HUQUQNI MUXOFAZA QILISH ORGANLARINING KIBERXAVFSIZLIKNI OLDINI OLISHDAGI O‘RNI

Radjabova M.Sh
Hafizov Sh.F
Abdullayev I.K
Avazbekov M.A
Toshkent axborot texnologiyalari unversiteti

Anatatsiya: *Kiberxavfsizlik texnologiyasining murakkab tabiati va kiberxavfsizlik tahdidlari tobora kuchayib borayotganini hisobga olsak, huquqni muxofaza qilish organlari doimiy ravishda so‘nggi tahdidga qanday munosabatda bo‘lish bo‘yicha qarorlar bilan to‘qnash kelishlarini kutish mumkin.*

Kalit so’zlar: *kiberxavfsizlik, tahdid, zaiflik, kiberxavfsizlik sistemagrammasi, xavfsizlik, autentifikatsiya, veb ilovalar, IOT, AI, ML, Kriptografiya.*

Kirish

Huquqni muhofaza qilish organlari kiberxavfsizlik tahdidlarini bartaraf etishda hal qiluvchi rol o’ynaydi, chunki ular kiberjinoyatlarni tergov qilish va ta’qib qilish uchun javobgardir. Huquqni muhofaza qilish organlari xodimlari kibertahdidlarni samarali aniqlash, tahlil qilish va ularga javob berish uchun zarur bo’lgan bilim va ko’nikmalarga ega bo’lishi kerak. Ular kiberxavfsizlik bo’yicha mutaxassislar va boshqa manfaatdor tomonlar bilan hamkorlikda xavflarni yumshatish va kiberjinoyat sodir bo’lishining oldini olishlari kerak.

Har kuni jismoniy shaxslar, tashkilotlar va hukumatlar duch keladigan turli xil kibertahdidlar va xavflar mavjud. Kiberxavfsizlikning eng keng tarqalgan tahdidlaridan ba’zilari zararli dasturlar, fishing, to’lov dasturi, ijtimoiy muhandislik, xakerlik va xizmat ko’rsatishni rad etish (DoS) hujumlarini o’z ichiga oladi. Zararli dastur deganda kompyuter tizimlari yoki tarmoqlariga zarar yetkazish, o’chirish yoki ruxsatsiz kirishni qo’lga kiritish uchun mo’ljallangan dasturiy ta’minot tushuniladi. Fishing maxfiy ma’lumotlarni oshkor qilish yoki zararli dasturlarni o’rnatish uchun foydalanuvchilarni aldash uchun soxta elektron pochta xabarlari, xabarlar yoki veb-saytlardan foydalanishni o’z ichiga oladi. Ransomware - bu fayllarni shifrlaydigan yoki to’lov to’lanmaguncha foydalanuvchilarni qurilmalaridan bloklaydigan zararli dastur turi. Ijtimoiy muhandislik maxfiy ma’lumotlarni oshkor qilish uchun shaxslarni manipulyatsiya qilishni anglatadi. Xakerlik ruxsatsiz kirish uchun kompyuter tizimlaridagi zaifliklardan foydalanishni o’z ichiga oladi. DoS hujumlari server yoki tarmoqning ishdan chiqishiga yoki ishlamay qolishiga olib keladigan trafik bilan to’lib ketishini o’z ichiga oladi.

Kibertahdidlarning tabiati doimiy ravishda o’zgarib turadi va muntazam ravishda yangi xavflar paydo bo’ladi. Xakerlar va kiberjinoyatchilar hujumlarni amalga oshirish uchun sun’iy intellekt (AI) va mashinali o’rganish (ML) kabi ilg’or usullardan foydalangan holda o’z usullarida tobora murakkablashmoqda. Bulutli hisoblash va buyumlar internetining (IoT) keng qo’llanilishi ham hujum maydonini kengaytirib, kiberjinoyatchilarga jismoniy shaxslar va tashkilotlarni nishonga olishni osonlashtirdi. Ijtimoiy tarmoqlar va onlayn platformalarning

ko'payishi, shuningdek, yovuz niyatli shaxslarning yolg'on ma'lumotlarni tarqatish va jamoatchilik fikriga ta'sir qilishini osonlashtirdi.

