin bo‘lgan strategiyalar va harakatlar rejalari haqida batafsilroq ma’lumot beradi. Bundan tashqari, axborot xavfsizligini kuzatish va o‘lchash uchun muhim muvaffaqiyat omillari va ko‘rsatkichlari kiritilgan bo‘lib, ushbu qo‘llanma yuqorida aytib o‘tilganidan pastroq boshqaruv darajasiga qaratilganligini ko‘rsatadi.[14]

ISO 27002. Xalqaro standartlashtirish tashkiloti (ISO-the International Organization for Standarization) axborot xavfsizligini boshqarish tizimlari va amaliyotlarini o‘z ichiga olgan keng ko‘lamli mavzularda xalqaro standartlarning dunyodagi eng yirik ishlab chiquvchisi va nashriyotchisi. ISO 27002 (2006) standarti, rasmiy ravishda ISO 17799 (2005) standarti, axborot xavfsizligi amaliyoti uchun sanoat standarti kodidir (ISO, 2009). IT 11 ta boshqaruv mexanizmlarini va 130 ta xavfsizlik nazoratini belgilaydi. Standart tashkilotida axborot xavfsizligini boshqarishni boshlash, joriy etish, qo‘llab-quvvatlash va takomillashtirish bo‘yicha ko‘rsatmalar va umumiy tamoyillarni belgilaydi (ISO, 2006) [9].

PCI. (PCI Data Security Standard-PCI DSS), to‘lov ma’lumotlari xavfsizligini oshirish uchun keng qamrovli talablar to‘plami. PCI Xavfsizlik Standartlari Kengashining asoschi to‘lov brendlari, jumladan American Express, Discover Financial Services, JCB International, MasterCard Worldwide va Visa tomonidan ishlab chiqilgan. PCI DSS xavfsizlikni boshqarish, siyosatlar, protseduralar, tarmoq arxitekturasi, dasturiy ta’minot loyihasi va boshqa muhim himoya choralariga qo‘yiladigan talablarni o‘z ichiga olgan ko‘p qirrali xavfsizlik standartidir (PCI, 2010).[10]

CGTF. Korporativ boshqaruv bo‘yicha ishchi guruhi (CGTF-the Corporate Governance Task Force) maqsadli standartlarga asoslangan, keng qamrovli va hamkorlikda ishlab chiqilgan tashkilotlarga yordam berish uchun ISG tuzilmasiga asos soldi. Ushbu yo‘nalish keng miqyosda moslashtirilishi mumkin bo‘lgan turli tashkilotlar, shu jumladan korporatsiyalar turli sanoat tarmoqlarida barcha o‘lchamlarda, shuningdek ta’lim va notijorat muassasalarida ham qo‘llashi mumkin. Bundan foydalanishni osonlashtirish uchun ushbu yo‘nalishda ISG ishchi guruh ishlab chiqilgan bo‘lib, boshqa qo‘shimcha vositalar funktsiyalari va majburiyatlari bo‘yicha qo‘llanma va axborot xavfsizligini boshqarishni baholash vositasi sifatida tuzilgan. (Corporate Governance Task Force, 2004). [11]

IISA. Axborot tizimlari xavfsizligi assotsiatsiyasi (ISSA- Information Systems Security Association) Umumiy qabul qilingan axborot xavfsizligi tamoyillarini (GAISP- The Generally Accepted Information Security Principles) nashr etadi. ISSAning asosiy maqsadi kengash zalidan tortib to zalgacha axborot xavfsizligi bo‘yicha mutaxassislar maxfiyligi, axborotlar yaxlitligi va tashkiliy ma’lumotlar mavjudligini targ‘ib qilishdir. ISSA o‘zaro hamkorlikni osonlashtiradi va yanada muvaffaqiyat yaratish uchun ta’lim, global axborot yaratish uchun tizimlar xavfsizligi va mutaxassislar jalb qiladi.[12]

CISWG. Korporativ axborot xavfsizligi ishchi guruhi (CISWG- The Corporate Information Security Working Group) rivojlantirish bo‘yicha ko‘rsatma,

axborot xavfsizligi ko‘rsatkichlari, yaratilgan axborot xavfsizligining yakuniy xulosasi va boshqaruv ma’lumotnomalarini ishlab chiqadi. CISWG – Adam H. Putnam tomonidan tuzilgan dasturiy texnologiya, axborot siyosati, hukumatlararo munosabatlar, aholini ro‘yxatga olish, hukumatni isloh qilish kabi masalalari bo‘yicha ishlarni AQSh Kongressi Vakillar Palatasi quyi komissiya raisi amlaga oshiradi.[13]

