កម្មវិធីសិក្សាជាន់ខ្ពស់នៃ អាយស៊ីធី ពិសេស
សំរាប់ថ្នាក់ដឹកនាំក្នុងជួររដ្ឋាភិបាល

ផ្នែកទី ៦

បណ្តាញ និង សន្តិសុខពត៌មាន និង ឯកជនភាព

ភ្នាក់ងារសន្តិសុខពត៌មានភូរ៉ៃ

Emmanuel C.Lallana

APCICT មជ្ឈមណ្ឌលហ្វឹកហ្វឺន អាស៊ី និង ប៉ាស៊ីហ្វិច សំរាប់វិស័យ បច្ចេកវិទ្យាពត៌មាន និង គមនាគមន៍ សំរាប់ការអភិវឌ្ឍន៍

កម្មវិធីសិក្សាជាន់ខ្ពស់នៃ អេយស៊ីធី សំខាន់ សំរាប់ថ្នាក់ដឹកនាំក្នុងជួរ ឆ្ពោតិចាលបន្ត

មេរៀន ទី ៦: បណ្តាញ និង សន្តិសុខពត៌មាន និង ឯកជនភាព

មជ្ឈមណ្ឌលហ្វឹកហ្វឺន អាស៊ី និង ប៉ាស៊ីហ្វិច
នៃអង្គការសហប្រជាជាតិ សំរាប់វិស័យ បច្ចេកវិទ្យា
ពត៌មានវិទ្យា និង គមនាគមន៍សំរាប់ការអភិវឌ្ឍ (UN-APCICT)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

ទូរស័ព្ទ: +82 32 245 1700-02

ទូរសារ: +82 32 245 7712

អ៊ីម៉ែល: info@unapcict.org

http://www.unapcict.org

ISBN: 978-89-955886-1-1 [94560]

រៀបចំ និង រចនាដោយ: Sccandinavian Publishing Co., Ltd. និង studio triangle

បោះពុម្ពនៅក្នុង: សាធារណរដ្ឋកូរ៉ែ

បុព្វកថា

សតវត្សទី ២១ គឺបានលេចចេញយ៉ាងច្បាស់តាមរយៈការរីកចម្រើននៃផ្នែកទំនាក់ទំនង គ្នាក្នុងចំណោមប្រជាជន នៅក្នុងសាកលលោកនេះ វាគឺជាពិភពលោកមួយដែលឱកាស កំពុងបើកចំហរសំរាប់ប្រជាជនរាប់លាននាក់ ធ្វើការទាក់ទងគ្នាដោយឆ្លងកាត់បច្ចេកវិទ្យាថ្មីជាច្រើន, ការរីកដុះដាល់នៅការទទួលបានពត៌មាននិងចំណេះដឹងចាំបាច់ ដទៃទៀត បានធ្វើឲ្យប្រសើរឡើងគួរឲ្យកត់សម្គាល់សំរាប់ជីវភាពរស់នៅរបស់ប្រជាជននិង ជួយកាត់បន្ថយភាពក្រីក្រផងដែរ ។ រឿងនេះត្រឹមតែអាចទៅរួច ប្រសិនបើការរីកចម្រើននៃផ្នែកទាក់ទងគ្នាគឺត្រូវបានគេឲ្យតម្លៃ ភាពប្តេជ្ញាចិត្ត និង សាមគ្គីភាព ដោយការដាក់បញ្ចូលទាំងការការពារនៃការអភិវឌ្ឍទាំងនោះ ដែលត្រូវ ធ្វើឡើងសំរាប់ មនុស្សគ្រប់គ្នា ។

នៅក្នុងរយៈកាលថ្មីៗនេះ តំបន់អាស៊ីនិងប៉ាស៊ីហ្វិច គឺជាតំបន់ដ៏វិសេសធំបំផុតមួយ នៅពេលដែលតំបន់នេះបានប្រើប្រាស់នៅ បច្ចេកវិទ្យា ពត៌មាន និង គមនាគមន៍ (អាយស៊ីធីអេស) ។ យោងតាមសហគមគមនាគមន៍អន្តរជាតិ តំបន់អាស៊ីនិងប៉ាស៊ីហ្វិចគឺមានផ្ទះ ដែលប្រើប្រាស់ទូរស័ព្ទលើតុច្រើនជាង ពីររយកោដិ និង អ្នក ប្រើប្រាស់ទូរស័ព្ទដៃចំនួន ១.៤ រយកោដិ ។ បើគិតចំពោះតែប្រទេសចិននិងឥណ្ឌានោះគឺស្មើនឹងពាក់កណ្តាល នៃការ ប្រើប្រាស់ ទូរស័ព្ទនៅក្នុងពិភពលោក សម្រាប់ទិន្នន័យគិតត្រឹមឆ្នាំ ២០០៨។ តំបន់អាស៊ីនិងប៉ាស៊ីហ្វិចផងដែរ គឺតំណាងឲ្យ ៤០ ភាគរយ នៃអ្នកប្រើប្រាស់ប្រព័ន្ធអ៊ីនធើរណេតរបស់ពិភពលោក និងជាទីផ្សារនៃការប្រើប្រាស់ រលកអាកាសផ្សព្វផ្សាយដ៏ធំបំផុត នៅក្នុងពិភពលោក គឺ ស្មើនឹង ចំនួន ៣៩ ភាគរយ នៃការចែកចាយសរុបទាំងមូល។

ការជំទាស់ទៅនឹងប្រវត្តិនៃការរីកចម្រើនជឿនលឿនយ៉ាងរហ័សនៃបច្ចេកវិទ្យានេះ មានមតិភាគច្រើនមានមន្ទិលសង្ស័យថា ប្រសិនបើការបែកចែករលកសញ្ញាត្រូវរិនាសបាត់បង់ នឹងទៅជាយ៉ាងម៉េច។ ជាអកុសល ការឆ្លើយ តបនឹងសំនួរនេះនៅមិនទាន់មាននៅឡើយ។ សូម្បីជារយៈពេល ៥ ឆ្នាំហើយ បន្ទាប់ពីជំនួបកំពូលពិភពលោកទៅលើ វិស័យពត៌មានវិទ្យា (The World Summit on The Information Society (ដាប់ប៊ែយូអេសអាយអេស)) ត្រូវ បានធ្វើឡើងនៅក្នុង ជេនណេវ៉ា(Geneva) នៅក្នុងឆ្នាំ ២០០៣ និងថ្វីបើរាល់ការរកឃើញនៃបច្ចេកវិទ្យាដ៏ធំសម្បើម ព្រមទាំងការប្តេជ្ញាចិត្តនៃអ្នកបំរើការងារដល់សំខាន់ៗក្នុងតំបន់ក៏ដោយ ក៏ដំណើរការគមនាគមជាមូលដ្ឋាននៅតែបន្តគម្លាតដ៏ឆ្ងាយពីចំនួនមនុស្សភាគច្រើន ជាពិសេសសំរាប់ជនក្រីក្រ ។

ច្រើនជាង ២៥ ប្រទេសនៃតំបន់មួយ ភាគច្រើនជាប្រទេសកំពុងអភិវឌ្ឍន៍នៃដែនកោះតូចៗ និង ប្រទេសកំពុងអភិវឌ្ឍន៍ដែលមិនមានព្រំដែនជាប់នឹងឆ្នេរសមុទ្រ មានចំនួនអ្នក ប្រើប្រាស់ប្រព័ន្ធអ៊ីនធើរណេតតិចជាង ១០ នាក់ក្នុងចំណោមមនុស្ស ១០០ នាក់ ដែលភាគច្រើនជាអ្នករស់នៅក្នុងទីក្រុងធំៗនៃប្រទេសទាំងនោះ ផ្ទុយទៅវិញ កំឡុងពេលដែលប្រទេសជឿនលឿនដែលស្ថិតនៅក្នុងតំបន់នោះដែរ មានអត្រានៃអ្នកប្រើប្រាស់ប្រព័ន្ធ អ៊ីនធើរណេត ៨០ នាក់ ក្នុងចំណោមមនុស្ស ១០០ នាក់ ។ រលកនៃការផ្សាយរបស់ប្រទេសរីកចំរើន និង ប្រទេសកំពុងអភិវឌ្ឍន៍ គឺមានភាពខុសគ្នាយ៉ាងសម្បើម ។

ដើម្បីភ្ជាប់ការបែងចែកនៃរលកសញ្ញា និង ការធ្វើឲ្យលេចឡើងនៅ អាយស៊ីធី យ៉ាងមានសក្តានុពលមួយនោះ ទាំងទៅក្នុងការអភិវឌ្ឍសង្គមសេដ្ឋកិច្ចវិទ្យានៅក្នុងតំបន់ រួមទាំងអ្នកបង្កើតច្បាប់នៅក្នុងប្រទេសកំពុងអភិវឌ្ឍន៍នោះ ពួកយើងត្រូវការបង្កើតនៅ អទិភាពឲ្យបានច្រើន, អនុម័តនៅគោលនយោបាយមួយចំនួន, រៀបចំយ៉ាងជាក់លាក់នៅ ច្បាប់ និង និយតករគម្រោង, ផ្តល់ប្រាក់មូលនិធិ, និងជួយសម្រួលក្នុងភាពជាដៃគូផ្សេងៗជាច្រើនទៀត ដើម្បីជំរុញ វិស័យ ឧស្សាហកម្ម អាយស៊ីធី ព្រមទាំងធ្វើការអភិវឌ្ឍនៅជំនាញ អាយស៊ីធី ឲ្យដល់ចំណោមប្រជាជនរបស់ពួកគេ ។

ដូចដែលគម្រោងសកម្មភាពមួយ (The Plan of Action) នៃ ដាប់ប៊ែយូអេសអាយអេស(WSIS) បានថ្លែងថា "...រាល់បុគ្គលគួរតែទទួលបាន ឱកាសក្នុងការទទួលយកនៅជំនាញចាំបាច់ណាមួយ រួមទាំងចំណេះដឹង ដើម្បីយល់ដឹង ដើម្បីចូលរួម និងដើម្បីទទួលបានប្រយោជន៍ពីសង្គមពត៌មានវិទ្យា រួមទាំងចំណេះដឹង ផ្នែកសេដ្ឋកិច្ច។" នៅទីបញ្ចប់ គម្រោងសកម្មភាពនេះ បានអំពាវនាវឲ្យមានការសហការនៅក្នុងតំបន់និងជាអន្តរជាតិសំរាប់វិស័យ នៃការកសាង សមត្ថភាព ដោយធ្វើការសង្កត់ធ្ងន់ ទៅលើការបង្កើតការប្រមូលផ្តុំយ៉ាងធំមួយសំរាប់អ្នកមាន វិជ្ជាជីវៈនិងជំនាញការ ខាង អាយស៊ីធី អោយបានច្រើន ។

ជាការឆ្លើយតបនឹងការអំពាវនាវនេះ កីស៊ីអាយស៊ីធី(PCICT) បានធ្វើការអភិវឌ្ឍនៅ អាយស៊ីធី ដ៏ធំទូលាយមួយ នេះសំរាប់ ការអភិវឌ្ឍន៍នៅកម្មវិធីហ្វឹកហ្វឺនដែលមានឈ្មោះថា *កម្មវិធីសិក្សាជាន់ខ្ពស់នៃអាយស៊ីធី ពិសេស សំរាប់ ថ្នាក់ដឹកនាំក្នុងជួររដ្ឋាភិបាល* ដែលក្នុងពេលឥឡូវនេះ មានប្រាំបីវគ្គ ផ្សេងៗពីគ្នាប៉ុន្តែវគ្គនីមួយៗមានទំនាក់ទំនងគ្នា ដោយមានគោលបំណងចែករំលែក ចំណេះដឹងរួមទាំងជំនាញពិសេស

ដែលនឹងជួយអ្នកបង្កើតច្បាប់ ឲ្យមានចិត្តនឹង ប្រើនូវចំណេះដឹង ដែលទទួលបានពី អាយស៊ីធី ប្រកបដោយប្រសិទ្ធិភាព ។

អេភីស៊ីអាយស៊ីធី(APCICT) គឺជាវិទ្យាស្ថានមួយក្នុងចំណោមវិទ្យាស្ថាន ៥ របស់គណកម្មាធិការសង្គមនិងសេដ្ឋកិច្ច នៃ អង្គការសហប្រជាជាតិដែលប្រចាំនៅក្នុងតំបន់អាស៊ីនិងប៉ាស៊ីហ្វិច (the United Nations Economic and Social Commission of Asia and the Pacific (**អ៊ីអេសស៊ីអេភី**(ESCAP)) ។ អ៊ីអេសស៊ីអេភី ជំរុញឲ្យមានការគាំពារនិង ការដាក់បញ្ចូលការអភិវឌ្ឍផ្នែក សេដ្ឋកិច្ចសង្គម ទៅក្នុងអាស៊ីនិងប៉ាស៊ីហ្វិច តាមរយៈការវិភាគ, ការងារសាមញ្ញៗ, ការកសាងសមត្ថភាព, ការសហការក្នុងតំបន់, រួមទាំងការចែករំលែកនៅចំណេះដឹងក្នុងភាពជាដៃគូក្នុងស្រុក និង បណ្តាភាគហ៊ុនផ្សេងៗទៀត, អ៊ីអេសស៊ីអេភី, តាមរយៈ អេភីស៊ីអាយស៊ីធី គឺបាន ទទួលយកការផ្តត់ផ្តង់ចំពោះ ការប្រើប្រាស់ សេចក្តីត្រូវការ និង ការបកប្រែនៃមេរៀនរបស់ អាខេឌឺមិច (Academic) នេះនៅក្នុងប្រទេស ផ្សេងៗពីគ្នាជាច្រើន ព្រមទាំងការចែកចាយយ៉ាងទៀងទាត់របស់ពួកគេដែលធ្វើឡើងជាបន្តបន្ទាប់ តាមរយៈសិក្ខាសាលាថ្នាក់ជាតិនិងតំបន់ សំរាប់មន្ត្រីជាន់ខ្ពស់ និង មន្ត្រីថ្នាក់កណ្តាល រួមទាំងទិសដៅផ្សេងទៀតដែលទាក់ទងនឹង ការកសាងសមត្ថភាពរួម ព្រមទាំងទទួលបានមកវិញនូវចំណេះដឹង ហើយត្រូវបានគេបកប្រែដាក់ បញ្ចូលបន្ថែម ដើម្បីបង្កើនការយល់ដឹងនៃសារៈប្រយោជន៍ អាយស៊ីធី និង សកម្មជាក់ស្តែងឆ្ពោះទៅរកការ អភិវឌ្ឍទិសដៅជាច្រើន ។

Noeleen Heyzer

អនុរដ្ឋលេខាធិការនៃអង្គការសហប្រជាជាតិ
និង លេខាធិការប្រតិបត្តិនៃ អ៊ីអេសស៊ីអេភី

អារម្ភកថា

ដំណើរការនៅក្នុងការរិវត្តនៃ *កម្មវិធីសិក្សាជាន់ខ្ពស់នៃ អាយស៊ីធី ពិសេសសំរាប់ថ្នាក់ដឹកនាំក្នុងជួរ រដ្ឋាភិបាលសម្រាប់វគ្គ បន្ត* នេះ ពិតជាបានបង្ហាញនៅការផុសឡើងនៅបទពិសោធន៍ថ្មីៗ ។ The Academy មិនត្រឹមតែបំពេញបន្ថែមទៅ ក្នុងការកសាងសមត្ថភាពនៃការយល់ដឹងអំពី អាយស៊ីធី ប៉ុន្តែថែមទាំងបានត្រួសត្រាផ្លូវថ្មីមួយសំរាប់ការអភិវឌ្ឍន៍នៅកម្មវិធីសិក្សា (តាមរយៈការចូលរួមរបស់ អ្នកសិក្សា និងភាពជាម្ចាស់នៃការអនុវត្ត) ។

The Academy គឺជាកម្មវិធីដល់ល្អបំផុតរបស់ អេភីស៊ីអាយស៊ីធី, ដែលបានធ្វើការអភិវឌ្ឍន៍ពីងផ្អែកលើ: លទ្ធផល នៃការស្ទង់មតិដ៏ចាំបាច់ជាច្រើនប្រកបដោយភាពទូលំទូលាយ ដែលធ្វើឡើងជាមួយចំនួន ប្រទេសច្រើនជាង ២០ នៅក្នុងតំបន់ រួមទាំងទទួលការប្រឹក្សាយោបល់ពីមន្ត្រីរដ្ឋាភិបាលជាច្រើនរូប, សមាជិកជាច្រើននៃសហគមន៍អភិវឌ្ឍន៍អន្តរជាតិ, កម្មវិធីសិក្សានិងអ្នកអប់រំជាច្រើនរូប, ធ្វើការស្រាវជ្រាវ និងវិភាគយ៉ាងស៊ីជំរៅអំពីភាពខ្លាំង និង ភាពខ្សោយ ចំពោះឧបករណ៍សម្រាប់ការហ្វឹកហ្វឺនដែលមាន ស្រាប់, ប្រតិកម្មតបរបស់អ្នកចូលរួមសិក្ខាសាលារបស់ អេភីស៊ីអាយស៊ីធី ដែលបានរៀបចំឡើងជាបន្ត បន្ទាប់សម្រាប់ថ្នាក់តំបន់ និងអនុតំបន់ទៅលើអត្ថប្រយោជន៍និងភាពជាប់ទាក់ទងគ្នា ពីវគ្គមួយទៅវគ្គមួយ រួមទាំងយុទ្ធសាស្ត្រហ្វឹកហ្វឺនយ៉ាងសមរម្យមួយ, និងមានភាពប្រាកដនិយមនៅក្នុងការរំលឹក ឡើងវិញ អំពីវគ្គទាំងនោះ ដោយមានការដឹកនាំពីអ្នកជំនាញជាច្រើនរូបនៅក្នុងវគ្គសិក្សា សម្រាប់ការអភិវឌ្ឍវិស័យ អាយស៊ីធី ។ សិក្ខាសាលារបស់ The Academy ត្រូវបានធ្វើឡើង តាមតំបន់ដែលបានផ្តល់ ឱកាសដែលមិនអាចកាត់ថ្លៃ បានក្នុងការផ្លាស់ប្តូរបទពិសោធន៍ និងចំណេះដឹងក្នុងចំណោមអ្នកចូលរួមពី ប្រទេសផ្សេងៗ សិក្ខាសាលានេះដែលបានបង្កើតនៅ Academy Alumni នឹងដើរតួយ៉ាងសំខាន់ ក្នុងការធ្វើឲ្យលេចចេញជារូបរាងនៅមេរៀនជាបន្តបន្ទាប់ ។

ការដាក់បង្ហាញចេញដំបូងនៅវគ្គសិក្សាទាំងប្រាំបី សម្គាល់ឃើញថាជាការចាប់ផ្តើមសម្រាប់ដំណើរការ ដ៏ជោគជ័យ ដែលជាភាពខ្លាំងនៃដៃគូដែលមានស្រាប់ និងការកសាងភាពថ្មីផ្សេងមួយទៀតដើម្បីអភិវឌ្ឍ នៅក្នុងការធ្វើឲ្យសម្រេច នៅគោលនយោបាយរបស់ អាយស៊ីធីឌី កាត់តាមតំបន់ ។ អេភីស៊ីអាយស៊ីធី គឺបានប្តេជ្ញាចិត្តជាអ្នកផ្តល់ ក្នុងការផ្គត់ផ្គង់ផ្នែកបច្ចេកទេសនៅក្នុងការផ្សព្វផ្សាយពី National Academies ពីព្រោះថាការឆ្ពោះទៅមុខយ៉ាង សំខាន់របស់វា គឺការធានាថា The Academy គឺចាប់បានរាល់ការ