Kiberjinoyat shaxslar, tashkilotlar va hukumatlarga jiddiy ta'sir ko'rsatadi. Jismoniy shaxslar moliyaviy yo'qotishlarga, shaxsiy ma'lumotlarning o'g'irlanishiga yoki shaxsiy ma'lumotlarining buzilishi natijasida yuzaga keladigan zararning boshqa shakllariga duch kelishi mumkin. Tashkilotlar kiberhujumlar tufayli obro'siga putur etkazishi, moliyaviy yo'qotishlar yoki intellektual mulkni yo'qotishi mumkin. Hukumatlar milliy xavfsizlikka tahdidlar yoki kiber josuslik yoki kiberhujumlar natijasida maxfiy ma'lumotlarni yo'qotishi mumkin.

Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha ekspertlar o'rtasidagi hamkorlik.

Bugungi raqamli asrda huquq-tartibot idoralari kiberjinoyatchilik xavfi ortib borayotganiga qarshi kurashishda jiddiy muammolarga duch kelmoqda. Kiberjinoyatchilar tomonidan tobora murakkablashib borayotgan taktikalar oldida jinoyatchilikka qarshi kurashning an'anaviy usullari endi yetarli emas. Shunday qilib, samarali kiberxavfsizlik huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislar o'rtasida hamkorlikdagi sa'y-harakatlarni talab qiladi. Ushbu ikki guruh o'rtasidagi fanlararo hamkorlik zarurligini ortiqcha baholab bo'lmaydi.

Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlik kibertahdidlarni samarali aniqlash, oldini olish va tekshirishni ta'minlash uchun muhim ahamiyatga ega. Ikkala guruh ham kibertahdidlarni samarali hal qilish uchun zarur bo'lgan noyob tajriba va istiqbolga ega. Huquqni muhofaza qilish organlari qonuniy vakolat va tergov vakolatlariga ega, kiberxavfsizlik bo'yicha mutaxassislar esa maxsus texnik ko'nikmalarga va kiber tahdidlar bo'yicha bilimga ega. Shu sababli, hamkorlikdagi yondashuv kiberjinoyatning ham huquqiy, ham texnik jihatlarini ko'rib chiqishga yordam beradi.

Xususiy sektor kiberxavfsizlik firmalari kibertahdidlarni yumshatishda hal qiluvchi rol o'ynashi mumkin. Ushbu firmalar odatda eng yangi texnologiyalar va vositalarga ega bo'lib, ularni kiberhujumlarni aniqlash va oldini olish uchun yaxshi jihozlangan qiladi. Huquqni muhofaza qilish idoralari xususiy sektor kiberxavfsizlik firmalari bilan ishlashdan bir necha usulda, jumladan, ekspertizadan foydalanish, ma'lumot almashish va qo'shma tekshiruvlardan foydalanishlari mumkin.

Axborot almashish kiberxavfsizlikning muhim tarkibiy qismidir va xususiy sektor firmalari huquqni muhofaza qilish organlariga qimmatli ma'lumotlar va razvedka ma'lumotlarini taqdim etishi mumkin. Xususiy sektor firmalari paydo bo'layotgan kibertahdidlar, hujum shakllari va yangi zararli dasturlar haqida ma'lumot almashish orqali huquqni muhofaza qilish organlariga kibertahdidlarni yaxshiroq tushunish va oldindan ko'rishda yordam berishi mumkin. Bundan tashqari, xususiy sektor firmalari huquqni muhofaza qilish organlariga potentsial gumonlanuvchilarni aniqlash va kiberjinoyatchilarni kuzatishda yordam berishi mumkin.

Samarali kiberxavfsizlik axborot almashish va razvedka ma'lumotlarini yig'ishga proaktiv yondashuvni talab qiladi. Huquqni muhofaza qilish idoralari boshqa idoralar, xususiy sektor firmalari va xalqaro hamkorlar bilan paydo bo'layotgan kibertahdidlar bo'yicha razvedka ma'lumotlarini almashish uchun hamkorlik qilishi kerak. Bunday ma'lumot almashish jinoiy faoliyat shakllarini aniqlashga yordam beradi va huquqni muhofaza qilish organlariga

kiberhujumlarning oldini olish va ularga javob berish bo'yicha samarali strategiyalarni ishlab chiqish imkonini beradi.