BSA. Biznes dasturiy ittifoqi (BSA-Business Software Alliance) axborot xavfsizligini boshqarish bo‘yicha ishchi guruhini tuzdi. Uning maqsadi tashkilotlar tushunishi va amalga oshirishi mumkin bo‘lgan shartlarga javob berishdir. Ushbu ishchi guruh boshqa hisobotlarda, qonun hujjatlarida va yo‘riqnomalarda mavjud bo‘lgan ko‘plab g‘oyalar va tushunchalarni ikkiga ajratib davom ettirishdi.

Birinchidan, (BSA, 2003) mualliflar IT xavfsizligi atrofida allaqachon qonunchilik va tartibga solish rejimi mavjudligini va kompaniyalar xavfsizligini texnologik muammo sifatida ko‘rib chiqishni to‘xtatishlari va uni korporativ boshqaruv muammosi sifatida ko‘rib chiqishlari kerakligini ta’kidlaydilar. Ular ISO/IEC 17799 (keyinchalik ISO/IEC 27000 oilasiga kiritilgan) kabi ilg‘or amaliyotlar va standart protseduralarni qabul qilishni tavsiya qiladilar va tashkilotlar qabul qilishi mumkin bo‘lgan ISG tizimi yo‘qligini tan oladilar. Ishchi guruh har bir boshqaruv roli o‘z vazifalari nimadan iboratligini, o‘z maqsadlariga qanday erishishni va bajarilgan faoliyatni qanday tahlil qilish va tekshirishni biladigan tizimni taklif qiladi.

Ikkinchidan, taklif (Korporativ boshqaruv bo‘yicha ishchi guruhi, 2004 yil) xavfsizlik bilan bog‘liq bo‘lgan har bir manfaatdor tomonning funksiyalari va mas’uliyatini batafsil tavsiflovchi ilgari kiritilgan doirani kengaytiradi. Ushbu asosni amalga oshirish uchun mualliflar besh bosqichga asoslangan IDEAL modelini taklif qilishadi: boshlash, tashxis qo‘yish, o‘rnatish, harakat qilish va o‘rganish. Nihoyat, tegishli ishlarni baholash, tekshirish va muvofiqlik uchun vositalar taqdim etishadi.

ISACA. Axborot tizimlarini tekshirish va nazorat qilish assotsiatsiyasi (ISACA- Information Systems Audit and Control Association) (ISACA, 2009), korporatsiyalarda axborot xavfsizligini hal qilish uchun umumiy modelni taklif qiladi. U model tizimlar nazariyasiga asoslanadi va shuning uchun to‘liq funktsiya birligi sifatida yaxlit ko‘rib chiqiladigan kirish va chiqishlarga ega bo‘lgan jarayonlardan iborat. Model tetraedr tuzilishiga ega bo‘lib, uning tepalarida joylashgan to‘rtta element va ular orasidagi elementlarni bir-biriga bog‘laydigan o‘zaro bog‘liqlik oltita dinamik mavjud.[14],[16] To‘rt element quyidagilardir:

- Tashkilot loyihasi va strategiyasi
- Odamlar
- Jarayon
- Texnologiya

O‘zaro bog‘liqlik oltita dinamik:

- Boshqarish
- Madaniyat
- Yordam berish va qo‘llab-quvvatlash
- Paydo bo‘lish
- Inson omillari
- Arxitektura

NIST. AQSh Savdo Departamentiga qarashli Milliy Standartlar va Texnologiyalar Instituti (NIST- The National Institute of Standards and Technology) axborot xavfsizligi bilan bog‘liq ko‘plab ko‘rsatmalarni nashr etdi. Qo‘llanmaning (Bowen va boshqalar, 2006) ikkinchi bobi ISGga bag‘ishlangan. Ushbu kitobga ko‘ra, ISGning beshta komponenti mavjud:

- Strategik rejalashtirish
- Tashkiliy tuzilma
- Rol va mas’uliyat
- Korxona arxitekturasi
- Siyosat va yo‘riqnoma