សម្រេចនៅគោលនយោបាយរបស់ខ្លួន ។ អេភីស៊ីអាយស៊ីធី ផងដែរបាននឹងកំពុងធ្វើការយ៉ាងជិតស្និទ្ធ ជាមួយវិទ្យាស្ថានហ្វឹកហ្វឺនរបស់ជាតិនិងតំបន់មួយចំនួន ដែលមានទំនាក់ទំនងជាមួយការគ្រប់គ្រង ថ្នាក់កណ្តាល, ការគ្រប់គ្រងរបស់រដ្ឋ និងការគ្រប់គ្រង់តាមលំដាប់ថ្នាក់ ប្រចាំតំបន់ ដើម្បីធ្វើឲ្យប្រសើរ ឡើងនៅសមត្ថភាពរបស់ពួកគេក្នុងការឆ្លើយតបនៅតំរូវការ ការបកប្រែ និង ការប្រគល់ ឲ្យនៅមេរៀន នីមួយៗរបស់ Academy ព្រមទាំងធ្វើវាទៅជាសេចក្តីត្រូវការ និងជាអទិភាពដំបូងសម្រាប់រដ្ឋ ។

ច្រើនជាងនេះទៅទៀត អេភីស៊ីអាយស៊ីធី កំពុងតែជួលនៅប៉ុស្តិ៍ជាច្រើនសម្រាប់ការខិតទៅរកការ ធានាមួយថា ខ្លឹមសារមេរៀនរបស់ Academy បានទៅដល់អ្នកមើលក្នុងលក្ខណៈយ៉ាង ទូលំទូលាយ នៅក្នុងតំបន់មួយ ។ ក្រៅពីការផ្តល់ឲ្យជាលក្ខណៈផ្ទាល់របស់ Academy តាមរយៈកម្មវិធីសិក្សា ជាច្រើនរបស់ជាតិនិងតំបន់ Academy ផងដែលផ្តល់ឲ្យជា លក្ខណៈ the APCICT Virtual Academy (អេវីអា(AVA)), គឺជាទម្រង់នៃការសិក្សាពីចម្ងាយ តាមប្រព័ន្ធ Online របស់ Academy, ដែលត្រូវបង្កើតឡើងដើម្បីឲ្យអ្នកសិក្សាទទួល បានចំណេះដឹងពីកន្លែង របស់ខ្លួនគេផ្ទាល់ ។ AVA ធានាថាវគ្គនីមួយៗរបស់ Academy រួមទាំងឧបករណ៍ដទៃទៀត ដូចជា ផ្ទាំងបញ្ចាំងអំពី បទបង្ហាញនៃមេរៀន និង ករណីសិក្សាដទៃទៀត គឺមានភាពងាយស្រួលក្នុងការទាញយកមកពីប្រព័ន្ធ អ៊ីនធើរណិត, ការយកមកប្រើម្តងទៀត, ឆ្លើយតបតាមតំរូវការនិងហានបរិច្ឆេទ រួមទាំងការប្រើប្រាស់នៅលើ មុខងារផ្សេងៗទៀត រួមមាន ការបង្រៀនជា មូលដ្ឋានគ្រឹះ, ការសិក្សាស្វែងយល់ទៅលើការគ្រប់គ្រង ឧបករណ៍ផ្សេងៗ, ខ្លឹមសារមេរៀនស្តីអំពីការអភិវឌ្ឍន៍ទៅលើ ឧបករណ៍មួយចំនួន ព្រមទាំង វិញ្ញាបណ្ណប័ត្រ។

ជាអាទិ៍ការបង្កើតនៅវគ្គទាំងប្រាំបីរបស់ Academy និងការផ្តល់ឲ្យពួកគេតាមរយៈសិក្ខាសាលាស្តីពី Academy របស់ថ្នាក់ជាតិ, ថ្នាក់តំបន់និងអនុតំបន់ និងមិនអាចប្រព្រឹត្តទៅបានប្រសិនបើគ្មានការប្តេជ្ញាចិត្ត ការចង្អុលបង្ហាញនិង ពីអ្នកចូលរួមយ៉ាងសកម្មរបស់ បុគ្គលៗម្នាក់ ឬពីអង្គការជាច្រើននោះទេ ។ ខ្ញុំសូមយកឱកាសនេះ សំដែងនៅសមានចិត្ត សម្រាប់ការប្រឹងប្រែង ព្រមទាំងការសម្រេចនូវស្នាដៃនៃ Academy Alumni ដោយមានការសហការពីក្រសួង រដ្ឋាភិបាល, វិទ្យាស្ថានហ្វឹកហ្វឺន, ព្រមទាំង អង្គការជាតិនិងអង្គការ ប្រចាំតំបន់ជាច្រើនដែលបានចូលរួមក្នុងសិក្ខាសាលា Academy ។ ពួកគេមិន ត្រឹមតែ ផ្តល់នៅទស្សនៈដ៏មានតំលៃជាច្រើន ដើម្បីដាក់បញ្ចូលទៅក្នុងវគ្គនីមួយៗ ប៉ុន្តែថែមទាំង

ដើរតួយ៉ាងសំខាន់ជាច្រើនទៀត ដោយពួកគេបានក្លាយជាអ្នកជួយគាំទ្រ Academy នៅក្នុងប្រទេសពួកគេ ដែលឲ្យជា លទ្ធផលសម្រាប់ការយោគយល់គ្នាជាលក្ខណៈផ្លូវការ រវាង អេភីស៊ីអាយស៊ីធី ជាមួយ វិទ្យាស្ថានរបស់ជាតិ និងតំបន់មួយចំនួន ក្នុងការផ្តល់នៅការឆ្លើយតបតាមតំរូវការ និងការប្រគល់ឲ្យ នៅមុខវិជ្ជារបស់ Academy សម្រាប់ប្រទេសទាំងនោះ យ៉ាងទៀងទាត់ ។

ខ្ញុំសូមសម្តែងនៅសមានចិត្តជាការថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅបំផុត សម្រាប់ការខិតខំប្រឹងប្រែងក្នុង ការចូលរួមពីបុគ្គលដែលប្រកបដោយគតិបណ្ឌិតជាច្រើនរូប ក្នុងការបង្កើតនៅដំណើរការប្រតិបត្តិ ដ៏អស្ចារ្យមួយនេះឲ្យប្រព្រឹត្តទៅ បាន ដែលមានដូចជា លោក Shahid Akhtar, ទីប្រឹក្សាគម្រោងនៃ *The Academy*, Patricia Arinto, Christine Apikul, Publications Manager, និងរាល់អ្នកនិពន្ធ *Academy,* និងក្រុម អេភីស៊ីអាយស៊ីធី ។

ខ្ញុំសង្ឃឹមយ៉ាងស្មោះស្ម័គ្រថា *Academy* មួយនេះនឹងជួយប្រទេសជាច្រើនឲ្យរួចផុតពីចន្លោះប្រហោងក្នុង ការ បណ្តុះបណ្តាលធនធានមនុស្សផ្នែក អាយស៊ីធី, ដកចេញនៅភាពវាំងស្នះក្នុងការទទួលយក អាយស៊ីធី មកប្រើប្រាស់ ដោយផ្ទាល់ខ្លួន ព្រមទាំងជួយជំរុញឲ្យមានការអនុវត្តន៍នៃវិស័យ អាយស៊ីធី ដើម្បីពន្លឿន ការអភិវឌ្ឍវិស័យសេដ្ឋកិច្ចសង្គម រួមទាំង ការសម្រេចបានស្នាដៃក្នុងគោលដៅ រាប់លានផ្សេងទៀត។

Hyeun-Suk Rhee

ប្រធាន

UN-APCICT

អំពីមេរៀនបន្ត

នៅក្នុងយុគសម័យនៃពត៌មានសព្វថ្ងៃ, ភាពងាយស្រួលក្នុងការទាញយកពត៌មាននិងកំពុង ធ្វើការផ្លាស់ប្តូរនៅលើ មធ្យោបាយ សម្រាប់ការរស់នៅ ការធ្វើការងារ និង ការកំសាន្ត របស់ពួកយើង ។ digital economy គឺត្រូវ បានគេស្គាល់ផងដែរថាជា ចំណេះដឹងផ្នែក សេដ្ឋកិច្ច, សេដ្ឋកិច្ចបណ្តាញ ឬ សេដ្ឋកិច្ចសម័យថ្មី, ដែលត្រូវបាន ចង្អុលបង្ហាញដោយការផ្លាស់ប្តូរពីការការផលិតនៅទំនិញទៅជាការ បង្កើតនៅគំនិតជាច្រើន ។ ប្រសិនបើមិនដឹងនៅ ឡើយពីសារៈសំខាន់នៅការរីកចម្រើនក្នុងពេល បច្ចុប្បន្ននេះ ការគូសបញ្ជាក់អំពីការរីកចម្រើនមួយនេះនឹងបានដើរ តួនាទីយ៉ាងសំខាន់ប្រាប់ពី ការរីកចម្រើននៃ វិស័យបច្ចេកវិទ្យា ពត៌មាន និង គមនាគមន៍ (ICT) ទាំងនៅក្នុងវិស័យ សេដ្ឋកិច្ច ក៏ដូចជានៅក្នុង សង្គមទាំងមូលផងដែរ ។

ជារឿយៗ រដ្ឋាភិបាលនៅទូទាំងពិភពលោកបានធ្វើការគិតគូរយ៉ាងខ្លាំងទៅលើការអភិវឌ្ឍន៍វិស័យ ICTs (Information and Communication Technology for Development (ICTD)។ សម្រាប់រដ្ឋាភិបាល ទាំងនេះ ICTD គឺមិនត្រឹម តែដើរតួនាទីអំពី ការអភិវឌ្ឍន៍វិស័យ ឬ ឧស្សាហកម្ម ICT ចំពោះតែសេដ្ឋកិច្ច ប៉ុណ្ណោះ ប៉ុន្តែក៏សម្រាប់ការប្រើប្រាស់លើកត្តាផ្សេងៗទៀតផងដែរ នោះជាហេតុនាំឲ្យមានការលូតលាស់ លើផ្នែក សេដ្ឋកិច្ច ក៏ដូចជាការលូតលាស់របស់សង្គមនិង នយោបាយ ។

ទោះបីយ៉ាងណាក៏ដោយ, ក្នុងចំណោមភាពពិបាកជាច្រើន ដែលរដ្ឋាភិបាលប្រឈមមុខ នៅក្នុងបង្កើត ច្បាប់ ICT គឺថាអ្នកបង្កើតច្បាប់ជាញឹកញាប់គឺមិនស្គាល់ច្បាស់ជាមួយ បច្ចេកទេសណាមួយដែលពួកគេ បាននឹងកំពុងបំពាក់សម្រាប់ការអភិវឌ្ឍន៍ប្រទេសនោះទេ ។ គ្មានបុគ្គលណាម្នាក់អាចធ្វើនៅអ្វីមួយផ្សេង ទៀតដែលខ្លួនមិនបានដឹងអំពីវាបានឡើយ ដូច្នេះ អ្នកបង្កើតច្បាប់ទាំងនោះបានស្ថិតទៅម្ខាងពីការបង្កើត ច្បាប់ ICT ។ ប៉ុន្តែការផ្តល់ភារកិច្ចនោះ ទៅឲ្យអ្នកបច្ចេកទេសគឺជា ការខុសឆ្គង ពីព្រោះជាញឹកញាប់អ្នក បច្ចេកទេសគឺមិនដឹងមុនពីការជាប់ទាក់ទិនគ្នានៃច្បាប់ ជាមួយនឹង បច្ចេកវិទ្យា ដែលពួកគេកំពុងតែ អភិវឌ្ឍន៍និងកំពុងប្រើប្រាស់នោះទេ ។

មេរៀនបន្តនៃ *កម្មវិធីសិក្សាជាន់ខ្ពស់នៃ អាយស៊ីធី(ICT) ពិសេស សម្រាប់ថ្នាក់ដឹកនាំក្នុងជួររដ្ឋាភិបាល* ត្រូវបាន អភិវឌ្ឍន៍ឡើងដោយមជ្ឈមណ្ឌលហ្វឹកហ្វឺន អាស៊ីនិង ប៉ាស៊ីហ្វិចនៃអង្គការសហប្រជាជាតិ

សម្រាប់ការអភិវឌ្ឍវិស័យ បច្ចេកវិទ្យា ពត៌មាន និង គមនាគមន៍ (United Nations Asia and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT)) សម្រាប់ឲ្យ

១. អ្នកបង្កើតច្បាប់ប្រចាំប្រទេស និង កម្រិតអ្នកគ្រប់គ្រងតាមតំបន់ ដែលមានតួនាទីទទួលខុស ត្រូវក្នុងការបង្កើត ច្បាប់ អាយស៊ីធី (ICT) ។

២. មន្ត្រីរដ្ឋាភិបាលដែលទទួលខុសត្រូវសម្រាប់ការអភិវឌ្ឍន៍និងមន្ត្រីដែលជាប់ពាក់ព័ន្ធ ទៅលើ ដំណើរការជាមូលដ្ឋានគ្រឹះរបស់ អាយស៊ីធី(ICT) នឹង

៣. អ្នកគ្រប់គ្រងផ្សេងៗទៀតក្នុងផ្នែកសាធារណ៍ដែលកំពុងស្វះស្វែងរកការជួលពី អាយស៊ីធី (ICT) សម្រាប់បម្រើលើគម្រោងនៃការគ្រប់គ្រងណាមួយ ។

មេរៀនបន្តនេះមានគោលបំនងដើម្បីអភិវឌ្ឍឲ្យថ្មឹកជាមួយបញ្ហាសំខាន់ៗជាច្រើន ដែលមានការទាក់ទងនឹង អាយស៊ីធី (ICT) ដែលបានមកទាំងពីច្បាប់ រួមទាំង ទស្សនវិស័យនៃបច្ចេកវិទ្យា។ គ្មានការប៉ុនប៉ងណាមួយក្នុងការអភិវឌ្ឍវិស័យ អាយស៊ីធី(ICT) ដែលដំណើរការដោយដៃ ប៉ុន្តែវាបែរជាផ្តល់នៅការយល់ដឹងដល់ល្អចំពោះសមត្ថភាពនៃបច្ចេកវិទ្យាថ្មីរបស់ប្រព័ន្ធឌីជីថល (Digital) ឬនៅកន្លែងណាដែលបច្ចេកវិទ្យាមានការនាំមុខគេ និងអ្វីដែលគួស បញ្ជាក់សម្រាប់ការ បង្កើតច្បាប់របស់ អាយស៊ីធី(ICT) ។ ប្រធានបទជាច្រើនក្នុងមេរៀនទាំងនេះ ត្រូវបានដឹងមកតាមរយៈការវិភាគពី សេចក្តីត្រូវការនានានៃវគ្គហ្វឹកហ្វឺន និង ការស្ទាបស្ទង់ពីឧបករណ៍ហ្វឹកហ្វឺនដទៃទៀតពីជុំវិញពិភពលោក ។

មេរៀនទាំងនេះត្រូវបានរៀបចំឡើងដូចជាមធ្យោបាយមួយ ដែលអាចត្រូវបានគេប្រើប្រាស់ ក្នុងការសិក្សាផ្ទាល់ខ្លួន ដោយអ្នកអានម្នាក់ៗ ឬក៏ជាប្រភពមួយនៅក្នុងកម្មវិធីសិក្សា ឬ សម្រាប់វគ្គ ហ្វឹកហ្វឺនណាមួយ ។ មេរៀនគឺមួយៗដាច់ ដោយឡែកពីគ្នា តែដូចជាត្រូវបានចងភ្ជាប់បញ្ចូលគ្នាតែមួយ រួមទាំងការខិតខំព្យាយាមធ្វើនៅមេរៀននីមួយៗនេះតភ្ជាប់គ្នាទៅនឹងវិជ្ជានិពន្ធខ្លីៗ រួមទាំងបទពិភាក្សា មួយចំនួនដែលមាននៅក្នុងមេរៀនផ្សេងៗទៀតជាបន្តមក ។ គោលបំណង ក្នុងរយៈពេលវែងគឺការបង្កើត មេរៀនទាំងនោះឲ្យមានភាពជាប់ប្រទាក់គ្នា ដែលអាចត្រូវបានទទួលស្គាល់ជាផ្លូវការ ។

មេរៀននីមួយៗចាប់ផ្តើមជាមួយការប្រាប់ពីគោលបំណងនៃមេរៀននោះ និងទិសដៅនៃលទ្ធផលនៃការសិក្សា ដែលបានមកពីការប្រឆាំងតបតរបស់អ្នកអានចំពោះអ្វីដែលពួកគេបានសិក្សា ការធ្វើដូច្នោះអាច

ធ្វើឲ្យពួកគេប៉ាន់ប្រមាណបាននៅភាពរីកចម្រើនផ្ទាល់ខ្លួនរបស់ពួកគេ។ មាតិកាមេរៀនគឺត្រូវបានចែកចេញជាផ្នែកៗ ដែលរួមមានទាំងផ្នែក មេរៀន និង លំហាត់ ដើម្បីជាជំនួយឲ្យរឹតតែយល់ដឹងកាន់តែច្បាស់អំពីគន្លឹះសំខាន់ៗនៃមេរៀន ។ លំហាត់ ទាំងនោះ អាចធ្វើដោយអ្នកអានរៀងៗខ្លួន ឬ អាចដោះស្រាយជាលក្ខណៈជាក្រុមនៃអ្នកចូលរួមវគ្គហ្វឹកហ្វឺននោះ ។ ដើម្បីគូសបញ្ជាក់នៅទិដ្ឋភាពជាក់លាក់ទៅលើចំនុចនីមួយៗនោះ រូបភាព និង តារាង គឺត្រូវបានប្រើប្រាស់សម្រាប់ការលម្អិតខ្លឹមសារទាំងនោះ ។ ឯកសារយោង និង ប្រភពមួយចំនួនពីអ៊ីនធើរណិត គឺបានរាយជាបញ្ជីសម្រាប់អ្នកអានធ្វើការស្វែងរក ដើម្បីជាជំនួយបន្ថែមទៅលើការសិក្សានេះ ។

របៀបរៀបចំនៃ អាយស៊ីធីឌី(ICTD) គឺដូចជាមានលក្ខណៈផ្សេងៗពីគ្នា ដែលពេលខ្លះផ្នែក មេរៀន និង លំហាត់ អាចមានភាពផ្ទុយគ្នា ។ ករណីនេះគឺត្រូវបានរំពឹងថាមាននៅក្នុងការរៀបចំនេះ ។ ហើយករណីនេះ គឺគ្រាន់តែធ្វើឲ្យមានភាពភ្ញាក់ផ្អើល និង ប្រកបដោយភាពប្រកួតប្រជែងអំពីការផ្ទុសឡើងនៅរបៀបអប់រំថ្មីៗ និង ភាពប៉ិនប្រសប់របស់វា ដូចដែលរាល់ប្រទេស លើពិភពលោកទាំងអស់ ចាប់ផ្តើមព្យាយាមរុករកនៅសក្តានុពលនៃ អាយស៊ីធីអេស(ICTs) ដើម្បីប្រើប្រាស់សម្រាប់ការអភិវឌ្ឍន៍ដូច្នោះដែរ ។