Samarali ma'lumot almashish, shuningdek, eng yaxshi tajribalar va olingan saboqlarni almashishni o'z ichiga oladi. Huquqni muhofaza qilish organlari kelajakdagi tahdidlarga yaxshiroq tayyorgarlik ko'rish uchun oldingi voqealardan saboq olishlari kerak. Ushbu ma'lumotni boshqa agentliklar va kiberxavfsizlik bo'yicha mutaxassislar bilan baham ko'rish umumiy kiberxavfsizlikni yaxshilashga yordam beradi va huquqni muhofaza qilish organlari kiberhujumlarning oldini olish va ularga javob berish uchun yaxshi jihozlanishini ta'minlaydi.

Kiberjinoyatlarni tekshirish va raqamli kriminalistika

Kiberjinoyatlarni tergov qilish maxsus ko'nikma va bilimlarni talab qiladi. Huquq-tartibot idoralari dalillar to'plash, kiberjinoyatchilarni izlash va jinoiy javobgarlikka tortish uchun ish yaratish uchun turli texnika va vositalardan foydalanishi kerak. Ushbu texnikalar va vositalar quyidagilarni o'z ichiga oladi:

1. Tarmoq kriminalistikasi: Bu ruxsatsiz kirishga urinishlar yoki ma'lumotlarni o'tkazib yuborish kabi shubhali faoliyat namunalarini aniqlash uchun tarmoq trafigini tahlil qilishni o'z ichiga oladi;

2. Zararli dasturlarni tahlil qilish: Bu hujumning kelib chiqishi va kiberjinoyatchilar tomonidan qo'llaniladigan taktikani aniqlash uchun zararli dastur kodini tahlil qilishni o'z ichiga oladi;

3. Ijtimoiy muhandislik: Bu shaxslarni maxfiy ma'lumotlarni oshkor qilish yoki ularning xavfsizligiga putur etkazadigan harakatlarni amalga oshirish uchun manipulyatsiya qilish uchun psixologik usullardan foydalanishni o'z ichiga oladi;

4. Kriptografiya: Bu maxfiy xabarlar yoki jinoiy faoliyat maxfiyligini ochish uchun shifrlangan ma'lumotlarni tahlil qilishni o'z ichiga oladi.

Raqamli dalillar anchagina mo'rt bo'lib, to'g'ri ishlatilmasa, osongina yo'qolishi yoki buzilishi mumkin. Huquqni muhofaza qilish idoralari raqamli dalillarni sudda qabul qilinishini ta'minlash uchun to'plash va saqlashga katta e'tibor berishlari kerak. Bu dalillar to'plangan paytdan boshlab sudga taqdim etilgunga qadar ularning ko'rib chiqilishini kuzatib boradigan zanjirini o'rnatishni o'z ichiga oladi.

Huquqni muhofaza qilish organlari raqamli dalillarni olish uchun qonuniy talablardan ham xabardor bo'lishi kerak. Bu order yoki sud qarorini olish yoki chet eldan dalillar olish uchun xalqaro hamkorlar bilan ishlashni o'z ichiga olishi mumkin. Qonuniy talablarga rioya qilmaslik dalillarni suddan chiqarib yuborishga olib kelishi mumkin.

Kiberxavfsizlikning huquqiy asoslari

Kiberxavfsizlik qonunlari va qoidalari kibertahdidlar va hujumlarni yumshatishda hal qiluvchi ahamiyatga ega. Ular huquqni muhofaza qilish organlariga kiberjinoyatchilarni tekshirish va jinoiy javobgarlikka tortish uchun asos yaratadi, shu bilan birga shaxslar va tashkilotlarning kiber tahdidlardan himoyalanishini ta'minlaydi. Misol sifatida keltiradigan bo'lsak, Amerika Qo'shma Shtatlarida kiberxavfsizlik qonunlari va qoidalari federal va shtat darajasida qo'llaniladi. Kiberxavfsizlikni tartibga soluvchi asosiy federal qonunlar qatoriga Kompyuter firibgarligi va suiiste'moli to'g'risidagi qonun (CFAA), Elektron kommunikatsiyalar

maxfiyligi to'g'risidagi qonun (ECPA) va Kiberxavfsizlik ma'lumotlarini almashish to'g'risidagi qonun (CISA) kiradi.