Boshqaruvning ushbu tarkibiy qismlarining barchasi doimiy monitoring orqali xavfsizlikni joriy tatbiq etish bilan bog‘langan bo‘lishi kerak. Ushbu natijaga erishish va monitoringni amalga oshirish uchun faoliyat va yordamchi jarayonlar tavsifi taklif etiladi. Boshqa NIST nashrida (Bowen va boshq., 2007) asosiy e’tibor Axborot xavfsizligi dasturini ishlab chiqishga qaratilgan. Ushbu tadbirlar orasida ISG alohida ta’kidlangan. Shuningdek, AQSh nuqtai nazaridan xavfsizlik dasturlariga tegishli qonunlar va qoidalar qayta tiklandi.[17]

Biznesga yo‘naltirilgan axborot xavfsizligini loyihalash faqat biznes strategiyasiga mos keladigan axborot strategiyasidan kelib chiqishi mumkin. Korporativ axborot xavfsizligini boshqarish IT boshqaruvi va risklarni boshqarish bilan bir qatorda korporativ boshqaruv doirasida o‘z o‘rniga ega bo‘lishi kerak. Hoekstra, Conradie va Spafford ham korporativ boshqaruvda ishlab chiqilgan va keng qo‘llanilgan ba’zi qoidalar mavjudligiga rozi bo‘lishdi, ammo ularning har biri o‘zining kuchli va zaif tomonlariga ega. Shuning uchun, xususiylashtirish tashkilot muhitiga mos ravishda bo‘lishi kerak.

Bank tizimi uchun taklif etilayotgan ISG asosining dastlabki loyihasi

Taklif etilayotgan ISG asosining dastlabki loyihasi bank sektori tomonidan adabiyotlarni ko‘rib chiqishda aniqlangan tahdidlardan bank axborot aktivlarini himoya qilish uchun yo‘riqnomalarni ishlab chiqish va nazoratni amalga oshirish orqali axborot xavfsizligini boshqarish uchun boshlang‘ich nuqta sifatida ishlatilishi mumkin.

Ushbu qoida muhokama qilingan va adabiyotlarni ko‘rib chiqishdan olingan barcha mavjud qoida komponentlarining integratsiyasidir. Shunga qaramay, tavsiya etilgan asos hali ham axborot xavfsizligini boshqarish dasturiga umumiy yondashuv bo‘lib, u mutaxassislar tomonidan ko‘rib chiqilishi va haqiqiy bank muhitida sinovdan o‘tkazilishi kerak. Har bir tashkilotning ish uslubi har xil va turli milliy va xalqaro qonunchilik va qoidalarga bo‘ysunishi sababli, qo‘shimcha komponentlar talab qilinishi mumkin, boshqalari esa tegishli bo‘lmasligi mumkin. Rastogi va Von Solm tomonidan berilgan axborot xavfsizligini boshqarishning ta’rifiga asoslanib, axborot xavfsizligini boshqarish tizimining dastlabki loyihasi axborot xavfsizligi tarkibiy qismlarini strategik daraja, taktik va operatsion daraja mavjud. Axborot xavfsizligi komponentlarining har bir darajasi va ularning tarkibi quyidagicha muhokama qilinadi:

Strategik daraja

Strategik daraja direktorlar kengashi va yuqori boshqaruvni anglatadi. Adabiyotda ko‘rib chiqilgan ko‘pgina asoslar, standartlar va amaliyotlar ushbu darajada taklif qilinadi, yetakchilik va boshqaruv komponenti muvaffaqiyatli axborot xavfsizligi dasturini hal qilish uchun axborot xavfsizligi strategiyasini tuzishni o‘z ichiga oladi. Axborot xavfsizligi strategiyasi tashkilot maqsadlariga ham qisqa, ham uzoq muddatda erishishni ta’minlash uchun tashkiliy va IT strategiyasi bilan bog‘langan bo‘lishi kerak. Bu daraja axborot xavfsizligi dasturi ijirosi uchun hamkorlikni, shuningdek, boshqaruv kengashi va rahbariyatning axborot aktivlarini himoya qilish majburiyatini talab qiladi. Buning sababi, axborot xavfsizligini boshqarish korporativ boshqaruvning ajralmas qismi sifatida qabul qilingan. Korporativ boshqaruv, boshqaruv kengashining yetakchilik sa’y-harakatlari orqali tashkilotni samarali boshqarish va nazorat qilish uchun javobgarligi bilan bog‘liq. Bu IT boshqaruvi bilan bog‘liq bo‘lib, tashkilot o‘z texnologiyasidan foydalanishni qanday boshqarishi va nazorat qilishi hamda ma’lumotlarini himoya qilishini belgilaydigan siyosat va tartiblar haqida qayg‘uradi. Ushbu darajada, joriy qoidalar axborot xavfsizligini boshqarish dasturining samaradorligini aniqlash uchun o‘lchov tushunchalarini o‘z ichiga oladi. Ko‘pgina tashkilotlar o‘zlarining axborot xavfsizligi dasturlarining umumiy samaradorligini va bu tashkilot strategiyasiga erishishga hissa qo‘shayotganini baholash uchun ko‘rsatkichlarga murojaat qiladilar.