គាំទ្រឲ្យមានការបោះពុម្ពនៅមេរៀន Academy បន្ទាប់ជាលក្ខណៈ សិក្សាពីចម្ងាយនៅលើ ប្រព័ន្ធអនឡាយន៍(Online) □ the APCICT Virtual Academy (AVA http://www.unapcict.org/academy) ដែលមានលក្ខណៈដូចជា ការសិក្សាក្នុងបន្ទប់រៀនពិតៗ ដែលបទបង្ហាញក្នុងមេរៀននីមួយៗ អ្នកបង្រៀនគឺធ្វើឡើងក្នុង ទម្រង់ជា វីដេអូ និង PowerPoint សម្រាប់ការមេរៀនទាំងនោះ ។

បន្ថែមលើនេះទៀត អេភីស៊ីអាយស៊ីធី(APCICT) បានធ្វើការវិវឌ្ឍន៍ជាមណ្ឌលសហការតាមប្រព័ន្ធអេឡិចត្រូនិច (e-Collaborative Hub) សម្រាប់ ICTD (e-Co Hub □ http://www.Unapcict.org/ecohub), រៀបសាយដែលបាន បង្ហាញនេះ សម្រាប់អ្នកហ្វឹកហាត់ និង អ្នកបង្កើតច្បាប់ ICTD ផ្លាស់ប្តូរបទពិសោធន៍នៃការហ្វឹកហ្វឺន និង ការសិក្សា របស់ពួកគេ ។ e-Co Hub មួយនេះអនុញ្ញាតឲ្យធ្វើការស្វែងយល់ចំពោះប្រភពចំណេះដឹងទៅលើទិដ្ឋភាពផ្សេងៗពីគ្នា នៃ ICTD និងផ្តល់នៅកន្លែងទំនេរសម្រាប់ការអនុវត្តទៅវិញទៅមកក្នុងការចែករំលែកនៅចំណេះដឹង ព្រមទាំង បទពិសោធន៍, និង ជាការសហការដើម្បីពន្លឿនលើវិស័យ អាយស៊ីធីឌី(ICTD)។

មេរៀនទី៦

នៅក្នុងយុគ្គសម័យព័ត៌មានវិទ្យា ព័ត៌មានគឺជាទ្រព្យសម្បត្តិមួយដែលត្រូវបានគេការពារហើយអ្នកច្បាប់នានាក៏ត្រូវការដើម្បីដឹងពីអ្វីជាសន្តិសុខព័ត៌មាន និងរបៀបម៉េចដែលត្រូវធ្វើដើម្បីប្រឆាំងនឹងការលេចធ្លាយព័ត៌មានរួមទាំងព័ត៌មានត្រូវបានគេរំលោភលើ។ មេរៀននេះផ្តល់នៅកំរិតចាំបាច់មួយចំនួនសម្រាប់សន្តិសុខព័ត៌មាន និន្នាការ និងបញ្ហាសន្តិសុខព័ត៌មាននានា រួមទាំងដំណើរការនៃការបង្កើតយុទ្ធសាស្ត្រគំរូនៃសន្តិសុខព័ត៌មាន។

គោលបំណងមេរៀន:

បំណងរបស់មេរៀនគឺ:

១. បញ្ជាក់អំពីគំនិតនៃសន្តិសុខព័ត៌មាន ឯកជនភាពនិងគំនិតដែលជាប់ពាក់ព័ន្ធផ្សេងៗទៀត ។

២. ពិពណ៌នាអំពីការគំរាមកំហែងលើសន្តិសុខព័ត៌មាន និងរបៀបម៉េចដែលការគំរាមកំហែងនោះអាច ត្រូវបានធ្វើជាមួយ។

៣. ពិភាក្សាលើសេចក្តីស្នើនានាសម្រាប់ការបង្កើត និងអនុវត្តច្បាប់នៅលើសន្តិសុខព័ត៌មាន ក៏ដូច ដែលអាយុកាលនៃច្បាប់សន្តិសុខព័ត៌មាន។

៤. ផ្តល់នៅការរលឹកឡើងវិញនៅគំរូនានានៃសន្តិសុខពត័ត៌មាននិងការការពារឯកជនភាពដែលត្រូវបានប្រើដោយប្រទេសមួយចំនួន និង អង្គការសន្តិសុខពត៌មានអន្តរជាតិ ។

លទ្ធផលទទួលបានពីការសិក្សា:

បន្ទាប់ពីការសិក្សានៅមេរៀននេះហើយអ្នកសិក្សាគួរតែអាច៖

១. អោយនិយមន័យអំពីសន្តិសុខព័ត៌មាន ឯកជនភាព និងគោលគំនិតដែលទាក់ទងមួយចំនួនផ្សេងទៀត។

២. ស្គាល់ពីភាពគំរាមកំហែងនានាចំពោះសន្តិសុខព័ត៌មាន

៣. ប៉ាន់ប្រមាណមើលនៅច្បាប់សន្តិសុខព័ត៌មានដែលមានស្រាប់នៅក្នុងច្បាប់សន្តិសុខព័ត៌មានអន្តរជាតិ រួមទាំងការការពារជាឯកជនភាព និង

៤. បង្កើតរូបមន្ត ឬជាអនុសាស្ត្រនានាក្នុងការយល់ឃើញទៅលើច្បាប់សន្តិសុខព័ត៌មានដែលមានលក្ខណៈសមរម្យចំពោះច្បាប់នេះ

តារាងមាតិកា

បញ្ជីផ្នែកសិក្សាស្វែងយល់

បញ្ជីឆ្លាន់រូបភាព

បញ្ជីតារាងនានា

អក្សរកាត់

APCERT	ក្រុមទទួលខុសត្រូវបន្ទាន់ផ្នែកកុំព្យូទ័រនៃអាស៊ីប៉ាស៊ីហ្វិក
APCICT	មជ្ឈមណ្ឌលហ្វឹកហ្វឺនអាស៊ីប៉ាស៊ីហ្វិចសម្រាប់បច្ចេកវិទ្យាព័ត៌មានវិទ្យា និងគមនាគមន៍សម្រាប់ការអភិវឌ្ឍន៍
APEC	សហប្រតិបត្តិការសេដ្ឋកិច្ចអាស៊ីប៉ាស៊ីហ្វិច
BPM	ការការពារធ្វើដោយដៃសម្រាប់ Beseline
BSI	វិទ្យាស្ថានគំរូរបស់ចក្រភពអង់គ្លេស
BSI	Bundesamt (មើលក្នុងឯកសារ)
CAP	សមាជិកដែលមានវិញ្ញាបនប័ត្រ
CC	លក្ខណៈវិនិច្ឆ័យ
CCP	សមាជិកដែលទទួលស្គាល់វិញ្ញាបនប័ត្រលើការប្រើ
CCRA	ការរៀបចំលើការទទួលស្គាល់លក្ខណៈវិនិច្ឆ័យសាមញ្ញៗ
CECC	សន្និបាតគណៈរដ្ឋមន្ត្រីអឺរ៉ុបលើរលកសញ្ញាឧក្រិដ្ឋកម្ម
CERT	ក្រុមទទួលខុសត្រូវបន្ទាន់លើផ្នែកកុំព្យូទ័រ
CERT/CC	មជ្ឈមណ្ឌលសហប្រតិបត្តិការនៃក្រុមទទួលខុសត្រូវបន្ទាន់លើផ្នែកកុំព្យូទ័រ
CIIP	ការការពារហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានសំខាន់ៗ
CISA	សវនកម្មធានារ៉ាប់រងលើប្រព័ន្ធព័ត៌មាន
CISO	មន្ត្រីសន្តិសុខព័ត៌មានសម្បង
CISSP	អ្នកជំនាញការធានារ៉ាប់រងប្រព័ន្ធសន្តិសុខព័ត៌មាន
CM	ការគ្រប់គ្រងលើរូបរាង
CSEA	សកម្មភាពបង្កើនរលកសញ្ញាសន្តិសុខ
CSIRT	ក្រុមទទួលខុសត្រូវលើឧបទ្ទវហេតុសន្តិសុខលើប្រព័ន្ធកុំព្យូទ័រ
DID	ការការពារដ៏រឹងមាំ
DNS	Domain Name System
Dos	Denial-of-Service
ECPA	សកម្មភាពឯកជនភាពនៃគមនាគមន៍អេឡិចត្រូនិចនានា
EGC	ក្រុមទទួលខុសត្រូវបន្ទាន់លើកុំព្យូទ័រនៃរដ្ឋាភិបាលអឺរ៉ុប
ENISA	ភ្នាក់ងារសន្តិសុខព័ត៌មាន និងបណ្តាញរបស់អឺរ៉ុប
ERM	ការគ្រប់គ្រងហានិភ័យសហគ្រាស
EU	សហគមអឺរ៉ុប
FEMA	ភ្នាក់ងារគ្រប់គ្រងបន្ទាន់នៃសហព័ន្ធ
FIRST	វេទិកានៃការទទួលខុសត្រូវលើឧបទ្ទវហេតុ និងក្រុមសន្តិសុខនានា

FISMA	សកម្មភាពគ្រប់គ្រងសន្តិសុខព័ត៌មាននៃសហព័ន្ធ
FOI	ឯករាជ្យភាពនៃព័ត៌មាន
GCA	របៀបវារៈនៃរលកសញ្ញាសន្តិសុខជាសាកល
HTTP	ពិធិការបញ្ជូនជាលក្ខណៈ Hypertext
ICT	បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មានវិទ្យា
ICTD	បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មានវិទ្យាសម្រាប់ការអភិវឌ្ឍន៍
IDS	ប្រព័ន្ធការពារនៃការរំលោភបំពាន
IGF	វេទិកាស្តីពីការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធើរណិត
IM	ការបញ្ជូនសាររហ័ស
IPS	ប្រព័ន្ធទប់ស្កាត់ការរំលោភបំពាន
ISACA	សហគមសាវនកម្ម និងត្រួតពិនិត្យលើប្រព័ន្ធព័ត៌មាន
ISMS	ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន
ISO/IEC	អង្គការអន្តរជាតិសម្រាប់គំរូភាវូបនីយកម្មនិងគណៈកម្មាធិការអេឡិចត្រូនិចអន្តរជាតិ
ISP	អ្នកផ្តល់សេវាកម្មផ្នែកប្រព័ន្ធអ៊ីនធើរណិត
ISP/NSP	អ្នកផ្តល់សេវាកម្មផ្នែកបណ្តាញ និងអ៊ីនធើរណិត
IT	បច្ចេកវិទ្យាព័ត៌មានវិទ្យា
ITU	សហគមទូរគមនាគមន៍អន្តរជាតិ
ITU-D	ផ្នែកអភិវឌ្ឍន៍សហគមទូរគមនាគមន៍អន្តរជាតិ
ITU-R	ផ្នែកគមនាគមន៍វិទ្យុសហគមទូរគមនាគមន៍អន្តរជាតិ
ITU-T	ផ្នែកគំរូភាវូបនីយកម្មសហគមទូរគមនាគមន៍អន្តរជាតិ
KISA	ភ្នាក់ងារសន្តិសុខព័ត៌មានប្រទេសកូរ៉េ
MIC	ក្រសួងព័ត៌មាន និងគមនាគមន៍ សាធារណៈរដ្ឋកូរ៉េ
NIS	សន្តិសុខព័ត៌មាន និងបណ្តាញ
NISC	មជ្ឈមណ្ឌលសន្តិសុខព័ត៌មានជាតិ ប្រទេសជប៉ុន
NIST	វិទ្យាស្ថានគំរូ និងបច្ចេកវិទ្យាជាតិ សហរដ្ឋអាមេរិក
OECD	អង្គការសម្រាប់កិច្ចសហប្រតិបត្តិការ និងការអភិវឌ្ឍន៍សេដ្ឋកិច្ច
OMB	ការិយាល័យគ្រប់គ្រង និងគម្រោងថវិកា សហរដ្ឋអាមេរិក
OTP	One-Time-Passwords
PC	កុំព្យូទ័រផ្ទាល់ខ្លួន
PP	ការការពារឯកសារ
PSG	ក្រុមពហុភាគហ៊ុនអចិន្ត្រៃយ៍
RFID	ការកំនត់រលកសញ្ញានៃការផ្សាយវិទ្យុ

SAC	សមាសភាពធានារ៉ាប់រងសន្តិសុខ
SFR	តម្រូវការនៃមុខងារសន្តិសុខ
SME	សហគ្រាសធុនតូច និងមធ្យម
ST	ទិសដៅសន្តិសុខ
TEL	ក្រុមការងារព័ត៌មាន និងទូរគមនាគមន៍
TOE	ទិសដៅនៃការវាយតម្លៃ
TSF	មុខងារសន្តិសុខ TOE
UK	ចក្រភពអង់គ្លេស
UN	អង្គការសហប្រជាជាតិ
US	សហរដ្ឋ
USA	សហរដ្ឋអាមេរិក
WPISP	គណៈបក្សការងារនៅលើផ្នែកសន្តិសុខព័ត៌មាន និងឯកជនភាព
WSIS	ជំនួបកំពូលពិភពលោកស្តីពីសន្តិសុខព័ត៌មាន

បញ្ជីនៃសញ្ញាសំគាល់

សញ្ញាសម្រាប់ផ្នែកសិក្សា

សំនួរត្រិះរិះ

អ្វីដែលត្រូវអនុវត្ត/ការងារដែលត្រូវធ្វើ

សាកល្បងខ្លួនអ្នក

១. សេចក្តីត្រូវការសម្រាប់សន្តិសុខព័ត៌មាន

ចំនុចនេះមានគោលដៅទៅលើ៖

- ពន្យល់ទៅលើគោលគំនិតនៃព័ត៌មាន និងសន្តិសុខព័ត៌មាន និង
- ពិពណ៌នាពីគំរូផ្សេងៗដែលត្រូវបានប្រើប្រាស់ចំពោះសកម្មភាពនានារបស់សន្តិសុខព័ត៌មាន

ជីវិតមនុស្សសព្វថ្ងៃគឺពឹងផ្អែកយ៉ាងខ្លាំងទៅលើបច្ចេកវិទ្យាព័ត៌ និងគមនាគមន៍ (ICT)។ នេះធ្វើឲ្យអ្នកប្រើប្រាស់ផ្ទាល់ខ្លួន អង្គការ និងជាតិនានាទទួលរងគ្រោះថ្នាក់ខ្ពស់ដោយសារការវាយប្រហារលើប្រព័ន្ធព័ត៌មាន ដូចជា ការលួចយកព័ត៌មាន រលកសញ្ញានៃភេរវកម្ម រលកសញ្ញាឧក្រិដ្ឋកម្ម និងទៅតាមអ្វីដែលពួកគេចូលចិត្ត។អ្នកប្រើប្រាស់ផ្ទាល់ខ្លួន និងអង្គការមួយចំនួនក៏ត្រូវបានផ្តល់ការផ្តត់ផ្តង់ដើម្បីដោះស្រាយលើការលុកលុយនេះ។ រដ្ឋាភិបាលជាច្រើនមានតួនាទីយ៉ាងសំខាន់ដើម្បីដើរតួនៅក្នុងការធានាសន្តិសុខព័ត៌មានដោយការពង្រីកហេដ្ឋារចនាសម្ព័ន្ធគមនាគមន៍ព័ត៌មាន និងការបង្កើតនៅប្រព័ន្ធនានាដើម្បីការប្រឆាំងនឹងការគំរាមកំហែងនានាលើសន្តិសុខព័ត៌មាន។

១.១ គោលគំនិតមូលដ្ឋានផ្សេងៗនៅក្នុងសន្តិសុខព័ត៌មាន

អ្វីជា "ព័ត៌មាន"?

ជាទូទៅព័ត៌មានគឺត្រូវបានឲ្យនិយមន័យថាជាលទ្ធផលនៃសកម្មភាពខាងគំនិតបញ្ញា។ វាគឺជាផលិតផលអរូបីដែលត្រូវបានបញ្ជូនតាមរយៈព័ត៌មាន។ នៅក្នុងវគ្គសិក្សា ICT ព័ត៌មានគឺជាលទ្ធផលនៃការប្រតិបត្តិការរៀបចំ និងចាត់ចែងនៅទិន្នន័យដែលបានមកពីការប្រមូលជាធម្មតាៗពីហេតុការណ៍នានា។

នៅក្នុងវគ្គសិក្សាពីសន្តិសុខព័ត៌មាន ព័ត៌មានគឺត្រូវបានកំនត់ថា "ទ្រព្យសម្បត្តិមួយ" ។ វាគឺជាអ្វីៗដែលមានតម្លៃ និងគួរត្រូវបានការពារ។ ISO/IEC 27001 នេះកំណត់អត្ថន័យនៃព័ត៌មាន និងសន្តិសុខព័ត៌មានតាមរយៈ ការពិពណ៌នានៅក្នុងមេរៀននេះ។

តម្លៃដែលត្រូវបានផ្តល់ទៅឲ្យព័ត៌មានសព្វថ្ងៃជាឥទ្ធិពលទៅលើការផ្លាស់ប្តូរសង្គមពីសង្គមកសិកម្មទៅកាន់សង្គមឧស្សាហកម្ម និងជាចុងក្រោយគឺសង្គមមួយដែលបែរទៅរកសង្គមព័ត៌មានវិទ្យា។ នៅក្នុងសង្គមនានា ដីគឺជាទ្រព្យសម្បត្តិដ៏សំខាន់បំផុតហើយប្រទេសដែលសំបូរទៅដោយផលានុផលមានកំលាំងនៃការប្រកួតប្រជែងខ្លាំង។ នៅក្នុងសង្គមឧស្សាហកម្មនានាភាពខ្លាំងនៃប្រទេស ដូចជាការមានប្រេងចំរុងទុក គឺជាកត្តាសំខាន់នៅក្នុងការប្រកួតប្រជែង។ នៅក្នុងសង្គមចំណេះដឹង និងការងារបែរទៅរកព័ត៌មានវិទ្យា ព័ត៌មានគឺជាទ្រព្យសម្បត្តិដ៏សំខាន់បំផុត និងសមត្ថភាព នៃការប្រមូល ការវិភាគនិងប្រើនៅព័ត៌មានគឺជាផលើប្រយោជន៍សម្រាប់ការប្រកួតប្រជែងសម្រាប់ប្រទេស**មួយចំនួន**។

ពីព្រោះតែទស្សន:វិស័យបានប្តូរពីការឲ្យតម្លៃទៅលើទ្រព្យពិតទៅឲ្យតម្លៃលើព័ត៌មានវិញនោះគឺធ្វើឲ្យមានកិច្ចព្រមព្រាងគ្នាកាន់តែច្រើនថាព័ត៌មានត្រូវការទទួលបាននូវការការពារ។ព័ត៌មានខ្លួនវាគឺត្រូវបានឲ្យតម្លៃច្រើនជាងបណ្តាញព័ត៌មានដែលគ្រប់គ្រងព័ត៌មាននេះ។