CFAA himoyalangan kompyuter tizimlariga, jumladan, davlat va moliya institutlari tarmoqlariga ruxsatsiz kirishni taqiqlaydi. ECPA elektron xabarlarni, shu jumladan elektron pochta va telefon suhbatlarini ushlash va oshkor qilishni tartibga soladi. CISA kiberhujumlarning oldini olish va ularga javob berish uchun xususiy va davlat tashkilotlari o'rtasida ma'lumot almashishni rag'batlantiradi. Bundan tashqari, davlat darajasidagi qonunlar va qoidalar mavjud bo'lib, ular qo'shimcha yo'l-yo'riq va himoyani ta'minlaydi, masalan, ma'lumotlar buzilishi haqida xabar berish qonunlari.

Kiberxavfsizlik tekshiruvlarida yurisdiktsiya muammolari paydo bo'ladi, chunki kiberhujumlar ko'pincha dunyoning turli joylaridan kelib chiqadi. Kiberjinoyatchilar o'z shaxsi va joylashuvini yashirishi mumkin, bu ularni kuzatish va jinoiy javobgarlikka tortishni qiyinlashtiradi. Bu huquq-tartibot idoralari uchun qiyinchilik tug'diradi, chunki ular xalqaro hamkorlar bilan kiberjinoyatchilarni tergov qilish va jinoiy javobgarlikka tortish uchun ishlashlari kerak.

Xalqaro hamkorlik kibertahdidlarni yumshatishda hal qiluvchi ahamiyatga ega, chunki kiberjinoyat global muammo bo'lib, muvofiqlashtirilgan javob choralarini talab qiladi. Yevropa Kengashining Kiberjinoyatlar to'g'risidagi konventsiyasi, shuningdek, Budapesht konventsiyasi sifatida ham tanilgan, kiberjinoyat qonunlarini uyg'unlashtirish va kiberjinoyatlarni tergov qilishda xalqaro hamkorlikni osonlashtirishga qaratilgan xalqaro shartnomadir. Konvensiya 60 dan ortiq mamlakatlar tomonidan ratifikatsiya qilingan va kiberjinoyatchilikka qarshi kurashda yetakchi xalqaro hujjat hisoblanadi.

Maxfiylik va fuqarolar erkinliklarini himoya qilish kiberxavfsizlik sohasidagi sa'y-harakatlarning muhim jihati hisoblanadi. Huquq-tartibot idoralari kiberjinoyatchilarni tergov qilishlari va jinoiy javobgarlikka tortishlari kerak bo'lsa-da, ular buni shaxslarning huquqlarini buzmaydigan tarzda amalga oshirishlari kerak. Maxfiylikni himoya qilishning bir misoli elektron qurilmalar va ma'lumotlarni qidirish va musodara qilish uchun orderlardan foydalanishdir. Garantlar ehtimoliy sabablarni talab qiladi va tintuv va olib qo'yish qonuniy va mutanosib bo'lishini ta'minlash uchun sud tomonidan tekshirilishi kerak.

Bundan tashqari, kiberxavfsizlik choralari shaxslarning shaxsiy hayoti va fuqarolik erkinliklarini buzishga emas, balki ularni himoya qilishga qaratilgan bo'lishi kerak. Masalan, shifrlash va anonimlashtirish texnologiyalari shaxslarning shaxsiy daxlsizligini himoya qilishi va ma'lumotlar buzilgan taqdirda ularning shaxsiy ma'lumotlari oshkor qilinmasligini ta'minlashi mumkin. Huquqni muhofaza qilish organlari samarali kiberxavfsizlik choralari zarurligini shaxslarning shaxsiy hayoti va fuqarolik erkinliklarini himoya qilish bilan muvozanatlashi kerak.

Huquqni muhofaza qilish organlari xodimlarining kiberxavfsizlik bo'yicha bilim va ko'nikmalarini oshirishda ta'lim va o'qitish dasturlari muhim ahamiyatga ega. Ushbu dasturlar huquqni muhofaza qilish organlari xodimlariga kiberjinoyatlarni tekshirish va kiberhujumlarning oldini olish uchun zarur ko'nikmalarni beradi. Kiberxavfsizlik bo'yicha ta'lim va o'qitish dasturlari tarmoq xavfsizligi, raqamli sud ekspertizasi, hodisalarga javob berish va tahdidlarni razvedka kabi bir qator mavzularni qamrab oladi.