Taktik va operatsion daraja

Taktik va operatsion daraja yuqori darajali menejerlar va operativ menejerlarga tegishli. Ko‘rib chiqilgan qoidalarning aksariyati shuni ko‘rsatadiki, bu daraja foydalanuvchilarning xabardorligiga qaratilgan ta’lim va etika asosiy komponent sifatida ko‘rsatilgan. Ammo ko‘pchilik tadqiqotchilar axloqiy xatti-harakatlar tufayli ishonchni taklif qilmaydi va maxfiylik ushbu darajaga kiritilishi kerak. Tadqiqotchi

axloqiy xulq-atvorni o‘z ichiga oladi, chunki OECD xavfsizlik madaniyatini yaratish tamoyillaridan biri axloqiy xulq-atvor ekanligini ta’kidlaydi. Bunda menejment ham, kengash ham korporativ axloq kodeksini ishlab chiqadi va muloqot qiladi. Axborot xavfsizligini boshqarish tizimining bir qismi sifatida, masalan, shaxsiy hayotga tajovuz qilish, mijozlar ma’lumotlarini sotish va ma’lumotlarni ruxsatsiz o‘zgartirish xavfini minimallashtirish uchun tashkilot axloqiy xulq-atvorni ko‘rib chiqishi kerak. Ushbu axloqiy xulq-atvor xodimlarga xavfsizlik haqida xabardorlik dasturining bir qismi sifatida saqlanadi.

Ushbu darajadagi taklif qilingan boshqa asosiy komponent - bu "ishonch". Axborot xavfsizligini boshqarish tizimi tarkibiy qismlarini amalga oshirishda rahbariyat xodimlarga axborot xavfsizligi siyosatiga rioya qilishiga ishonishi, xodimlar esa axborot xavfsizligi dasturini amalga oshirish majburiyatini bajarishda boshqaruvga ishonishlari kerak. Shuningdek, savdo hamkorlari va tashkilot obro‘siga hissa qo‘shishi mumkin bo‘lgan mijozlar o‘rtasida ishonchli munosabatlar o‘rnatilishi kerak. Maxfiylik bu darajadagi asosiy komponent sifatida, shuningdek, mijozlar, yetkazib beruvchilar va boshqa biznes sheriklar bilan yaxshi munosabatlarga kelganda ishonch muhim masaladir.

Texnik daraja.

Dastur tashkilot axborot xavfsizligining tashkiliy loyihasi, tarkibi va hisobot tuzilmalarini anglatadi. Shuningdek, u korporativ xavfsizlik arxitekturasiga oid rol va mas’uliyat, ko‘nikma va tajriba hamda resurslar darajasini belgilaydi. Huquqiy va tartibga solish masalalari asosiy komponent sifatida taklif etiladi, chunki turli mamlakatlarda turli xil qonunlar va qoidalar mavjud, shuning uchun axborot xavfsizligini boshqarish dasturida buni hisobga olish kerak.