តារាង១. ការប្រៀបធៀបទ្រព្យសម្បត្តិជាព័ត៌មាន និងទ្រព្យសម្បត្តិពិត

លក្ខណៈ	**ទ្រព្យសម្បត្តិជាព័ត៌មាន**	**ទ្រព្យសម្បត្តិពិត**
ទម្រង់-ការថែទាំ	មិនមានរូបរាងពិត និងអាចបត់បែនទៅតាមកាល:ទេស:	មានរូបរាងពិតប្រាកដ
តម្លៃ-ភាពប្រែប្រួល	ទទួលបានតម្លៃខ្ពស់នៅពេលដែលវាត្រូវបានបញ្ចូលគ្នា និងដំណើរការរួមគ្នា	តម្លៃសរុបគឺបានមកពីការបូកបញ្ចូលគ្នានៃតម្លៃនិមួយៗ
ការចែករំលែក	ទ្រព្យសម្បត្តិព័ត៌មានអាចផលិតឡើងវិញបានដោយគ្មានដែនកំណត់ និងប្រជាជន ឬអ្នកប្រើប្រាស់អាចចែករំលែកគ្នាលើការប្រើប្រាស់វា	ការមានឡើងវិញគឺមិនអាចទៅរួច ហើយប្រើកាន់តែច្រើនវាកាន់តែរិចរិល
បណ្តាញផ្សព្វផ្សាយ-ភាពមិនឯករាជ្យ	ត្រូវការចែកចាយតាមបណ្តាញផ្សព្វផ្សាយ	អាចចែកបានដោយឯករាជ្យ (ពីព្រោះវាស្ថិតនៅក្នុងរូបរាងពិត)

ដូចដែលបានបង្ហាញក្នុងតារាងទី១. ទ្រព្យសម្បត្តិព័ត៌មានគឺមានភាពផ្សេងគ្នាដាច់ស្រឡះពីទ្រព្យសម្បត្តិពិតៗ។ដូច្នេះទ្រព្យសម្បត្តិជាព័ត៌មានគឺងាយស្រួលទទួលនៅភ័យន្តរាយផ្សេងៗ

ហានិភ័យនានាកើតឡើងចំពោះទ្រព្យសម្បត្តិជាព័ត៌មាន

ពីព្រោះតម្លៃនៃទ្រព្យសម្បត្តិដែលជាព័ត៌មាននោះបានកើនឡើង ការសម្រេចឲ្យមានសិទ្ធិក្នុងការប្រើប្រាស់នៅព័ត៌មាន និងមានសិទ្ធិត្រួតត្រាលើវានេះក៏មានចំនួនមនុស្សច្រើនផងដែរ។ ក្រុមជាច្រើនត្រូវបានបង្កើតឡើងដើម្បីប្រើប្រាស់លើទ្រព្យសម្បត្តិដែលជាព័ត៌មានទាំងនោះក្នុងគោលបំណងផ្សេងៗពីគ្នា និងការខិតខំប្រឹងប្រែងយ៉ាងខ្លាំងក្លាមួយចំនួនដើម្បីយកឲ្យបាននៅទ្រព្យសម្បត្តិជាព័ត៌មាននោះទៅតាមអ្វីក៏ដោយឲ្យតែគេចង់បាន។ ហើយក្រោយមកទៀតក៏មានការលួចយកព័ត៌មាន ប្លន់ បំផ្លាញនៅប្រព័ន្ធព័ត៌មានតាមរយៈមេរោគនានារបស់កុំព្យូទ័រ និងតាមវិធីផ្សេងៗ។ ហានិភ័យទាំងនេះដែលមាននៅក្នុងព័ត៌មានភាវូបនីយកម្មគឺត្រូវបានគេលើយកមកពិភាក្សានៅក្នុងចំនុចទី២នៃមេរៀននេះ។

ទិដ្ឋភាពជាអវិជ្ជមាននៃបរិដ្ឋាននានាចំពោះទិសដៅទៅរកព័ត៌មាននេះរួមមានដូចខាងក្រោម៖

ការកើនឡើងក្នុងលក្ខណៈគ្មានសីលធម៌ដែលកើតចេញពីភពអនាមិក - ICT អាចត្រូវបានគេប្រើដើម្បីការពារនៅភាពអនាមិកដែលបង្កលក្ខណៈងាយស្រួលសម្រាប់បុគ្គលម្នាក់ៗជាប់ពាក់ព័ន្ធនៅក្នុងការធ្វើនៅលក្ខណៈដែលគ្មានសីលធម៌ឬបែបឧក្រិដ្ឋកម្ម រួមមានការទទួលបានព័ត៌មានដែលមិនមានភាពត្រឹមត្រូវតាមច្បាប់។

ផលប៉ះពាល់ទៅលើភាពជាម្ចាស់ព័ត៌មាន និងការត្រួតត្រាលើវា - ភាបស្មុគស្មាញនានាបណ្តាលមកពីម្ចាស់ព័ត៌មាន និងការត្រួតត្រាលើវានោះបានកើនឡើងជាមួយការរីកធំធាត់នៃព័ត៌មានភាវូបនីយកម្ម។ ឧទាហរណ៍: រដ្ឋាភិបាលស្វះស្វែងរកការបង្កើតប្រព័ន្ធគ្រប់គ្រងទិន្នន័យលើព័ត៌មានផ្ទាល់ខ្លួននៃបុគ្គលម្នាក់ៗស្ថិតនៅក្រោមស្លាករបស់ “e-government” ផ្នែកខ្លះបានបង្ហាញពីចម្ងល់ទៅលើភាពរាតត្បាតណាមួយដែលអាចទៅរួចចំពោះព័ត៌មានផ្ទាល់ខ្លួនពីការបើកបង្ហាញនៅព័ត៌មាននោះទៅកាន់ផ្នែកផ្សេងៗទៀត។

ព័ត៌មាន និងទ្រព្យសម្បត្តិធ្វើឲ្យញែកចេញពីគ្នារវាងវណ្ណៈ និងប្រទេសនានា - ទំហំនសការកាន់កាប់ទ្រព្យសម្បត្តិដែលជាព័ត៌មានអាចជាការវាស់ស្ទង់នៅទ្រព្យសម្បត្តិរបស់អ្នកកាន់កាប់នោះនៅក្នុងសង្គម ចំណោះ

ដឹង/សង្គមដែលមានទិសដៅទៅខាងព័ត៌មានវិទ្យាទាំងនោះ។ ប្រទេសរីកចំរើនមានសមត្ថភាពផលិតនៅព័ត៌មានជាច្រើនហើយទទួលបានប្រាក់ចំណេញពីការលក់នៅព័ត៌មានទាំងនោះដូចជាផលិតផល។ ម្យ៉ាងវិញតៀតសម្រាប់ប្រទេសអ្នកក្រត្រូវការ បណ្តាក់ទុនយ៉ាងច្រើនទើបអាចដំណើរការលើព័ត៌មាននោះបាន។

ការកើនឡើងសម្រាប់ការផ្សព្វផ្សាយព័ត៌មានបណ្តាលមកពីបណ្តាញសំខាន់ៗជាច្រើន - សង្គមចំណេះដឹង/សង្គមដែលមានទិសដៅខាងព័ត៌មានគឺជាសង្គមបណ្តាញមួយ។ពិភពលោកទាំងមូលគឺត្រូវបានតភ្ជាប់គ្នាដូចជាបណ្តាញតែមួយ ដែលមានន័យថាភាពទន់ខ្សោយនៅក្នុងផ្នែកមួយនៃបណ្តាញអាចមានផលប៉ះទង្គិចយ៉ាងអាក្រក់លើផ្នែកផ្សេងទៀត។

អ្វីជាសន្តិសុខព័ត៌មាន?

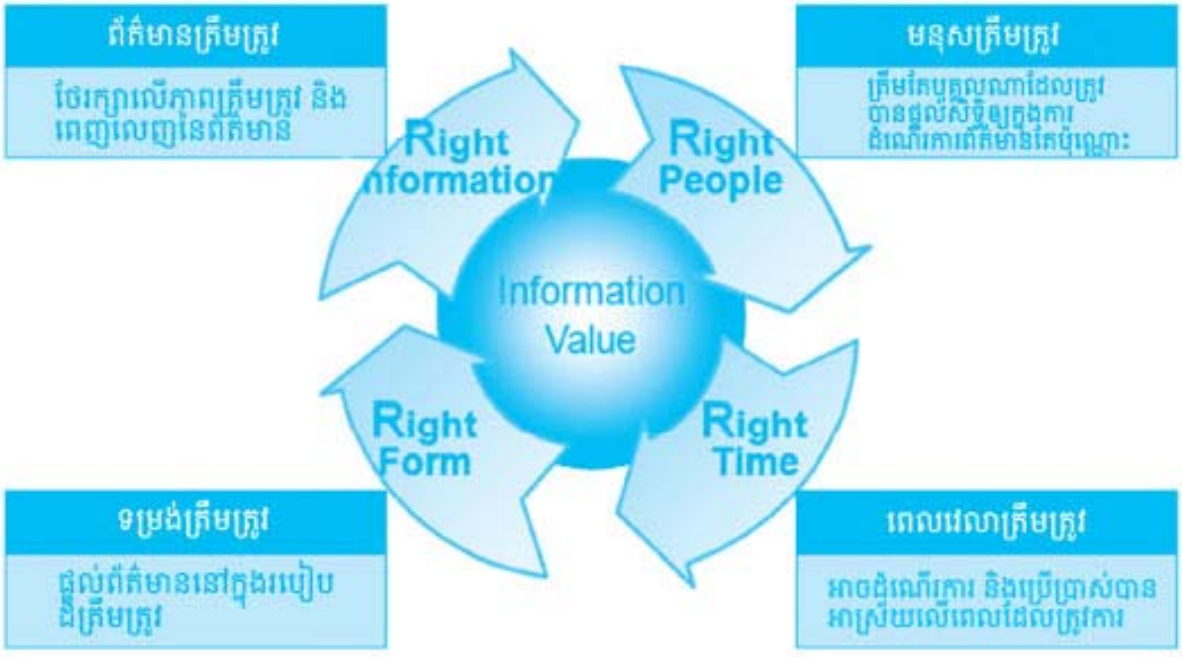
នៅក្នុងការឆ្លើយតបទៅនឹងការទាញយកព័ត៌មានក្នុងលក្ខណៈមិនត្រឹមត្រូវតាមច្បាប់ប្រជាជនកំពុងបង្កើតការខិតខំប្រឹងប្រែងមួយដើម្បីការពារឧក្រិដ្ឋកម្មនានាដែលទាក់ទង និងព័ត៌មានឬធ្វើឲ្យការបំផ្លាញដែលបណ្តាលពីឧក្រិដ្ឋកម្មទាំងនោះឲ្យស្ថិតក្នុងកម្រិតដ៏ទាបមួយ។នេះគឺត្រូវបានហៅថា
“សន្តិសុខព័ត៌មាន”។

ការដាក់ចេញយ៉ាងសាមញ្ញៗនោះ សន្តិសុខព័ត៌បានកំពុងតែរៀបចំតម្លៃសម្រាប់ព័ត៌មាននិងការការពារវា។

៤Rs នៃសន្តិសុខព័ត៌មាន

៤Rs នៃសន្តិសុខព័ត៌មានគឺព័ត៌មានត្រឹមត្រូវ (Right Information) ប្រជាជនត្រឹមត្រូវ (Right People) ពេលវេលាត្រឹមត្រូវ (Right Time) និងទម្រង់ត្រឹមត្រូវ (Right Form) ។ការត្រួតពិនិត្យលើ ៤Rs គឺជាមធ្យោបាយដ៏មានប្រសិទ្ធិភាពបំផុតដើម្បីថែរក្សា និងត្រួតត្រាលើតម្លៃនៃព័ត៌មាន។

រូបទី១. ៤Rs នៃសន្តិសុខព័ត៌មាន



“ព័ត៌មានត្រឹមត្រូវ” សំដៅលើភាពត្រឹមត្រូវ និងភាពពេញលេញនៃព័ត៌មានដែលធានាលើសុច**រិ**តភាពនៃព័ត៌មាន

“មនុស្សត្រឹមត្រូវ” មានន័យថាព័ត៌មានអាចទាញយកបាន ឬដំណើរការបានត្រឹមត្រូវតែបុគ្គលណាដែលត្រូវបានគេផ្តល់សិទ្ធិអនុញ្ញាតឲ្យតែប៉ុណ្ណោះ ជាការធានាលើភាពដែលគួរឲ្យទុកចិត្តបាន

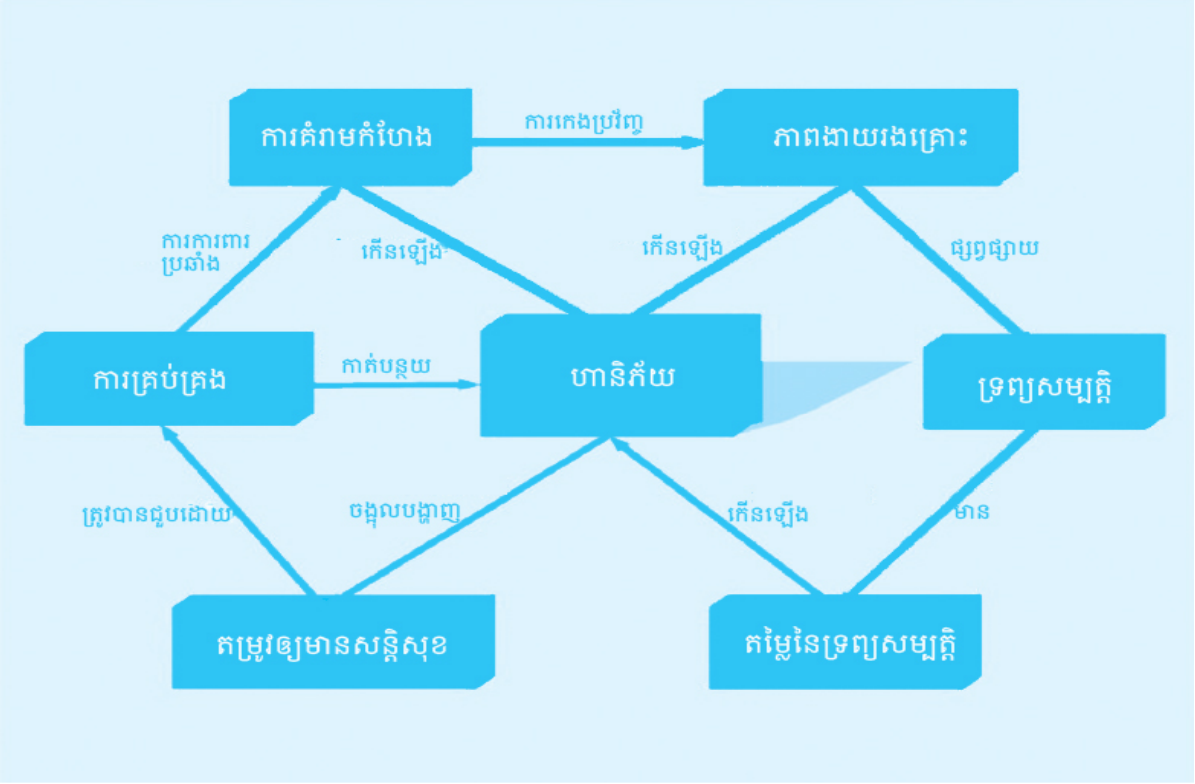
“ពេលវេលាត្រឹមត្រូវ” សំដៅលើភាពដែលអាចដំណើរការបានលើព័ត៌មាន និងភាបដែលអាចប្រើប្រាស់បានអាស្រ័យលើសេចក្តីត្រូវការរបស់អង្គភាពមួយដែលមានសិទ្ធិក្នុងការប្រើប្រាស់វា។ នេះគឺជាការធានាភាពដែលអាចប្រព្រឹត្តទៅបាន។

“ទម្រង់ត្រឹមត្រូវ” សំដៅលើការផ្តល់ឲ្យនៅព័ត៌មានក្នុងរបៀបដ៏ត្រឹមត្រូវមួយ។

ដើម្បីការពារសន្តិសុខព័ត៌មាន ៨Rs ត្រូវ**បាន**ប្រើប្រាស់ជារឿយៗ។ នេះមានន័យថាភាពគួរឲ្យទុកចិត្ត សុចរិតនិងភាពដែលអាចរកបានគួរត្រូវបានសង្កេតមើលនៅពេលដែលកំពុងប្រើប្រាស់ព័ត៌មាន។

សន្តិសុខព័ត៌មានក៏ស្មើផងដែរឲ្យយល់ច្បាស់ពីតម្លៃទ្រព្យសម្បត្តិជាព័ត៌មានទាំងនេះ។ ក៏ដូចទៅនឹងការងាយរងគ្រោះ និងការជាប់ទាក់ទងនូវការគំរាមកំហែងនានាលើព័ត៌មានទាំងនោះ។ នេះគឺគេស្គាល់ថាជាការគ្រប់គ្រងលើហានិភ័យ។ រូបទី២បង្ហាញពីភាពជាប់ទាក់ទងគ្នារវាងទ្រព្យសម្បត្តិជាព័ត៌មាន និងហានិភ័យ។

រូបទី២. ភាពជាប់ទាក់ទងគ្នារវាងហានិភ័យ និងទ្រព្យសម្បត្តិជាព័ត៌មាន



ហានិភ័យគឺត្រូវបានកំណត់ដោយតម្លៃនៃទ្រព្យសម្បត្តិ ការគំរាមគំហែង និងភាពងាយរងគ្រោះថ្នាក់នានា។ រូបមន្តគឺដូចខាងក្រោម៖

ហានិភ័យ = $\int$(តម្លៃទ្រព្យសម្បត្តិ ការគំរាងកំហែង ភាពដែលងាយរងគ្រោះ)

ហានិភ័យគឺជាសមាមាត្រ**ដោយត្រង់**ទៅរកតម្លៃទ្រព្យសម្បត្តិ ការគំរាមកំហែងនិងភាពងាយរងគ្រោះនានា។ដូច្នេះហានិភ័យកើនឡើង ឬធ្លាក់ចុះដោយការរៀបចំលើទំហំនៃតម្លៃទ្រព្យសម្បត្តិ ការគំរាមកំហែងនិងភាពងាយរងគ្រោះនានា នេះគឺត្រូវបានធ្វើតាមរយៈការគ្រប់គ្រងលើហានិភ័យ។

យុទ្ធវិធីនៃការគ្រប់គ្រងលើហានិភ័យមានដូចខាងក្រោម៖

កាត់បន្ថយហានិភ័យ (ការសម្រាលនូវហានិភ័យ) - នេះគឺត្រូវបានធ្វើនៅពេលដែលតវ៉ានីយភាពនៃការគំរាមកំហែង ភាពងាយរងគ្រោះនានាគឺខ្ពស់ ប៉ុន្តែផលប៉ះពាល់ពួកគេគឺទាប។ វាជាប់ពាក់ព័ន្ធនៅលើការយល់ដឹងអ្វីគឺជាការគំរាមកំហែង និងភាពងាយមានគ្រោះថ្នាក់ទាំងនោះធ្វើការកែប្រែ ឬកាត់បន្ថយពួកគេនិងចាត់ការឲ្យបានមុន។ ទោះបីជាយ៉ាងណាក៏ដោយការកាត់បន្ថយហានិភ័យគឺមិនមែនកាត់បន្ថយនៅតម្លៃហានិភ័យឲ្យស្មើ '0' តែម្តង**នោះ**ទេ។