Jamoatchilikni xabardor qilish kampaniyalari kiberxavfsizlik bo'yicha ilg'or tajribalarni ilgari surish va kibertahdidlar haqida xabardorlikni oshirishda muhim ahamiyatga ega. Ushbu kampaniyalar jismoniy shaxslar va tashkilotlarni fishing va zararli dasturlar kabi kiberhujumlardan qanday himoya qilish haqida o'rgatadi. Jamoatchilikni xabardor qilish kampaniyalari, shuningdek, shaxsiy va maxfiy ma'lumotlarga ruxsatsiz kirishni oldini olish uchun kuchli parollar, ikki faktorli autentifikatsiya va boshqa xavfsizlik choralaridan foydalanishni rag'batlantirishi mumkin.

Jamoalar va korxonalar bilan hamkorlik kiberxavfsizlikni kuchaytirishda muhim ahamiyatga ega. Huquqni muhofaza qilish idoralari kiber tahdidlarni aniqlash va yumshatish uchun biznes bilan hamkorlik qilishi mumkin. Bundan tashqari, ular kibertahdidlar haqida xabardorlikni oshirish va kiberxavfsizlik bo'yicha ilg'or tajribalarni ilgari surish uchun jamoat guruhlari bilan ishlashlari mumkin. Ushbu hamkorlik zaifliklarni aniqlashga va kiberxurujlarning oldini olish uchun kiberxavfsizlik choralarini kuchaytirishga yordam beradi..

Huquq-tartibot idoralari kiber hodisalarga tez va samarali javob berishga tayyor bo'lishi kerak, xoh ular davlat idoralariga yoki xususiy sektor tashkilotlariga hujumlar bilan bog'liq. Hodisalarga samarali javob berishning asosiy tarkibiy qismlaridan biri bu hodisalarga javob berish rejalari va protokollarini ishlab chiqishdir. Ushbu rejalar va protokollar huquqni muhofaza qilish organlari xodimlariga har xil turdagi kiber hodisalarga qanday munosabatda bo'lish bo'yicha ko'rsatmalar beradi, jumladan, voqeani qanday aniqlash va ushlab turish, dalillarni qanday saqlash va boshqa idoralar va manfaatdor tomonlar bilan qanday muvofiqlashtirish.

Kiber hodisalar ko'pincha bir nechta agentliklar va manfaatdor tomonlar, jumladan, boshqa huquqni muhofaza qilish idoralari, davlat idoralari, xususiy sektor tashkilotlari va xalqaro hamkorlarni jalb qilishni talab qiladi. Hodisaga samarali javob berish, hodisaning oldini olish va ta'sirni kamaytirishni ta'minlash uchun ushbu tashkilotlar o'rtasida yaqin muvofiqlashtirish va hamkorlikni talab qiladi. Huquq-tartibot idoralari muvofiqlashtirilgan javobni ta'minlash uchun ushbu tuzilmalar bilan aniq aloqa va hamkorlikni yo'lga qo'yishlari kerak.

Hodisaga samarali javob berish uchun o'z vaqtida va samarali muloqot muhim ahamiyatga ega. Huquqni muhofaza qilish organlari kibertahdidlarni tezda aniqlash va baholash va bu ma'lumotlarni boshqa idoralar va manfaatdor tomonlarga etkazish imkoniyatiga ega bo'lishi kerak. Buning uchun mustahkam va xavfsiz aloqa infratuzilmasi, shuningdek, kiber tahdidlarni aniqlash va ularga javob berish uchun o'qitilgan xodimlar kerak bo'ladi.

Texnologik o'zgarishlarning tez sur'ati kiberxavfsizlik tahdidlarini yumshatish vazifasi yuklangan huquqni muhofaza qilish idoralari uchun asosiy muammo hisoblanadi. Sun'iy intellekt va narsalar interneti kabi yangi texnologiyalar yangi zaifliklar va hujum vektorlarini yaratmoqda, ularni hal qilish kerak. Huquqni muhofaza qilish idoralari ushbu o'zgarishlardan xabardor bo'lishlari va kiberjinoyatchilardan oldinda qolish uchun o'z strategiyalari va taktikalarini doimiy ravishda moslashtirishlari kerak.