Ko‘rib chiqilgan tizimlarning aksariyati xavfsizlik siyosati, protseduralari, standartlari va yo‘riqnomalarini boshqaruv va xodimlarga yo‘nalish va yordam bilan ta’minlash uchun axborot xavfsizligini ta’minlashning asosiy komponentlari sifatida taklif qiladi va ular xodimlardan nima kutilishi va ularning xatti-harakatlari bo‘yicha ko‘rsatmalarni aniq ko‘rsatishi kerak. Xavfsizlik siyosati tashkilotda samarali jarayonlar va muvofiqlik monitoringi orqali amalga oshirilishi kerak. Axborot xavfsizligi siyosatiga misol sifatida kirishni boshqarish siyosati, elektron pochta va Internet siyosati hamda jismoniy va atrof-muhit siyosati kiradi. Jarayon xavfsizlik siyosatining talqini bo‘lib, siyosatni amalga oshirish uchun bajarilishi kerak bo‘lgan qadamlardir. Protseduralar parol standarti kabi standartlar va xavfsizlik siyosati talablariga javob beradigan xavfsizlik devorini sozlash tartib-qoidalari kabi ko‘rsatmalar bilan ta’minlanadi.

Texnik daraja barcha xodimlarga tegishlidir. Ba'zi sharhlar tizimi axborot xavfsizligini boshqarish dasturining asosiy komponentalari sifatida texnologiyani himoya qiladi. U IT muhitini himoya qilish uchun amalga oshirilgan texnik va jismoniy mexanizmlarni o'z ichiga oladi. Xavfsizlikni boshqarish tizimini amalga oshirishda, tashkilotga tegishli texnologiya nazorati, atrof-muhit va aniqlangan xavflarni tahlili kerak. Bularga aktivlarni boshqarish, tizimni ishlab chiqish talablari, hodisalarni boshqarish, tarmoq va jismoniy kabi texnik operatsiyalar, atrof-muhit, xavfsizlik va biznesning uzluksizligini boshqarish va foydalanuvchilarni boshqarish kiradi. Texnologik muhitni doimiy ravishda kuzatib borish va bozorda texnologiya o'zgarishi xavfini bartaraf etish muhim ahamiyatga ega. Bundan tashqari shaxsiy raqamli yordamchilar va masofadan ishlash texnologiyasidan foydalanish mumkin.

Taklif etilayotgan ISG asosining dastlabki loyihasi

Strategik daraja

- Axborot xavfsizligi strategiyasi
- Etakchilik va homiylik
- Investitsiyalar bo'yicha daromadlar xavfsizligi
- Xavfsizlik ko'rsatkichi va o'lchovi
- Ichki va tashqi auditor axborot xavfsizligi dasturi

Taktik, operatsion daraja

- Xavfsizlik dasturini tashkil etish
- Xavfsizlik siyosati, tartibi, eng yaxshi amaliyot, standartlar va ko'rsatmalar
- Muvofiqlik
- Monitoring va audit
- Huquqiy va tartibga soluvchi
- Foydalanuvchilarning xabardorligi, ta'lim va o'qitish
- Axloqiy qadriyatlar va xulq-atvor
- Maxfiylik va ishonch
- Standartga muvofiq sertifikatlash
- Xatarlarni boshqarish va baholash jarayoni
- Eng yaxshi amaliyot va asosiy ko'rib chiqish

Texnik daraja

- Aktivlar boshqaruvi
- Jismoniy va atrof-muhitni nazorat qilish
- Texnik operatsiyalar
- Rivojlanish va xizmat
- Hodisalarni boshqarish

- Biznesning uzluksizligi rejasi
- Favqulotda vaziyatlarni tiklash rejasi foydalanuvchilarni boshqarish

Qoidalarning ushbu darajasida axborot xavfsizligi dasturini boshqarishning asosiy komponentlari sifatida monitoring, muvofiqlik va audit ham taklif etiladi. Bu o‘lchash va muvofiqlikni ta’minlash uchun zarurdir, axborot xavfsizligi siyosatiga rioya etilishini ta’minlash va aniqlangan hodisalarga samarali va o‘z vaqtida javob berish uchun texnologiya va xodimlarning xatti-harakatlari kuzatilishi kerak. Xodimlarning xatti-harakatlarini monitoring qilish ruxsatsiz dasturiy ta’minotni o‘rnatilishini kuzatishni, tashrif buyurilgan Internet saytlariga kuchli parollardan foydalanishni o‘z ichiga olishi mumkin yoki texnologiya monitoringi sig‘im va tarmoq trafigi monitoringi bilan bog‘liq bo‘lishi mumkin.