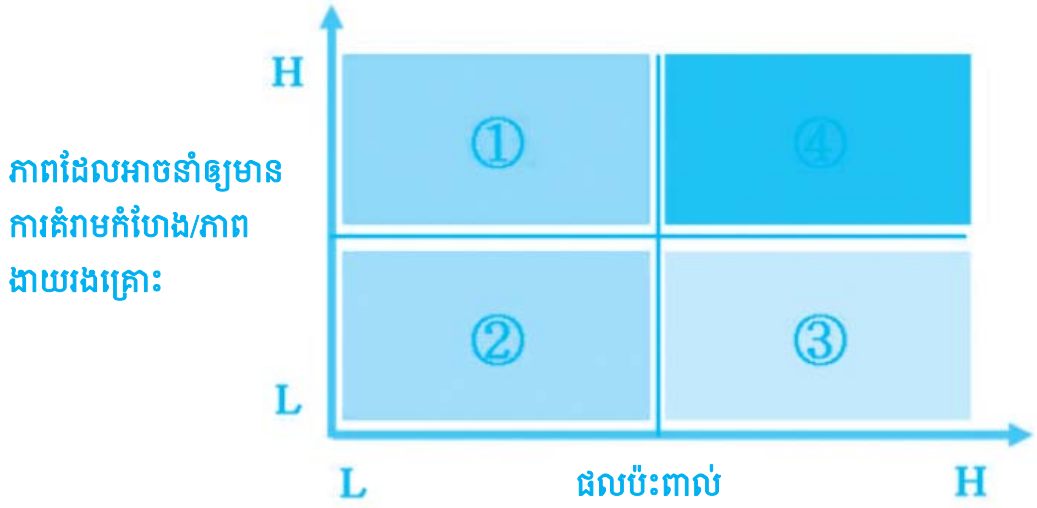
ការទទួលយកហានិភ័យនេះគឺ - ត្រូវបានធ្វើនៅពេលដែលតវ៉ានីយភាពនៃការគំរាមកំហែង ភាពងាយរងគ្រោះនានាគឺទាប និងផលប៉ះពាល់របស់ពួកគេទំនងជាតិចតួច ឬអាចទទួលយកបាន។

ការបញ្ចូលហានិភ័យ - ប្រសិនបើហានិភ័យគឺខ្ពស់ហួសប្រមាណ ឬក៏ស្ថាប័នមិនអាចរៀបចំលើការប្រកួតពិនិត្យយ៉ាងសំខាន់នាមួយបាន ហានិភ័យអាត្រូវបានបញ្ជូនចេញក្រៅនៃអង្គភាព។ ឧទាហរណ៍គឺយកចេញទៅឲ្យច្បាប់ធានារ៉ាប់រង។

ការគេចចេញពីហានិភ័យ - ជាឧទាហរណ៍ប្រសិនបើការគំរាមកំហែង និងភាពងាយរងគ្រោះគឺខ្ពស់នោះការកើតឡើង និងផលប៉ះពាល់របស់វាគឺពិតជាធំធេងផងដែរ ដូច្នេះអ្វីដែលល្អបំផុតដើម្បីគេចចេញពីហានិភ័យដោយជួលបុគ្គលិក និងគ្រឿងផ្គត់ផ្គង់លើការដំណើរការយកទិន្នន័យដោយក្រុមហ៊ុនផ្សេង។

រូបរាងទី៣៖គឺជាក្រាហ្វិកតំណាងឲ្យយុទ្ធវិធីទាំង៤នៃការគ្រប់គ្រងហានិភ័យ។ នៅក្នុងរូបរាងនេះត្រូវបានចែកចេញជាបួនផ្នែក ៖ផ្នែកទី ‘១’ គឺការកាត់បន្ថយហានិភ័យ ផ្នែកទី ‘២’ គឺការទទួលយកហានិភ័យ ផ្នែកទី ‘៣’ គឺការបញ្ជូលហានិភ័យ និងទី ‘៤’ គឺការគេចចេញពីហានិភ័យ។

រូបទី៣. យុទ្ធសាស្ត្រនៃការគ្រប់គ្រងលើហានិភ័យ



ការគិតដ៏សំខាន់នៅក្នុងការជ្រើសរើសយុទ្ធសាស្ត្រគ្រប់គ្រងលើហានិភ័យគឺត្រូវមានតម្លៃសមរម្យ។ការគិតគូរពីតម្លៃដ៏សមរម្យគួរត្រូវបានធ្វើឡើងមុនគម្រោងសម្រាប់ការកាត់បន្ថយហានិភ័យ ការទទួលយកហានិភ័យ ការបញ្ជូនហានិភ័យ ឬការគេចចេញពីហានិភ័យគឺត្រូវបានបង្កើតឡើង។

១.២ គំរូនានាសម្រាប់សកម្មភាពផ្សេងៗរបស់សន្តិសុខព័ត៌មាន

សកម្មភាពផ្សេងៗរបស់សន្តិសុខព័ត៌មានមិនអាចបង្កើតឡើងប្រកបដោយមានប្រសិទ្ធិភាពបើគ្មានការបូបនីយកម្មនៃការកែប្រែលើការបង្រួបបង្រួមគ្នានៅលើគម្រោងបច្ចេកទេស គម្រោងរូបរាងជាក់ស្តែង និងគម្រោងផ្នែករដ្ឋបាលទេនោះ។

អង្គការជាច្រើនបានផ្តល់អនុសាសន៍សម្រាប់គំរូផ្សេងៗសម្រាប់សកម្មភាពនានារបស់សន្តិសុខព័ត៌មាន។ ឧទាហរណ៍តំណាងឲ្យគឺអង្គការអន្តរជាតិសម្រាប់គំរូការរួបនីយកម្ម និងគណៈកម្មាធិការនៃអេឡិចត្រូនិចអន្តរជាតិ (ISO/IEC) ស្នើសុំនានាសម្រាប់សន្តិសុខព័ត៌មាន និងការវាយតម្លៃផ្នែកផ្សេងៗនៃសារនកម្មប្រព័ន្ធព័ត៌មានដែលមានការធានារ៉ាប់រង (CISA) និងជំនាញការខាងសន្តិសុខប្រព័ន្ធព័ត៌មានដែលមានការធានារ៉ាប់រង (CISSP) នៃសមាគមន៍ត្រួតពិនិត្យ និងសារនកម្មប្រព័ន្ធព័ត៌មាន (ISACA) គំរូទាំងឡាយនេះឲ្យអនុសាសន៍ទៅលើសកម្មភាពនានារបស់សន្តិសុខព័ត៌មានដែលមានការធានារ៉ាប់រង ដូចជាការបង្កើតនូវរូបមន្តនៃច្បាប់សន្តិសុខព័ត៌មាន ការកសាង និងប្រតិបត្តិការនៃអង្គការសន្តិសុខព័ត៌មាន ការគ្រប់គ្រងលើធនធានមនុស្ស ការគ្រប់គ្រងលើសន្តិសុខពិតៗ ការគ្រប់គ្រងលើសន្តិសុខបច្ចេកទេស និងការគ្រប់គ្រងលើនិរន្តន៍ភាពនៃជំនួញ និងសារនកម្មសន្តិសុខ។

តារាងលេខ២.បញ្ជីគំរូនានាដែលជាប់ពាក់ព័ន្ធទៅនឹងកម្មសិទ្ធិផ្សេងៗរបស់សន្តិសុខព័ត៌មាន។

តារាងលេខ២. កម្មសិទ្ធផ្សេងៗរបស់សន្តិសុខព័ត៌មាន និងគំរូនានាដែលជាប់ពាក់ព័ន្ធ

កម្មសិទ្ធិផ្សេងៗនៃសន្តិសុខ	ISO/IEC 27001	CISA	CISSP
រដ្ឋបាល	• ច្បាប់សន្តិសុខ	• ការគ្រប់គ្រងលើ IT	• អនុវត្តនានាលើការគ្រប់គ្រងផ្នែកសន្តិសុខ • គំរូនានានិងស្តាបត្យកម្មរបស់សន្តិសុខ
	• អង្គការនៃសន្តិសុខព័ត៌មាន	• ការគ្រប់គ្រងលើ IT	
	• ការគ្រប់គ្រងលើទ្រព្យសម្បត្តិ	• ការការពារនៃទ្រព្យសម្បត្តិដែលជាព័ត៌មាន	• អនុវត្តនានាលើការគ្រប់គ្រងផ្នែកសន្តិសុខ
	• ធនធានមនុស្សសម្រាប់		
	• ការគ្រប់គ្រងលើឧបទ្ទវហេតុនៃសន្តិសុខព័ត៌មាន	• ការស្តារឡើងវិញនៅគ្រោះមន្តរាយនិងនិរន្តភាពខាងជំនួញ	• គម្រោងការលើនិរន្តន៍ភាពខាងជំនួញនិងគម្រោងការលើកាស្តារឡើងវិញនៅគ្រោះមហន្តរាយ

	• ការគ្រប់គ្រងនិរន្តន៍ភាពនៃជំនួញ	• ការស្តារឡើងវិញនៅគ្រោះមន្តរាយ និងនិរន្តភាពខាងជំនួញ	• គម្រោងការលើនិរន្តន៍ភាពខាងជំនួញនិងគម្រោងការលើកាស្តារឡើងវិញនៅគ្រោះមហន្តរាយ
	• ការប្តេជ្ញា	• ដំណើរការប្រតិត្តិនៃសវនកម្មរបស់ IS	• ច្បាប់ ស៊ើបអង្កេត និងគោរពទៅតាមជាតិពន្ធ
លក្ខណៈសណ្ឋាន	• សន្តិសុខនៃបរិស្ថាន និងប្រាកដប្រជា		• សន្តិសុខនៃភាពប្រាដក ប្រជា
បច្ចេកវិទ្យា	• ការគ្រប់គ្រងលើប្រតិបត្តិការនិងទំនាក់ទំនងនានា	• ការគ្រប់គ្រងលើអាយុវឌ្ឍនកាលនៃហេដ្ឋារចនាសម្ព័ន្ធនិងប្រព័ន្ធផ្សេងៗដ៏ទៃទៀត	• រហស្សលិខសាស្ត្រ • សន្តិសុខបណ្តាញ និងទូរគមនាគមន៍ • សន្តិសុខលើដំណើរការប្រតិបត្តិផ្សេងៗ
	• ដំណើរការលើការ		
	• ត្រួតពិនិត្យ**និង** ការថែរក្សា អភិវឌ្ឍន៍ និង ការទទួលយកនៅប្រព័ន្ធព័ត៌មាន	• ការគាំទ្រនិងចែកចាយនៅសេវាកម្ម IT	

ISO/IEC 27001[1] ផ្តោតទៅលើសន្តិសុខនៃរដ្ឋបាល ជាពិសេសវាសង្កត់ធ្ងន់ទៅលើការប្រមូលនូវឯកសារ និងការប្រតិបត្តលើសវនកម្មដូចជាក្នុងលក្ខណៈរដ្ឋបាល និងអនុវត្តតទៅតាមការបញ្ជាត្តិនៃច្បាប់ គោលការណ៍ ការណែនាំរួមទាំងច្បាប់។ បន្តនៅការបញ្ជាក់អះអាងបន្ថែម និងការប៉ាន់ស្មាននានាដែលតម្រូវឲ្យធ្វើឡើងដោយរដ្ឋបាល។ ដូច្នេះ ISO/IEC 27001 ព្យាយាមកំនត់នៅចំនុចខ្សោយនានានៃប្រព័ន្ធសន្តិសុខ

1 ISO, "ISO/IEC27001:2005," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ឧបករណ៍ដែលត្រូវបានប្រើប្រាស់នៅក្នុងកុច្ចការសន្តិសុខ និងក៏ដូចជាបច្ឆោបាយដែលទាក់ទង និងផ្នែករដ្ឋបាលផងដែរ។

ផ្ទុយទៅវិញមិនមានការផ្តោតទៅលើធនធានមនុស្ស ឬសន្តិសុខរបស់សណ្ឋានលក្ខណៈនោះទេនៅក្នុង CISA[2] ដែលផ្តោតលើតែសកម្មភាពសារពកម្មនានាព្រមទាំងការត្រួតពិនិត្យទៅលើប្រព័ន្ធព័ត៌មាន។ ព្រោះហេតុនោះតួនាទីរបស់អ្នកសារពកម្មនានា និងដំណើរការបង្កើតនៃសារពកម្មគឺត្រូវបានគេគិតថាមានភាពសំខាន់។

CISSP[3] ផ្តោតយ៉ាងសំខាន់ទៅលើសន្តិសុខបច្ចេកវិទ្យា។វាសង្កត់ធ្ងន់ទៅលើការរៀបចំ និងត្រួតពិនិត្យលើឧបករណ៍ដែលប្រើប្រាស់ដូចជា Server និងកុំព្យូទ័រ។

អ្វីដែលត្រូវអនុវត្ត

១. ប៉ាន់ប្រមាណនៅកម្រិតនៃសន្តិសុខព័ត៌មានដែលគិតថាសមរម្យទៅនឹងចំនួនសមាជិករបស់អង្គការអ្នក។

២. តើអ្វីជាការស្វង់មើលលើសន្តិសុខព័ត៌មានដែលអង្គការរបស់អ្នកបានធ្វើ? ចូរដាក់ចំនុចនៃការស្វង់មើលទាំងនោះទៅតាមផ្នែកយុទ្ធសាស្ត្រទាំងបួននៃសន្តិសុខព័ត៌មាន?

៣. ឲ្យឧទាហរណ៍អំពីការវាស់ស្វង់ផ្នែកសន្តិសុខព័ត៌មាននោះនៅក្នុងទម្រង់ជារដ្ឋបាល ជាលក្ខណៈពិតៗរបស់វា និងជាលក្ខណៈបច្ចេកទេសដេលមាននៅក្នុងអង្គការរបស់អ្នក ឬអង្គការផ្សេងៗទៀតដេលនៅក្នុងប្រទេសរបស់អ្នក ឬសាលាក្តី។

សាកល្បងខ្លួនអ្នក

១. តើព័ត៌មានខុសពីទ្រព្យសម្បត្តិផ្សេងទៀតយ៉ាងដូចម្តេច?

២. ហេតុអ្វីបានជាច្បាប់របស់សន្តិសុខព័ត៌មានត្រូវបានគេយកចិត្តទុកដាក់?

៣. តើអ្វីជាមធ្យោបាយនៃការធានាលើសន្តិសុខព័ត៌មាន? បង្ហាញពីភាពខុសគ្នានៃយុទ្ធសាស្ត្រទាំងបួននោះដែលបានលើកឡើងចំពោះសន្តិសុខព័ត៌មាន។

៤. បង្ហាញពីភាពខុសគ្នានៃកម្មសិទ្ធិនានារបស់សន្តិសុខព័ត៌មាន (ដូចជាផ្នែករដ្ឋបាល រូបរាង និងបច្ចេកវិទ្យា។

2 See ISACA, "Standards for Information Systems Auditing," http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=19566.

3 See (ISC)², "CISSP® - Certified Information Systems Security Professional," http://www.isc2.org/cissp.

២. និន្នាការ និងទិសដៅនានារបស់សន្តិសុខព័ត៌មាន

ចំនុចនេះមានគោលដៅទៅលើ៖

- ផ្តល់នៅទស្សនៈមួយចំនួននៃភាពគំរាមកំហែងចំពោះប្រព័ន្ធព័ត៌មាន និង
- ពិពណ៌នាពីវិធានការបតទៅនឹងការគំរាមកំហែងទាំងនោះ

២.១ ប្រភេទនៃការលុកលុយនានាលើសន្តិសុខព័ត៌មាន

ការលួចចូលដោយគ្មានការអនុញ្ញាត (Hacking)

(Hacking) គឺជាសកម្មភាពចូលទៅដំណើរការលើកុំព្យូទ័រ ឬបណ្តាញកុំព្យូទ័រដើម្បីទាញយក ឬធ្វើការកែប្រែព័ត៌មានដោយគ្មានការអនុញ្ញាត។

(Hacking) អាចត្រូវបានគេបែងចែកចេញជាផ្នែកៗដូចជា ការលួចបែបលក្ខណៈនយោបាយ ឧក្រិដ្ឋកម្ម ឬក៏លក្ខណៈកំសាន្តវាអាស្រ័យទៅលើគោលបំណងនៃអ្នកធ្វើនោះ។ ការលួចបែបកំសាន្តគឺត្រូវបានធ្វើឡើងដោយការកែប្រែកម្មវិធី និងទិន្នន័យក្នុងលក្ខណៈសាមញ្ញៗមួយចំនួនទៅតាមសេចក្តីត្រូវការរបស់អ្នកធ្វើនោះ។ការលួចបែបឧក្រិដ្ឋកម្មគឺត្រូវបានប្រើប្រាស់នៅក្នុងការក្លែងបន្លំ ឬការធ្វើចារកិច្ច។ការលួចបែបនយោបាយគឺជាការអុកឡុកតាមរយៈគេហទំព័រដើម្បីផ្សព្វផ្សាយនៅ ឯកសារនយោបាយខុសច្បាប់ណាមួយ។[4]

ថ្មីៗនេះ Hacking បានក្លាយជាការជាប់ពាក់ព័ន្ធកាន់តែច្រើនឡើងនៅក្នុងរលកសញ្ញាភេរវកម្ម និងរលកសញ្ញានៃការធ្វើសម្បាំងដែលកំពុងចោទជាការគំរាមកំហែងធំៗចំពោះសន្តិសុខជាតិ។

4 Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell, "Governing Internet Use: Spam, Cybercrime and e-Commerce," in Danny Butt (ed.), *Internet Governance: Asia-Pacific Perspectives* (Bangkok: UNDP-APDIP, 2005), 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.

សង្គ្រាមបណ្តាញ ចិន និង អាមេរិក

ក្រុម Hacker ដែលមានឈ្មោះថា PoizonBox ដែលមានទីតាំងនៅក្នុងសហរដ្ឋអាមេរិកគឺ ត្រូវបានចោទប្រកាន់ថាបានធ្វើឲ្យខូចខាតនៅគេហទំព័រចិនច្រើនជាង៣៥០ នៅក្នុងរយៈពេលមួយខែៗក្រុមនេះផងដែរត្រូវបានគេចោទប្រកាន់លើការលុកលុយចំពោះគេហទំព័ររបស់ចិនចំនួន២៤ផ្សេងទៀត ដែលក្នុងនោះរួមមានអង្គការរដ្ឋាភិបាលចចិនចំនួនប្រាំបីផងដែរ កាលពីថ្ងៃតី ៣០ ខែមេសា ឆ្នាំ២០០១។បន្ទាប់មកក្រុម Hacker របស់ប្រទេសចិនបានប្រកាសធ្វើសង្គ្រាមបណ្តាញលើកទី៦នៃការការពារជាតិហើយបានវាយលុកទៅលើគេហទំព័រនានារបស់សហរដ្ឋអាមេរិក ដែលរួមទាំងគេហទំព័ររបស់ស្ថាប័នរដ្ឋាភិបាលអាមេរិកពីថ្ងៃទី ៣០ ខែមេសា ទៅថ្ងៃទី ១ ខែឧសភា ឆ្នាំ២០០១។ការលុកលុយគែដូចអ្វីដែល Pentagon បានធ្វើការប៉ាន់តម្លៃថាប្រព័ន្ធសន្តិសុខដ៏សំខាន់របស់វាត្រូវបានប្តូរពី INFO-CON NORMAL ALPHA។ នៅថ្ងៃទី ១ ខែឧសភា ឆ្នាំ២០០១ មជ្ឈមណ្ឌលការពារហេដ្ឋារចនាសម្ព័ន្ធជាតិរបស់ការិយាល័យ ស៊ើបអង្កេតរបស់សហព័ន្ធ បានធ្វើការព្រមានពីការលុកលុយរបស់ Hacker ចិនលើគេហទំព័រនានារបស់ក្រុមហ៊ុន និងរដ្ឋាភិបាលសហរដ្ឋអាមេរិក។

តាមរយៈសង្គ្រាមបណ្តាញនេះ សហរដ្ឋអាមេរិកបានទទួលស្គាល់ថាការគំរាមកំហែងតាមប្រព័ន្ធអេឡិចត្រូនិច (ដូចជាការលុកលុយ (Hacker)) អាចបណ្តាលឲ្យមានការបំផ្លិចបំផ្លាញច្រើនចំពោះស្ថាប័នរដ្ឋាភិបាលសហរដ្ឋនានា ហើយបន្ទាប់មកខាងក្រោយបានបង្កើនសាច់ដុំយ៉ាងមាំលើការការពារប្រឆាំង និងរលកសញ្ញាគំរាមកំហែងដោយការបង្កើនគម្រោងថវិកាលើផ្នែកសន្តិសុខព័ត៌មានឲ្យប្រសើរឡើងនៅគោលការណ៍ច្បាប់ព័ត៌មាននៅក្នុងស្ថាប័នរដ្ឋាភិបាលនានា។

Source:Attrition.org, “Cyberwar with China: Self-fulfilling Prophecy” (2001), http://attrition.org/security/commentary/cn-us-war.html.