Kibertahdidlarning doimiy rivojlanib borayotgan tabiati huquq-tartibot idoralaridan paydo bo'layotgan tahdidlarga samarali javob berish uchun o'z malakalari va strategiyalarini doimiy ravishda moslashtirishni talab qiladi. Bu huquqni muhofaza qilish organlari xodimlarini so'nggi

tahdidlar va texnologiyalardan xabardor bo'lishlari uchun doimiy o'qitish va o'qitish, shuningdek, ularning maxsus bilim va ko'nikmalariga ega bo'lish uchun kiberxavfsizlik bo'yicha mutaxassislar bilan hamkorlikni rivojlantirishni o'z ichiga oladi.

Huquqni muhofaza qilish organlari kibertahdidlardan himoya qilish zarurati bilan shaxslar va tashkilotlarning shaxsiy hayoti va fuqarolik erkinliklarini himoya qilish zaruratini muvozanatlashi kerak. Bu fuqarolik erkinliklari va shaxsiy daxlsizlikka potentsial ta'sirni hisobga oladigan kiberxavfsizlik sa'y-harakatlariga puxta va nozik yondashuvni talab qiladi.

So'nggi yillarda kiberjinoyatlar bo'yicha ko'plab shov-shuvli tekshiruvlar o'tkazildi, natijada sud jarayoni muvaffaqiyatli yakunlandi. Ushbu holatlar kiberjinoyatchilarni aniqlash, kuzatish va ushlashda huquqni muhofaza qilish idoralari va kiberxavfsizlik bo'yicha ekspertlar o'rtasidagi samarali hamkorlik muhimligini ko'rsatadi.

Huquqni muhofaza qilish idoralari va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlik ko'plab kiberxavfsizlik tekshiruvlarining muvaffaqiyati uchun muhim ahamiyatga ega. Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislar birgalikda ishlash orqali kibertahdidlarni yanada samarali aniqlash va ularga javob berish uchun o'z resurslari va tajribalarini birlashtirishlari mumkin.

Muvaffaqiyatli hamkorlikning bir misoli Federal, shtat va mahalliy huquq-tartibot idoralari hamda xususiy sektor hamkorlarini kibertahdidlarni tekshirish uchun birlashtirgan FQBning Kiber-ishchi guruhidir. Ishchi guruh ko'plab nufuzli kiberjinoyatchilarni muvaffaqiyatli tergov qilish va jinoiy javobgarlikka tortishda muhim rol o'ynadi.

Yana bir misol, AQSh Kiberqo'mondonligining kiberxavfsizliklarni aniqlash va ularni yumshatish uchun xususiy sektor kiberxavfsizlik firmalari bilan hamkorligi. Hamkorlik natijasida kiber tahdidlarni aniqlash va ularga javob berish uchun innovatsion yangi texnologiyalar va strategiyalar ishlab chiqildi.

Xulosa

Xulosa o'rnida shuni ta'kidlash kerakki, zamonaviy virtual olamda kiberxavfsizlik tushunchasiga bo'lgan e'tibor kundan-kunga ortib bormoqda. Bunga nafaqat bir foydalanuvchining kibermakondagi xavfsizligi, balki biror-bir korxona yoki tashkilot va hattoki, butun davlat miqyosidagi kiberxavfsizlik ham kiradi. Internet olamida xavfsizlikni taminlash foydalanuvchi va virtual makon orqasidagi har bir vosita bilan o'zaro kombinatsion tarzda bog'liq hisoblanadi. Bu bog'liqliklarning mukammal sistemagarammasini o'rgangan holda kiberxafsizlikni taminlash kerakdir.

FOYDALANILGAN ADABIYOTLAR:

7. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O'quv qo'llanma. – T.: «Aloqachi», 2020, 221 bet.

8. Cyber Security Policy Guidebook

9. Jennifer L. Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken

10. NJ Jason Healey Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington

11. D.C. Paul Rohmeyer Information Systems Program Director Howe School of Technology Management Stevens Institute of Technology, Hoboken
12. US-CERT Cybersecurity Tips: https://www.us-cert.gov/ncas/tips
13. National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/