Xulosa

Hozirgi texnologik va ijtimoiy sharoitda xavfsizlik bank va moliya institutlari tizimining juda muhim qismidir. Biznes hamkorlar, yetkazib beruvchilar va sotuvchilar bir-biridan yuqori axborot xavfsizligini talab qiladi, ayniqsa o‘zaro tarmoq va ma’lumotlarga kirishni ta’minlashda. Raqobatbardosh razvedka ma’lumotlariga ega bo‘lish orqali tovlamachilik maqsadida tarmoqlardan foydalangan holda josuslik keng tarqalmoqda. Banklarning kelajagi ko‘pincha ochiq, qulay, xavfsiz tarmoqga ulanishi va xizmatlarini taqdim etish qobiliyatiga bog‘liq. Axborotni himoya qilish tajribasiga ega bo‘lish va u bilan ishlaydigan muhit xavfsizligi tashkilotning bozor ulushini saqlab qoladi yoki qobiliyatini oshiradi. Bank axborot tizimi uchun axborot xavfsizligini boshqarishning keng qamrovli asosi juda zarur. FFIEC, COBIT, ISO 27002 va PCI ma’lumotlar xavfsizligi standartlari kabi ba’zi umumiy standartlar va eng yaxshi amaliyotlar ishlab chiqilgan, ammo ularning hech biri tashkilotning o‘ziga xos va noyob ehtiyojlarini qondira olmaydi. Ushbu davom etayotgan tadqiqot bank muhiti va IT axborot tizimini hisobga olgan holda axborot xavfsizligini boshqarishning aniq tizimini ishlab chiqishdan iborat. Shu maqsadda bazadan bank uchun axborot xavfsizligini boshqarish uchun dastlabki harakat sifatida foydalanish mumkin. Ushbu qoida bugungi kunda mavjud bo‘lgan barcha qoidalar komponentlarining integratsiyasidir. Aslini olganda, ushbu asos hanuzgacha axborot xavfsizligini boshqarish dasturiga umumiy yondashuv bo‘lib, u mutaxassislar tomonidan ko‘rib chiqilgan va real bank muhitida har tomonlama sinovdan o‘tgan. Ushbu tadqiqot rivojlangan mamlakatlarda axborot xavfsizligini boshqarish tizimi bo‘yicha IT-professional idrokini yanada ko‘proq web-so‘rovlar orqali o‘rganish davom etmoqda.

FOYDALANILGAN ADABIYOTLAR

[1]:https://bolster.ai/glossary/phishinghosting#:~:text=Phishing%20hosting%20involves%20offering%20a,like%20passwords%20or%20financial%20data.
[2]: https://www.investopedia.com/terms/i/insider.asp
[3]: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus
[4]:https://www.techtarget.com/searchsecurity/definition/keylogger#:~:text=A%20keylogger%2C%20sometimes%20called%20a,Apple%20iPhone%20and%20Android%20devices.
[5]: https://hubpages.com/money/forum/109409/imaginary-bank-account
[6]: https://www.investopedia.com/terms/n/nostroaccount.asp
[7]: https://www.ffiec.gov/about.htm
[8]: https://www.isaca.org/resources/cobit
https://ru.wikipedia.org/wiki/Cobit
[9]: https://ru.wikipedia.org/wiki/ISO/IEC_27002
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en
[10]: https://www.pcisecuritystandards.org/about_us/
[11]:https://asic.gov.au/regulatory-resources/corporate-governance/corporate-governance-taskforce/
https://download.asic.gov.au/media/5290879/rep631-published-2-10-2019.pdf
[12]: https://www.issa.org/
[13]:https://library.educause.edu/resources/2004/1/corporate-information-security-working-group
[14]:https://www.researchgate.net/publication/232252326_Comparative_Analysis_of_Information_Security_Governance_Frameworks_A_Public_Sector_Approach
[15]: https://www.bsa.org/about-bsa
[16]: https://www.isaca.org/
[17]: https://www.nist.gov/
Akhmad Syakhroza (2003). Best Practice Corporate Governance Dalam Kontek Perbankan Indonesia. Jakarta: Usahawan No. 06 Thn XXXII. 19.