សេវាកម្មក្លែងក្លាយ (Denial-of-Service)

សេវាកម្មក្លែងក្លាយវាយប្រហារដោយការរារាំងអ្នកប្រើប្រាស់ស្របច្បាប់នានា ពីការប្រើនៅសេវាកម្មណាមួយខណៈពេលដែលអ្នកប្រព្រឹត្តបទឧក្រិដ្ឋនោះទទួលបានការប្រើប្រាស់យ៉ាងខុសច្បាប់ទៅលើម៉ាស៊ីនឬទិន្នន័យណាមួយ។បញ្ហានេះកើតឡើងខណៈដែលអ្នកលុកលុយមានចំនួនយ៉ាងច្រើនដែលធ្វើឲ្យបណ្តាញមានចំនុះទិន្នន័យដ៏ច្រើន ឬក៏ការទាញយកការប្រើប្រាស់ឲ្យបានមុនចំពោះធនធានណាដែលមិនសូវសំបូរឬក៏មានដែនកំនត់សម្រាប់ការប្រើប្រាស់ដូចជាការរាំងខ្ទប់នៅដំណើរការត្រួតពិនិត្យ ឬដាក់ការតភ្ជាប់លើបណ្តាញឲ្យនៅរង់ចាំ។ ឬពួកគេអាចរំខានដល់ដំណើរការឧបករណ៍នៃប្រព័ន្ធបណ្តាញ ឬក៏បញ្ឆោតទិន្នន័យនៅក្នុងពេលឆ្លងកាត់រួមមានទាំងការបំលែងនៅនូវទិន្នន័យនោះផងដែរ។[5]

រលកសញ្ញាភេរវកម្មប្រឆាំងនឹងសាធារណរដ្ឋអេស្តូនី

នៅថ្ងៃទី ៨ ខែមិថុនា ឆ្នាំ២០០៧ នៅក្នុងទីក្រុងនៃប្រទេសអេស្តូនីធ្វើការផ្លាស់ប្តូរនៅបូជនីយដ្ឋានជ័យជំនះរបស់ USSR ពីកណ្តាលទីក្រុងទៅកាន់កន្លែងបញ្ចុះសព្វនាយទាហានបានបង្កឲ្យមានរលកសញ្ញាភេរវកម្មមួយប្រឆាំងនឹងអេស្តូនី និងរួមមានទាំងការលុកលុយរបស់សេវាកម្មក្លែងក្លាយ (DoS) ទៅលើកុំព្យូទ័រមួយលានគ្រឿង។ ប្រព័ន្ធបណ្តាញកុំព្យូទ័រ និងគេហទំព័រនៃវិមានប្រធានាធិបតី សភាអេស្តូនី ស្ថាប័នផ្សេងៗរបស់រដ្ឋាភិបាល ទីស្នាក់ការគណបក្សកន្លែងសារព័ត៌មាន និងធនាគារគឺត្រូវបានវាយប្រហារដោយរលកសញ្ញានោះ។សូម្បីតែបណ្តាញ Wireless ក៏ស្ថិតក្រោមការវាយលុកនោះដែរ។

អេស្តូនីក្រោយមកបានរកឃើញតំបន់របស់ពួកវាយប្រហារគឺចេញមកពីស្ថាប័នរដ្ឋាភិបាលរុស្សី។ប៉ុន្តែរដ្ឋាភិបាលប្រទេសរុស្សីបានបដិសេធការចោទប្រកាន់នេះ។

នៅពេលដែលការលុកលុយនៃរលកភេរវកម្មនោះត្រូវបានបំបែក អេស្តូនីគឺមិនអាចឆ្លើយតបភ្លាមៗសម្រាប់ការខ្វះខាតក្រុមទទួលខុសត្រូវលើឧបទ្ទវហេតុ និងគោលការណ៍ច្បាប់សន្តិសុខប័ត៌មាន។

Source: Beatrix Toth, “Estonia under cyber attack” (Hun-CERT, 2007), http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

5 ESCAP, “Module 3: Cyber Crime and Security,” http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

អក្សរសម្ងាត់ប្រកបដោយគ្រោះថ្នាក់ (Malicious Code)

Malicious Code សំដៅទៅលើកម្មវិធីទាំងឡាយណាដែលបណ្តាលឲ្យមានការបំផ្លិចបំផ្លាញចំពោះប្រព័ន្ធ នៅពេលដែលកម្មវិធីនោះដំណើរការ។ មេរោគនានា worms and Trojain horses គឺជាប្រភេទនៃ Malicious Code។

មេរោគកុំព្យូទ័រគឺជាកម្មវិធីកុំព្យូទ័រ ឬក៏ជាកូដកម្មវិធីដែលបំផ្លាញប្រព័ន្ធនានារបស់កុំព្យូទ័រ និងទិន្នន័យ ដោយការចម្លងនូវខ្លួនវាទៅកាន់កម្មវិធីដទៃទៀត ទៅកាន់ផ្នែកដែលកុំព្យូទ័រចាប់ផ្តើមដំណើរការ ឬទៅកាន់ឯកសារផ្សេងៗ។

Worm គឺជាមេរោគដែលធ្វើការចម្លងខ្លួនវាដែលមិនធ្វើឲ្យមានការខូចខាតលើឯកសារ ប៉ុន្តែវាទៅលាក់ខ្លួន នៅក្នុងអង្គចងចាំសកម្ម (Active Memory) និងធ្វើការលើផ្នែកណាមួយនៃប្រព័ន្ធប្រតិបត្តិការដោយស្វ័យ ប្រវត្តិ និងជាញឹកញាប់មិនឲ្យមើលឃើញដោយអ្នកប្រើប្រាស់។ ការចម្លងខ្លួនដោយមិនអាចគ្រប់គ្រងបាន របស់ពួកមេរោគទាំងនេះបំផ្លាញប្រភពនានានៃប្រព័ន្ធដំណើរការ ការធ្វើឲ្យយឺត ឬក៏បញ្ឈប់នៅដំណើរការ លើកិច្ចការណាមួយ។វាជារឿយកើតឡើងត្រឹមតែពេលវត្តមានរបស់ណា Worm ត្រូវបានរកឃើញ។

Trojan Horse គឺជាកម្មវិធីដែលបង្ហាញថាមានការប្រើប្រាស់និង ឬក៏មិនសូវបង្កឲ្យមានឥភាពគ្រោះថ្នាក់ ប៉ុន្តែពិតជាមានមុខងារប្រកបដោយគ្រោះថ្នាក់ដូចជាមិនអាចបង្ហាញចេញនៅកម្មវិធីដែលត្រូវបានលាក់ឲ្យ ឃើញឡើងវិញឬក៏ពាក្យបញ្ជាពិសេសៗដែលធ្វើឲ្យប្រព័ន្ធមួយដែលងាយរងគ្រោះទទួលការរុករានពីវា។

ទិបត្តិប្រព័ន្ធអ៊ីនធើរណិត ១.២៥ របស់សាធារណរដ្ឋកូរ៉េ

នៅថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០០៣ មេរោគកុំព្យូទ័រដែលមានឈ្មោះថា “Slamer Worm” បានបណ្តាលឲ្យបិទនៅការភ្ជាប់ប្រព័ន្ធអ៊ីនធើរណិតនៅទូទាំងប្រទេសកូរ៉េ។ការបិទនោះដែលមានរយៈពេលច្រើនជាងប្រាំបួនម៉ោងគឺបណ្តាលមកដោយសេវាកម្មរបស់ប្រធានមេនៃកុំព្យូទ័រ (DNS) កំពុងត្រូវបានឆាឆៅដោយ Worm។

លទ្ធផលទៅលើការបិទនោះ ទីផ្សារនៃប្រព័ន្ធ Online បានខាតបង់ដែលមានតម្លៃប្រមាណ ២០០,០០០ ទៅ ៥០០,០០០ ដុល្លា និងខាតបង់នៅក្នុងការធ្វើជំនួញតាមប្រព័ន្ធ Online នៅចំនួនប្រមាញ ២២.៥ កោដិដុល្លា។ វាត្រូវបានរាយការណ៍ថាការបំផ្លាញដែលបណ្តាលមកពី Slammer Worm គឺមានភាពធំធេងជាងការបំផ្លាញដោយ Worm ដែលមានឈ្មោះថា Code Red និង Nimela ពីព្រោះការលុកលុយរបស់ Worm ទាំងពីរនេះគឺត្រឹមតែរុករានលើអ្នកប្រើប្រាស់ធម្មតាតែប៉ុណ្ណោះ។

វិបត្តិប្រព័ន្ធអ៊ីនធើរណិតបានធ្វើឲ្យរដ្ឋាភិបាលកូរ៉េទទួលយកការធ្វើនៅការគ្រប់គ្រងដែលមានលក្ខណៈទូលំទូលាយនៃសេវាកម្មផ្តល់នៅសេវាផ្នែកអ៊ីនធើរណិត និងក្រុមហ៊ុនសន្តិសុខព័ត៌មាន។ប្រព័ន្ធនានាសម្រាប់ការការពារហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មាននិងការប៉ាន់មើលសន្តិសុខព័ត៌មានគឺត្រូវបានបង្កើតឡើង។ ហើយស្ថាប័នសន្តិសុខព័ត៌មាន ឬគណកម្មធិការសន្តិសុខព័ត៌មានគឺត្រូវបានបង្កើតឡើងនៅក្នុងស្ថាប័ននីមួយៗ។

សង្គមវិស្វកម្ម

ក្រុម “វិស្វកម្មរបស់សង្គម” សំដៅយកការបង្កើតបច្ចេកទេសដែលត្រូវបានឧេប្រើដើម្បីបញ្ឆោតមនុស្សគ្រប់រូបឲ្យបើកបង្ហាញនូវព័ត៌មានផ្ទាល់ខ្លួន។ ទោះបីវាស្រដៀងគ្នាទៅនឹងល្បិចដែលគួរឲ្យយើងជឿជាក់បានឬការបោកបញ្ឆោតសាមញ្ញក៏ដោយ ប៉ុន្តែក្រុមនេះបានធ្វើជាលក្ខណៈធម្មតានេះដើម្បីបោកយក

នូវព័ត៌មានឬការមានសិទ្ធិអាចដំណើរការលើប្រព័ន្ធកុំព្យូទ័របាន។ នៅក្នុងករណីជាច្រើនអ្នកលុកលុយមិនដែលបង្ហាញខ្លួនពួកគេប្រឈមមុខជាមួយនឹងជនរងគ្រោះទេ។

Phissing គឺជាឧបករណ៍មួយនៃសង្គមវិស្វកម្ម វាគឺជាសកម្មភាពនៃការលួចយកព័ត៌មានផ្ទាល់ខ្លួនតាមរយៈប្រព័ន្ធអ៊ីនធើរណិតក្នុងគោលបំណងធ្វើការលួចបន្លំផ្នែកហិរញ្ញវត្ថុ។ Phissing បានក្លាយជាសកម្មភាពឧក្រិដ្ឋដ៏សំខាន់មួយលើប្រព័ន្ធអ៊ីនធើរណិត

ធនាគារស្វីសត្រូវបានខាយប្រហារដោយក្រុមអ្នកលួចយកទឹនន័យឈ្មោះថា "Biggest Ever"

នៅថ្ងៃទី ៩ ខែមករា ឆ្នាំ ២០០៧ ធនាគារស្វីសដែលមានឈ្មោះថា Nordea គឺត្រូវបានវាយប្រហារដោយការលួចបន្លំទិន្នន័យគណនីយធនាគារតាមរយៈប្រព័ន្ធ Online ។ការវាយប្រហារនេះត្រូវបានចាប់ផ្តើមដោយការផ្ញើរនូវព័ត៌មានមួយដែលភ្ជាប់ជាមួយមេរោគ Trojan ទៅកាន់អ្នកប្រើប្រាស់។គណនីយធនាគាររបស់ Nordea ប្រើនូវឈ្មោះរបស់ធនាគារនោះផងដែរ។ អ្នកផ្ញើរបានលើទឹកចិត្តអ្នកប្រើប្រាស់ឲ្យទាញយកកម្មវិធីមួយឈ្មោះថា "Spam Fighting" អ្នកប្រើប្រាស់ណាដែលទាញយកនូវឯកសារដែលភ្ជាប់មកជាមួយកម្មវិធីនោះឈ្មោះថា "Ranking.zip" ឬ "Ranking.exe" គឺត្រូវបានរងការលុកលុយដោយ Torjan ដែលត្រូវបានហៅនៅឈ្មោះមួយផ្សេងទៀតថា "haxdoor.ki" ដោយក្រុមហ៊ុនសន្តិសុខខ្លះ។

"Haxdoor.zip" ដំឡើងយ៉ាងសាមញ្ញនៅ keylogger ដើម្បីចម្លង Keystroke និងលាក់ខ្លួនរបស់វាដោយប្រើនៅ Rootkit ។ការដឹកជញ្ជូននូវឯកសារដែលមានឈ្មោះខាងចុងថា ".ki" ដែលបានបំលែងបីមេរោគដែលមានឈ្មោះថា Trojan គឺនៅពេលដែលវាត្រូវបានគេធ្វើសកម្មភាពទៅលើដោយអតិថិជន ដែលកំពុងប៉ុនប៉ងចូលទៅក្នុងតំបន់របស់ធនាគារតាមរយៈប្រព័ន្ធ Online។ អតិថិជនគឺត្រូវបាននាំទៅកាន់គេហទំព័រផ្សេងដែលមិនមែនរបស់ធនាគារ Nordea និងជាកន្លែងសម្រាប់អតិថិជនបញ្ចូលព័ត៌មានសំខាន់ៗរួមទាំងលេខកូដសម្ងាត់របស់ពួកគេ។បន្ទាប់ពីការបញ្ចូលព័ត៌មានទាំងនោះហើយសារដែលប្រាប់ពីកំហុស

>>

>>

ឆ្គងបានបង្ហាញខ្លួនឡើងកោយបញ្ជាក់ប្រាប់អតិថិជនថាគេហទំព័ររបស់ធនាគារកំពុងជួបការលំបាកខាងបច្ចេកវិទ្យា។បន្ទាប់ពីធ្វើដូច្នោះហើយឧក្រិដ្ឋជនទាំងនោះបានយកព័ត៌មានរបស់អតិថិជនទៅប្រើប្រាស់ដើម្បីទាញយកគណនីយពីគេហទំព័ររបស់ Nordea ពិតប្រាកដ។

អតិថិជនរបស់ធនាគារ Nordea គឺត្រូវបានកំណត់ថាជាទិសដៅដោយការផ្ញើរនូវសារអេឡិចត្រូនិចទៅកាន់ពួកគេដោយភ្ជាប់ជាមួយមេរោគ Trojan អស់រយៈកាលច្រើនជាង១៥ខែ។ អតិថិជន ២៥០នាក់ បាននិយាយថាពួកគេបានទទួលរងនៅផលប៉ះពាល់ពីមេរោគនោះ ជាមួយការបំផ្លាញនៅទឹកប្រាប់សរុបប្រមាណប្រាពីរ ទៅ ប្រាំបីរយលានលុយស្វីស (7,300 – 8,000 ដុល្លា)។ករណីនេះបានបង្ហាញផងដែរថារលកសញ្ញានៃការវាយប្រហារនានាអាចធ្វើឲ្យប៉ះពាល់ដល់ក្រុមហ៊ុនហិរញ្ញវត្ថុដែលមានការការពារសន្តិសុខក្នុងកម្រិតខ្ពស់។

Source: Tom Espiner, "Swedish bank hit by 'biggest ever' online heist," *ZDNet.co.uk* (19 January 2007), http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm

២.២ និន្នាការនានានៅក្នុងការគំរាមកំហែងផ្សេងៗលើសន្តិសុខព័ត៌មាន[6]

សកម្មភាពដសំខាន់នៅក្នុងការការពារសន្តិសុខព័ត៌មានគឺ ការវិភាគលើនិន្នាការគំរាមកំហែងលើផ្នែកសន្តិសុខ។នេះសំដៅយកការស្វែងរកនៅគំរូនៅក្នុងការគំរាមកំហែងនានាលើផ្នែកសន្តិសុខនៅពេលកន្លងមកដើម្បីកំណត់នៅមធ្យោបាយផ្សេងៗដែលគំរូទាំងនោះធ្វើការផ្លាស់ប្តូរ និងអភិវឌ្ឍន៍ខ្លួនវា ងាកអរទៅកាន់ទិសដៅថ្មីៗទៀត គឺផ្លាស់ប្តូរទីកន្លែង។ដំណើរការដដែលគឺត្រូវបានធ្វើដើម្បីប្រមូលព័ត៌មានដែលទាក់ទងនានានៃការគំរាមកំហែងនោះ និងការធ្វើឲ្យប្រសើរឡើងចំពោះឧប្បទ្ទវហេតុលើទិន្នន័យដែលអាចឲ្យប្រមើលមលើជាមុន ឬក៏ការគំរាមកំហែងមួយចំនួនដែលអាចកើតឡើង និងការរៀបចំនៅការឆ្លើយតបយ៉ាងសមរម្យមួយទៅនឹងការគំរាមកំហែងទាំងនោះ។

6 This section is drawn from Tim Shimeall and Phil Williams, *Models of Information Security Trend Analysis* (Pittsburgh: CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

ស្ថាប័នមួយចំនួនដែលបង្កើតណោការវិភាគលើនិន្នាការគំរាមកំហែងចំពោះសន្តិសុខព័ត៌មាន និងបានបែងចែករំលែកនៅរបាយការណ៍ពីនិន្នាការនៃការគំរាមកំហែងនោះរួមមានស្ថាប័ន៖

- CERT (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid:threatreport)
- IBM (http://xforce.iss.net)

និន្នាការនានានៅក្នុងការគំរាមកំហែងផ្សេងៗលើសន្តិសុខព័ត៌មានត្រូវបានគេរាយការណ៍និងពិពណ៌នាដូចខាងក្រោម៖

ភាពស្វ័យប្រវត្តិនៃឧបករណ៍សម្រាប់ការលុកលុយ[7]

អ្នកឈ្លានពានទាំងឡាយឥឡូវប្រើនៅឧបករណ៍ដោយស្វ័យប្រវត្តិនានាដើម្បីប្រមូលយកព័ត៌មានបានរាប់ពាន់ពីអតិថិជនរបស់អ៊ីនធើរណិតយ៉ាងឆាប់រហ័ស និងយ៉ាងងាយស្រួលៗប្រព័ន្ធបណ្តាញនានាអាចត្រូវបានធ្វើការវិភាគពីតំបន់ឆ្ងាយ និងភាពទន់ខ្សោយរបស់អ្នកប្រើប្រាស់ដែលត្រូវបានកំនត់ដោយឧបករណ៍ស្វ័យប្រវត្តិនោះ។ អ្នកឈ្លានពានទាំងនោះបានរាយការណ៍ឈ្មោះព័ត៌មានទាំងនោះសម្រាប់ការប្រើប្រាស់នៅពេលក្រោយ ចែករំលែក ឬបញ្ជូនវាទៅកាន់អ្នកឈ្លានពានដទៃទៀត ឬក៏ធ្វើការវាយប្រហាក្លាមៗ។ ឧបករណ៍ខ្លះ (ដូចជា Cain&able) ធ្វើស្វ័យប្រវត្តិកម្មជាលក្ខណៈស៊េរីនៃការវាយប្រហារក្នុងទ្រង់ទ្រាយតូចៗឆ្ពោះទៅយករាល់ព័ត៌មានដែលត្រូវការ។ ឧទាហរណ៍ អ្នកលុកលុយទាំងនោះអាចប្រើនៅ Pocket Sniffer ដើម្បីទាញយកលេខសម្ងាត់របស់ Router ឬ Firewall ហើយប្រើលេខសម្ងាត់នោះចូលទៅកាន់ Firewall និងបិទនៅមុខងាររបស់ Firewall លើការស្រង់យកព័ត៌មានថាមួយណាត្រូវបានអនុញ្ញាត ឬមិនអនុញ្ញាតចូលកាន់ Server និងបន្ទាប់មកពួកគេប្រើនៅសេវាកម្មលើបណ្តាញដើម្បីអានទិន្នន័យនៅលើ Server ។

7 This section is drawn from CERT, "Security of the Internet," Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html

ឧបករណ៍ខាយប្រហារដែលពិបាកដើម្បីចាប់

ឧបករណ៍វាយប្រហារខ្លះប្រើនៅគំរូលក្ខណៈនៃការវាយប្រហាបែបថ្មីដែលជាការពិបាកក្នុងការចាប់ដោយ ឧបករណ៍សម្រាប់ចាប់សើរីចាស់។ ឧបករណ៍:បច្ចេកវិទ្យាឈ្មោះថា anti-forensic គឺកំពុងត្រូវបានគេប្រើប្រាស់ដើម្បីបិទ ឬក៏លាក់នៅឧបករណ៍នៃការវាយប្រហារទាំងនោះ។ ឧបករណ៍ Polymorphic គឺផ្លាស់ប្តូរ រាល់ពេលដែលពួកគេត្រូវបានប្រើ។ឧបករណ៍ខ្លះក្នុងចំណោមឧបករណ៍ទាំងនេះប្រើនៅពិធីការសាមញ្ញ។ ដូចជាពិធីការបញ្ជូនក្នុងទម្រង់ Hypertext (HTTP) ដែលធ្វើឲ្យពិបាកដើម្បីញែកពួកចេញពីការធ្វើចរាចរ ដែលមានភាពស្របច្បាប់នៅលើបណ្តាញ។[8] មេរោគ Worm គឺមាននៅក្នុងសាររហ័ស (Instant-Message) នៃ MSN Messenger របស់អ្នកប្រើប្រាស់ម្នាក់ដែលផ្ញើរទាក់ទងគ្នាជាមួយអ្នកប្រើប្រាស់ម្នាក់ទៀតដែលអ៊ីមែលរបស់គេផ្ទុកនៅកន្លែងរក្សាអ៊ីមែលនោះ (Address Book) មានការប៉ះពាល់រួចទៅហើយដោយ Worm ហើយបន្ទាប់ពីការកើតឡើងនៅបញ្ហាមួយនេះពួកគេបានទទួលនៅឯកសារមួយរួចទៅហើយសម្រាប់អ្នកលុកលុយ។ រាល់លក្ខណៈនៃអ្នកប្រើប្រាស់ IM ពិតប្រាកដគឺត្រូវបានធ្វើតាមអ្វីដែលកំពុងត្រូវប្រកាសអាសន្នអំពីបញ្ហាទាំងនេះ។[9]

ការរកឃើញយ៉ាងឆាប់រហ័សនៃភាពងាយរងគ្រោះ

ជារៀងរាល់ឆ្នាំភាពងាយរងគ្រោះនានាត្រូវបានរកឃើញថាមានភាពថ្មីៗជាច្រើនទៀតទៅលើផលិតផលកម្មវិធី Software ដែលត្រូវបានរាយការណ៍ទៅឲ្យមជ្ឈមណ្ឌលសហប្រតិបត្តិការនៃក្រុមទទួលខុសត្រូវបន្ទាន់លើផ្នែកកុំព្យូទ័រគឺមានចំនួនច្រើនជាងពីដងនៅក្នុងទិន្នន័យដែលទទួលបានមក និងបានធ្វើឲ្យវាមានភាពលំបាកដល់រដ្ឋបាលនានា ដើម្បីធ្វើឲ្យរបាំងការពារគ្រោះថ្នាក់នោះឲ្យស្ថិតនៅទាន់ពេលវេលាក្នុងការទប់ទល់ (Keep Up to Date) ។ហើយអ្នកលុកលុយបានដឹងអំពីចំនុចទន់ខ្សោយនេះ និងទាញយកប្រយោជន៍ក្នុងកាល:ទេស:នេះ។[10] អ្នកលុកលុយខ្លះបានវាយប្រហារនៅថ្ងៃសូន្យ ឬ ម៉ោងសូន្យ ទៅលើកុំព្យូទ័រពីព្រោះរបាំងការពារការវាយប្រហានោះមិនត្រូវទាន់បានកែប្រែឲ្យទាន់សភាពការណ៍លើការវាយលុកនោះដោយរដ្ឋបាលនានា។[11]

8 Suresh Ramasubrahmanian et al., op. cit., 94.
9 Munir Kotadia, "Email worm graduates to IM," *ZDNet.co.uk* (4 April 2005), http://news.zdnet.co.uk/security/0,1000000189,39193674,00.htm.
10 Suresh Ramasubrahmanian et al., op. cit.
11 Wikipedia, "Zero day attack," Wikimedia Foundation Inc., http://en.wikipedia.org/wiki/Zero_day_attack.

ការកើនឡើងនៅតាមតំរាមកំហែងក្នុងទម្រង់ផ្សេងៗគ្នា និងការបញ្ចូលគ្នានៃយុទ្ធវិធីវាយប្រហារតែមួយ

ភាពគំរាមកំហែងក្នុងទម្រង់ផ្សេងៗ គឺជាលក្ខខណ្ឌមួយដែលអ្នកលុកលុយមានប្រៀបលើជនរងគ្រោះ។ ចំនួននៃការកំរាមកំហែងផ្សេងៗទាំងនោះបង្កើននូវការពង្រាយនៅការវាយប្រហារជាលក្ខណៈស្វ័យប្រវត្តិ និងប្រើប្រាស់នៅឧបករណ៍វាយប្រហារប្រកបដោយភាពប៉ិនប្រសប់។

យុទ្ធសាស្ត្រវាយប្រហានានាបង្រួមចូលគ្នាតែមួយសំដៅលើការបង្រួមចូលគ្នានៃយុទ្ធវិធីវាយប្រហារក្នុងលក្ខណៈផ្សេងៗគ្នា រួមបញ្ចូលគ្នាតែមួយដោយអ្នកវាយលុកទាំងនោះដើម្បីបង្កើតជាបណ្តាញសកលដែលគាំទ្រនៅរាល់សកម្មភាពដែលប្រកបដោយគ្រោះថ្នាក់នោះ។ ឧទាហរណ៍ដូចជា MPack ដែលម៉ាស៊ីនរបស់អ្នកប្រើប្រាស់ម្នាក់មានផ្ទុកមេរោគ Trojan ហើយធ្វើការទំនាក់ទំនងជាមួយនិង**ម៉ាស៊ីនមេ** របស់ MPack ។ អ្នកលុកលុយបង្កើតចរាចរណ៍មួយទៅកាន់ Server នោះដោយបង្កើតគេហទំព័រស្របច្បាប់មួយ ដូច្នេះនៅពេលអ្នកប្រើប្រាស់ចូលទៅកាន់គេហទំព័រនោះ វានឹងប្តូរទិសដៅវាឲ្យដំណើរការជាមួយគេហទំព័រណាដែលបង្កឲ្យមានគ្រោះថ្នាក់ដល់អ្នកប្រើប្រាស់ ឬក៏គ្រាន់តែផ្ញើរជាលក្ខណៈតភ្ជាប់របស់គេហទំព័រទាំងនោះទៅឲ្យអ្នកប្រើប្រាស់តាមរយៈសារជា Spam ។ ហើយបន្ទាប់មកគេហទំព័រដែលអាចបង្កគ្រោះថ្នាក់នោះប្តូរទិសដៅ Browser របស់អ្នកប្រើប្រាស់ឲ្យទៅ MPack Server វិញ។[12]

ការកើនឡើងនៅតាមតំរាមកំហែងពីការវាយប្រហារលើហេដ្ឋារចនាសម្ព័ន្ធ

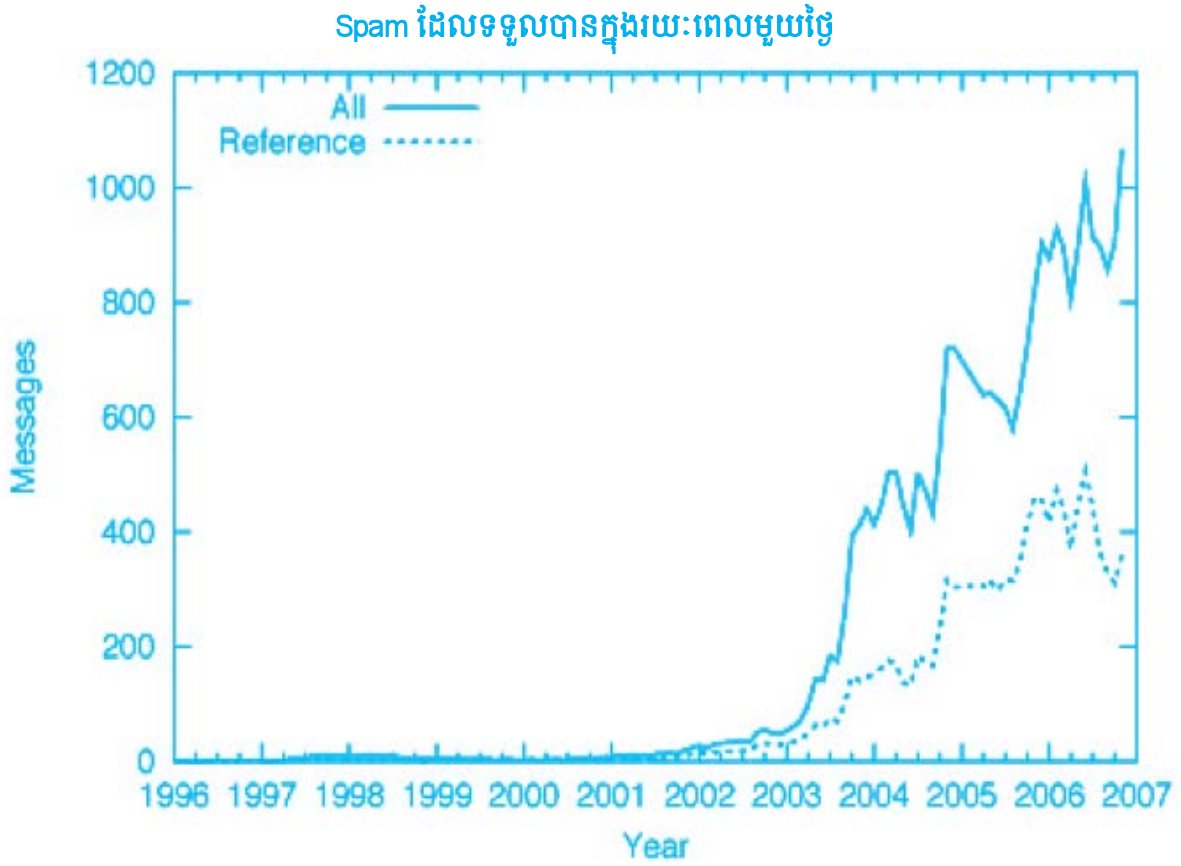
ការវាយប្រហារលើហេដ្ឋារចនាសម្ព័ន្ធគឺជាការវាយប្រហារទាំងឡាយណាដែលបង្កឲ្យមានផលប៉ះពាល់លើធាតុសំខាន់ៗនានាលើប្រព័ន្ធអ៊ីនធើរណិត។ ពួកគេគឺជាការបង្កឲ្យមានភាពខ្វល់ខ្វាយមួយដោយចំនួននៃអង្គការ និងអ្នកប្រើប្រាស់នានានៅលើប្រព័ន្ធអ៊ីនធើរណិតបានពឹងផ្អែកកាន់តែច្រើនលើប្រព័ន្ធមួយនេះក្នុងការធ្វើជំនួញរបស់ពួកគេពីមួយថ្ងៃទៅមួយថ្ងៃ។ការវាយប្រហារលើហេដ្ឋារចនាសម្ព័ន្ធគឺបណ្តាលមកពី DoS ដោយការប្រឌិតនៅព័ត៌មាន ហើយចែកចាយនៅព័ត៌មានដែលមិនត្រឹមត្រូវ និងបង្វែរនៅប្រភពនានាពីកិច្ចការដទៃៗទៀត។ Botnet គឺជាឧបករណ៍មួយសម្រាប់ការវាយប្រហារលើហេដ្ឋារចនាសម្ព័ន្ធ។ ក្រុមនៃ ‘Botnet’ សំដៅលើក្រុមមួយដែលធ្វើការបំផ្លាញកុំព្យូទ័រដោយបញ្ជារបស់ Server មួយដែលត្រូវបានប្រើ

12 Symantec, *Symantec Internet Security Threat Report: Trends for January–June 07*, Volume XII (September 2007), 13, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf.

ប្រាស់សម្រាប់ការបំផ្លាញពីចម្ងាយ។ កុំព្យូទ័រដែលទទួលរងផលប៉ះពាល់ទាំងនោះបានចែកចាយមេរោគ Worm និង Trojan ជាច្រើនឆ្លងកាត់ប្រព័ន្ធបណ្តាញ។

Spam ត្រូវបានបង្កើនចំនួនរបស់វាម្តងហើយម្តងទៀតដោយសារការបញ្ជារពីក្រុម Botnet។ Spam សំដៅលើសារទាំងឡាយណាដែលមិនរៃអង្គាសប្រាក់ចំណេញដែលជាញឹកញាប់វាធ្លាក់ចូលទៅក្នុងប្រអប់សារនៅក្នុងអ៊ីមែល សាររហ័ស (Instant Messages) ជំនាញស្វែងរក (Search engines) កំនត់ត្រាប្រចាំថ្ងៃលើប្រព័ន្ធអ៊ីនធើរណិត (Blogs) និងសូម្បីតែតាមរយៈទូរស័ព្ទដៃក៏មានដែរ។ រូបភាពទី៤បង្ហាញនិន្នាការនៅក្នុងចំនុះនៃ Spam.

រូបទី៤. ស្ថិតិ Spam



ការប្រឆាំងតបតនឹង Botnet

ដើម្បីកាត់បន្ថយការបំផ្លាញពី Botnet សហគមន៍ទូរគមនាគមន៍អន្តរជាតិបានផ្តល់អនុសាសន៍ឲ្យកាត់បន្ថយការរួមបញ្ចូលគ្នានៃគោលការណ៍ច្បាប់ បច្ចេកវិទ្យា និងយុទ្ធវិធីនៃសង្គម។

គោលការណ៍ច្បាប់:ប្រឆាំងនឹង Spam ប្រកបដោយប្រសិទ្ធិភាព ច្បាប់នានាទាក់ទងរលកសញ្ញាឧក្រិដ្ឋកម្ម និងធ្វើឲ្យមានភាពស្របច្បាប់

- កសាងសម្ថភាពក្នុងចំណោមច្បាប់ដែលមានការជាប់ទាក់ទងនានារបស់ក្រុមហ៊ុនទាំងឡាយ។
- បង្កើតគម្រោងការយ៉ាងទូលំទូលាយសម្រាប់ការឈានទៅរកកិច្ចសហប្រតិបត្តិការជាអន្តរជាតិ
- ធ្វើឲ្យមានស្ថិរភាពចំពោះច្បាប់ឯកជនភាព និងច្បាប់នៃរលកសញ្ញាឧក្រិដ្ឋកម្ម
- គម្រោងការយ៉ាងគំហុកដើម្បីធ្វើឲ្យមានការថយចុះនូវសកម្មភាព Botnet និងរលកសញ្ញាឧក្រិដ្ឋកម្មក្នុងតំបន់។

បច្ចេកទេស:ឧបករណ៍ និងបច្ចេកវិទ្យានានាត្រូវបានប្រើដើម្បីកំនត់ និងប្រមូលព័ត៌មានអំពីសកម្មភាព Botnet

- ISP ត្រូវអនុវត្តឲ្យបានល្អបំផុតដើម្បីបន្ថយនៅសកម្មភាពរបស់ Botnet
- អ្នកកាន់កាប់បញ្ជី និងការចុះឈ្មោះត្រូវធ្វើឡើងដោយល្អបំផុតដើម្បីបន្ថយសកម្មភាពរបស់ Botnet
- កសាងសមត្ថភាពឲ្យការធ្វើជំនួញលើប្រព័ន្ធ Online (e-commerce) និងអ្នកផ្តល់នៅការធ្វើជំនួញលើប្រព័ន្ធ Online នេះ។

សង្គម:ផ្តល់ការអប់រំយ៉ាងទូលំទូលាយទៅលើសន្តិសុខ និងសុវត្ថភាពលើប្រព័ន្ធអ៊ីនធើរណិត

- ជួយធ្វើការសម្របសម្រួលនានាដើម្បីការប្រើប្រាស់របស់អ្នកប្រើប្រាស់ឲ្យមានភាពមាំមួនក្នុងដំណើរការលើ ICT។

>>

>>

PIF ITU Spam គឺជាកញ្ចប់ព័ត៌មានដ៏ទូលំទូលាយដើម្បីជួយដល់អ្នកបង្កើតច្បាប់នានា និយតករ និងក្រុមហ៊ុនទាំងឡាយគ្រាន់តែធ្វើការកែសម្រួលនៅលើគោលការណ៍នោះដើម្បីអាចទាញយកមកវិញនូវភាពដ៏គួរឲ្យទុកចិត្តបាន នៅក្នុងការប្រើប្រាស់អ៊ីមែល។ PIF ITU Spam បានផ្តល់អនុសាសន៍ផងដែរឲ្យមានការចែកចាយព័ត៌មានពីប្រទេសមួយទៅប្រទេសមួយដើម្បីការពារនៅបញ្ហាជាអន្តរជាតិ។