Allen, J. H. & Westby, J. R. (2007). Governing for Enterprise Security (GES), Implementation Guide: Characteristics of Effective Security Governance1. USA: Carnegie Mellon University. 5-7

Biri, K .& Tentra, G.M. (2004). "Corporate Information Security Governance in Swiss Private Banking," Master's Thesis University of Zurich

Business Management (2010). Staying off The Hook. Business management Magazine Issue 4, Security & Data. Retrieved July 2010, from http://www.busmanagementme.com/artic le/ Middle East Bank - Security Breaches - Phishing Frauds - IT Security/

Corporate Governance Task Force (2004).'Corporate Governance Task Force Report: Information Security Governance A Call To Action,' National Cyber Security Summit April 2004, USA

Council III, C. (2006). 'An Investigation of a COBIT System Security IT Governance Initiative in Higher Education,' PhD Thesis. Nova Southeastern University

Donaldson, W. H. (2005). 'U.S. Capital Markets in The Post-Sarbanes Oxley World: Why our markets should matter to foreign issuers,' U.S: Securities and Exchange Commission. London School of Economics.

Ernst & Young (2003). Global Information Security Survey 2003. US: E&Y

Flowerday, S. & Solms, R. V. (2006). Trust an Element of Information Security Securityand Privacy in Dynamic Environments. IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

Harris, S. (2006). Information Security Governance Guide [online], [Retrieved 03- 04-2008]. www.SearchSecurity.com

Hoekstra, A. & Conradie, N., (2002). CobiT, ITIL and ISO17799, How to Use Them in Conjunction. USA: Price Water House Copper.

Holmquist, E. (2008). "Which Security Governance Framework is The Best Fit?," TechTarget ANZ, Australia [Online]. [Retrieved: August 2008], http://searchcio. techtarget.com. au/articles/24787-Which- security governance-framework-is the-best-fit-.htm,

ISO 27002-2006(2006). International Standard - Information Technology - Security Techniques - Code of Practice for Information Security Management [Online]. [Retrieved May 15, 2009], http://www.iso.org/iso/iso_catalogue/cat alogue_tc/

IT Governance Institute (2001). Information Security Governance: Guidance for Board of Directors and Executive Management. IT Governance Institute, Rolling Meadows, 11

IT Governance Institute (2006), Information Security Governance: Guiding for Board of Director and Executive Management 2nd Edition [online], [Retrieved May 15, 2009], www.itgi.org

IT Governance Institute (2007). CobiT 4.1 Excerpt [Online]. [Retrieved March 20, 2009],http://www.itgi.org/Template_ITGI.cfm?Section=Recent_publications&Tmpla te=/Content Management/ ContentDisplay.cfm&ContentID=45948

Ma, Q. (2004). 'A Study on Information Security Objectives and Practices,' PHD Dissertation, Southern Illinois University. 17

Mahncke, R. J., McDermid D. C.& Williams P. A. (2009). "Measuring Information Security Governance within General Medical Practice," Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia.

McCarthy, M.P. & Campbell, S. (2001). Security Transformation. New York: McGraw-Hill.

Moulton, R & Coles, R. S. (2003). "Applying Information Security Governance," Elsevier

MSNBC (2010). Massive Bank Security Breach Uncovered in New Jersey [online]. [Retrieved July 2010], from http://www.msnbc.msn.com/id/3303539

OECD. (2004). OECD Principles of Corporate Governance Organisation for Economic Co-Operation and Development. OECD

PCI. (2010). About the PCI Data Security Standard (PCI DSS) [online], [Retrieved July 2010], https://www.pcisecuritystandards.org/sec urity_standards/pci_dss.shtml Publisher

Power, R. (2002). CSI/FBI Computer Crime and Security Survey (2002), Computer Security Issues & Trends, vol. VIII, No.1.

Rastogi, R & Von Solms, R. (2006). Information Security Governance a Redefinition. IFIP International Federation for Information Processing, Volume 193/2006, Springer Boston.

Rogers, M. (2001). A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: an Exploration Study. Unpublished dissertation.[online],[RetrievedAugust2007],http://www.mts.net/mkr/cybercrimethesis.pdf

RSA (2010). Information Security Glossary: The Federal Financial Institutions Examination Council (FFIEC)[online].

Von Solms, B. (2000). "Information Security - The Third Wave?," Computers and Security, 19(7). November, 615-620.

Von Solms, R. & Von Solms S. H. (2006). "Information Security Governance: A Model Based on the Direct Control Cycle," Elsevier Ltd: Computers & Security, Volume 25, September 2006, Pp 408-412