ផ្ទាស់ប្តូរលើគោលបំណងនៃការវាយប្រហារ

ការវាយប្រហារលើកុំព្យូទ័រ និងនៅលើប្រព័ន្ធបណ្តាញគឺត្រូវបានធ្វើឡើងគ្រាន់តែចង់ដឹងចង់ឃើញ ឬសម្រាប់ការកំសាន្ត។ ឥឡូវគោលបំណងនៃការវាយប្រហារជាទូទៅគឺលុយ ការបង្ខូចកេរ្តិ៍ឈ្មោះ និងការបំផ្លាញ។ច្រើនជាងនេះទៀតប្រភេទនៃការវាយលុកទាំងនេះគ្រាន់តែតំណាងឲ្យផ្នែកតូចនៃវិសាលគមដ៏ធំនៃរលកសញ្ញាភេរវកម្មតែប៉ុណ្ណោះ។

រលកសញ្ញាឧក្រិដ្ឋកម្មគឺជាគម្រោងការបំផ្លាញដែលគ្រោងទុកជាមុន ការឆាវៅ ឬការធ្វើឲ្យខុសភាពដើមនៃទិន្នន័យឌីជីថល ឬព័ត៌មានដែលទាក់ទងនឹងនយោបាយ សេដ្ឋកិច្ច សាសនា ឬក៏ហេតុផលនានានៃគតិវិជ្ជា។ ភាគច្រើននៃឧក្រិដ្ឋកម្មសាមញ្ញៗរួមមាន Hacker, DoS កូដប្រកបដោយគ្រោះថ្នាក់ (malicious code) និងវិស្វកម្មសង្គម។ ពេលថ្មីនេះរលកសញ្ញាឧក្រិដ្ឋកម្មបានក្លាយជាផ្នែកមួយនៃរលកសញ្ញាភេរវកម្ម និងរលកសញ្ញានៃការធ្វើសង្គ្រាម ដែលជាផលប៉ះពាល់ដ៏អាក្រក់ទៅលើសន្តិសុខជាតិ។

តារាងលេខ៣ខាងក្រោមបង្ហាញអ្វីដែលអ្នកប្រព្រឹត្តនៅរលកសញ្ញាឧក្រិដ្ឋកម្មរកប្រាក់បានពីការធ្វើរបស់ពួកគេ

តារាងលេខ៣.ត្រឡប់ទៅរករលកសញ្ញាឧក្រិដ្ឋកម្មដែលកើតឡើងក្នុងឆ្នាំ ២០០៧

ទ្រព្យសម្បត្តិ	អត្រាដែលចំណាយ (គិតជារូបីយប័ណ្ណសហរដ្ឋ)
ការចំណាយលើការតំឡើងកម្មវិធីមួយ	៣០សេននៅក្នុងសហរដ្ឋអាមេរិក ២០សេននៅក្នុងកាណាដា ១០សេននៅក្នុងចក្រភពអង់គ្លេស ២សេននៅកន្លែងផ្សេងទៀត
Malware Package ជំនាន់ដើម	១000 - ២000ដុល្លារ
Malware Package ជាមួយសេវាកម្មផ្សេងទៀត	មានតម្លៃផ្សេងៗពីគ្នា ដែលតម្លៃនោះចាប់ពី ២០ ដុល្លាឡើងទៅ
អាជីវកម្មលើការជួលឧបករណ៍ - ១0ម៉ោង	០.៩៩ ទៅ ១ដុល្លារ
អាជីវកម្មលើការជួលឧបករណ៍ - ២.៥ម៉ោង	១.៦0 ទៅ ២ដុល្លារ
អាជីវកម្មលើការជួលឧបករណ៍ - ៥ម៉ោង	៤ដុល្លារ ឬប្រហែលផ្សេងពីនេះទៀត
ការលួចចំលងព័ត៌មានដោយប្រើ Trojan	៨0ដុល្លារ ឬប្រហែលផ្សេងពីនេះទៀត
វាយប្រហារដោយការចែកចាយមេរោគ DoS	១00ដុល្លាសម្រាប់រយពេលមួយថ្ងៃ
សម្រាប់ ១000 កុំព្យូទ័រ ក្នុងការផ្ញើរលកសញ្ញាឧក្រិដ្ឋកម្មទៅកាន់	១000ដុល្លារ
ការលួចគណនីយធនាគារ	កំណាត់តម្លៃចាប់ពី៥0ដុល្លារឡើងទៅ
ការប្រមូលអ៊ីមែលថ្មីៗបានចំនួនមួយលាន	តម្លៃចាប់ពី ៨ដុល្លារឡើងអាស្រ័យលើគុណភាពអ៊ីមែលនោះ

Source:Trend Micro, *2007 Threat Report and Forecast* (2007), 41, http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf

២.៣ ការធ្វើឲ្យប្រសើរឡើងផ្នែកសន្តិសុខ

ការវាយប្រហារតាមរយៈបច្ចេកវិទ្យា និងការគំរាមកំហែងនានាដែលបានរៀបរាប់មកនោះ រនាំងការពារដ៏រឹងមាំមួយគឺត្រូវស្នើឲ្យប្រើនៅយុទ្ធសាស្ត្រប្រកបដោយការបត់បែនដែលអាចប្រែប្រួល ទៅតាមទីកន្លែងដែលមានការវាយប្រហារ គោលការណ៍ច្បាប់ដ៏ល្អក្នុងការកំនត់លើការវាយប្រហាររួមទាំងនិតិក្រមនានាប្រើប្រាស់នៅបច្ចេកវិទ្យាដែលមានភាពសាកសមក្នុងការរក្សាសន្តិសុខ និងការឃ្លាំមមើលជាប្រចាំ។

វាគឺមានប្រយោជន៍ ដើម្បីចាប់ផ្តើមកម្មវិធីដែលជំរុញឲ្យមានភាពកាន់តែប្រសើរលើផ្នែកសន្តិសុខដោយគោរពទៅតាមសេចក្តីប្រកាសនៅពេលថ្មីៗនេះស្តីពីសន្តិសុខ។ រាល់កម្មវិធីសន្តិសុខទាំងអស់គឺត្រូវបានធ្វើឡើងដោយមានការសំអាងលើច្បាប់ និងនីតិក្រមនានាក៏ដូចដែលបច្ចេកវិទ្យាគាំទ្រលើការប្រើប្រាស់របស់កម្មវិធី សន្តិសុខទាំងនោះ។

សន្តិសុខរដ្ឋបាល

សន្តិសុខរដ្ឋបាលរួមមានយុទ្ធវិធី គោលការណ៍ច្បាប់ និងការណែនាំនានារបស់សន្តិសុខព័ត៌មាន។

យុទ្ធវិធីសន្តិសុខព័ត៌មាន បង្កើតនៅទិសដៅសម្រាប់រាល់សកម្មភាពរបស់សន្តិសុខព័ត៌មាន។

គោលការណ៍ច្បាប់សន្តិសុខព័ត៌មាន គឺជាគំរោងឯកសារដ៏សំខាន់សម្រាប់សន្តិសុខព័ត៌មានដ៏ធំធេងរបស់អង្គការ វាផ្តល់នៅគម្រោងមួយសម្រាប់ធ្វើការសម្រេចចិត្តជាក់លាក់ណាមួយដូចជាគម្រោងសន្តិសុខផ្នែករដ្ឋបាល និងលក្ខណៈសណ្ឋានពិតរបស់វា។

ពីព្រោះតែគោលការណ៍ច្បាប់សន្តិសុខព័ត៌មានមាននៅចំនុចដែលបង្កពីទស្សនៈវែងឆ្ងាយរបស់ស្ថាប័នណាមួយនោះ ដូច្នេះវាគួរតែចៀសវាងការប្រើនៅមាតិការចំៗនៃបច្ចេកទេស និងរួមទាំងគម្រោងអភិវឌ្ឍន៍ជានិរន្តភាពនៃកិច្ចការជំនួញដេលកមពុងដំណើរការរបស់ស្ថាប័ននោះ។

ការណែនាំនានាពីសន្តិសុខព័ត៌មាន: គួរត្រូវបានបង្កើតឡើងដោយយោងទៅលើយុទ្ធវិធី និងគោលការណ៍ច្បាប់របស់សន្តិសុខព័ត៌មាន។ ការណេនាំទាំងនោះគួរមាននៅនិយតករដ៏ជាក់លាក់សម្រាប់តំបន់និមួយៗដែលមានទំនាក់ទំនងទៅនឹងសន្តិសុខព័ត៌មាន។ និងពីព្រោះតែការណែនាំទាំងនោះមានលក្ខណៈទូលំទូលាយ និងស្ថិតក្នុងដែនសីមារបស់ជាតិនោះ ពួកគេត្រូវតែបានធ្វើការអភិវឌ្ឍន៍បន្ថែមព្រមទាំងត្រូវបានចែកចាយដោយរដ្ឋាភិបាលសម្រាប់គ្រប់ស្ថាប័ន្តគោរពតាម។

គំរូនានារបស់សន្តិសុខព័ត៌មាន: ពិតជាត្រូវបានធ្វើឯកទេសកម្ម និងប្រកបដោយភាពជាក់លាក់ដូច្នេះពួកគេអាចត្រូវបានយកទៅដាក់ឲ្យប្រើប្រាស់នៅគ្រប់តំបន់នៃសន្តិសុខព័ត៌មាន។ វាគឺល្អសម្រាប់ប្រទេសនិមួយៗដើម្បីធ្វើការអភិវឌ្ឍន៍នៅគំរូទាំងឡាយនោះបន្ទាប់ពីធ្វើការវិភាគ ទៅលើគំរូនានារបស់សន្តិសុខ

បច្ចេកវិទ្យា សន្តិសុខលក្ខណៈសណ្ឋានពិត និងសន្តិសុខរដ្ឋបាលដែលការធ្វើវិភាគនោះត្រូវបានគេធ្វើយ៉ាងទូលំទូលាយនៅទូទាំងពិភពលោក។ គំរូទាំងឡាយនោះគួរតែមានលក្ខណៈសមរម្យជាមួយ និងបរិស្ថានធម្មតារបស់ ICT ។

យុទ្ធសាស្ត្រ, គោលការណ៍ច្បាប់, និងសេចក្តីណែនាំនានារបស់សន្តិសុខព័ត៌មានរបស់ប្រទេសមួយគួរតែគោរពទៅតាមច្បាប់ដែលជាប់ពាក់ព័ន្ធ ។ រយៈកាលរបស់ពួកគេគួរតែស្ថិតនៅក្នុងដែនកំនត់នៃច្បាប់ជាតិ និង អន្តរជាតិ ។

ដំណើរការ និងការអនុវត្តន៍លើសន្តិសុខព័ត៌មាន

ម្តងទៀតសេចក្តីណែនាំទាំងឡាយ គោលការណ៍ច្បាប់ និងយុទ្ធវិធីរបស់សន្តិសុខព័ត៌មានគឺត្រូវបានគេបង្កើតឡើង។ ដូចនេះការអនុវត្តន៍នៃនីតិក្រម និងដំណើរការលើសន្តិសុខព័ត៌មាន និងត្រូវការឲ្យមានការកំនត់យ៉ាយច្បាស់លាស់។ ពីព្រោះមនុស្សគឺជាបុគ្គលដែលប្រព្រឹត្តនៅការវាយប្រហារទៅលើព័ត៌មាន ឬធ្វើឲ្យលេចចេញនៅព័ត៌មាន ដូច្នេះការគ្រប់គ្រងលើធនធានមនុស្ស គឺជាកត្តាដ៏សំខាន់បំផុតនៅក្នុងការអនុវត្តន៍សន្តិសុខព័ត៌មាន។ ហេតុនេះគេត្រូវការធ្វើដូចខាងក្រោម៖

១. កម្មវិធីហ្វឹកហ្វឺន និងអប់រំអំពីសន្តិសុខព័ត៌មាន - គឺមានយុទ្ធវិធីជាច្រើនដើម្បីបង្កើនឡើងនៅកម្រិតយល់ដឹងរបស់ស្ថាប័ន ប៉ុន្តែវគ្គហ្វឹកហ្វឺន និងអប់រំគឺជាសកម្មភាពដំបូងដែលគេត្រូវធ្វើ។ សមាជិកទាំងឡាយនៃស្ថាប័នពិតជាអបអរពីគុណភាពតម្លៃលើសេចក្តីត្រូវការលើសន្តិសុខព័ត៌មាន និងទទួលបាននៅជំនាញផ្សេៗទៀតដែលទាក់ទងនឹងសន្តិសុខព័ត៌មានតាមរយៈការអប់រំនិងវគ្គហ្វឹកហ្វឺនទាំងនោះ។ ទោះបីជាយ៉ាងណាក៏ដោយវាគឺសំខាន់ក្នុងការអភិវឌ្ឍន៍នៅកម្មវិធីផ្សេងៗហើយដាក់វាចូលរួមក្នុងការអប់រំនោះឲ្យបានច្រើន ពីព្រោះថាការអប់រំវគ្គហ្វឹកហ្វឺនពីសន្តិសុខព័ត៌មានដែលគោរពទៅតាមគំរូដែលបានកំនត់មកប្រហែលជាមិនមានប្រសិទ្ធិភាពទេល។

២. ធ្វើការជំរុញដ៏ខ្លាំងក្លាតាំរយៈព្រឹត្តិការផ្សេងៗដ៏ទៃទៀតឲ្យបានច្រើន - ការចូលរួមរបស់និយោជិកគឺសំខាន់នៅក្នុងការអនុវត្តន៍ប្រកបដោយភាពជោគជ័យនៃសេចក្តីណែនាំ គោលការណ៍ច្បាប់ និង

យុទ្ធវិធីរបស់សន្តិសុខព័ត៌មាន។ សន្តិសុខព័ត៌មានគួរត្រូវបានជំរុញឲ្យមានការអនុវត្តន៍ក្នុងចំណោមនិយោជិកតាមរយៈសកម្មភាពផ្សេងៗប្រចាំថ្ងៃ។

៣. ភាពមានអ្នកធានាលើសន្តិសុខ - ខណៈពេលដែលវាបានក្លាយទៅជាសន្តិសុខព័ត៌មានស្ថិតនៅក្នុងកម្រិតខ្ពស់របស់និយោជិក ហើយពួកគេទាំងនោះនិងមានឆន្ទៈមោះមុតក្នុងការថែរក្សានៅសន្តិសុខព័ត៌មាននោះ។ ដូច្នេះវាហាក់ដូចជាពិបាកក្នុងការធានាទៅលើសន្តិសុខព័ត៌មាន បើគ្មានការគាំទ្រពីថ្នាក់ដឹកនាំជាន់ខ្ពស់នៃស្ថាប័ន (អង្គការ)។ ការគាំទ្រពីប្រធានប្រតិបត្តិ និងមន្ត្រីប្រធានផ្នែកព័ត៌មានគួរតែមាន។

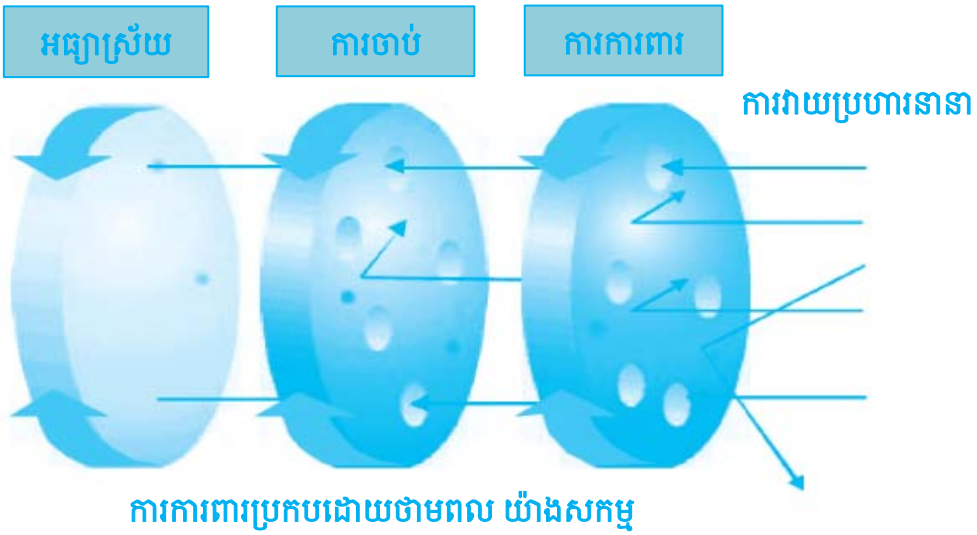
សន្តិសុខដែលប្រើឆ្លងបច្ចេកវិទ្យា

បច្ចេកវិទ្យាផ្សេងៗជាច្រើនត្រូវបានអភិវឌ្ឍន៍ឡើងដើម្បីជួយអង្គភាពនានារក្សានូវប្រព័ន្ធព័ត៌មានរបស់ពួកគេប្រឆាំងនឹងអ្នកលុកលុយទាំងឡាយ។ បច្ចេកវិទ្យាទាំងនេះចួយការពារប្រព័ន្ធ និងព័ត៌មានប្រឆាំងនឹងការវាយលុកជាច្រើន។ ជួយចាំនៅសកម្មភាពណាដែលមានលក្ខណៈខុសធម្មតា និងគួរឲ្យសង្ស័យ ព្រមទាំងឆ្លើយតបចំពោះព្រឹត្តិការណ៍ទាំងឡាយនាដែលបង្កឲ្យមានផលប៉ះពាល់ដល់សន្តិសុខ។

ប្រព័ន្ធសន្តិសុខជាច្រើនក្នុងពេលបច្ចុប្បន្នត្រូវបានបង្កើត និងអភិវឌ្ឍន៍ឡើងដោយផ្អែកលើគំរូការការពារដ៏រឹងមាំ (Defense-In-Depth model) ដែលនាំទៅរកការគ្រប់គ្រងលើការបង្រួបបង្រួមនៅបច្ចេកវិទ្យានានាដែលជាប់ពាក់ព័ន្ធក្នុងការការពារ។ គំរូនេះគឺខុសពីគំរូបាំងការពារក្នុងបរិវិលា (perimeter-defense) ដែលមានត្រឹមតែមួយស្រទាប់ដែលការពារប្រឆាំងរាល់ការគំរាមកំហែងជាច្រើន។គំរូ DID រួមមានទាងការការពារ ការចាប់នឹងការអធ្យាស្រ័យ ជាមួយការគំរាមកំហែងទាំងនោះកំពុងត្រូវបានកាត់បន្ថយតាមដំណាក់កាលនិមួយៗ។ (រូបទី ៥)

រូបភាពទី៥.ការការពារជ្រៅជ្រះ (Defense In Depth)

(Source: Defense Science Board, *Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II* (Washington, D.C.: Defense Science Board, 2001), 5, http://www.acq.osd.mil/dsb/reports/dio.pdf)



បច្ចេកវិទ្យាលើការការពារ

បច្ចេកវិទ្យាលើការការពារទប់ទល់ប្រឆាំងនឹងអ្នកឈ្លានពាន និងការគំរាមកំហែងទាំងឡាយនៅឯកម្រិតនៃការរក្សា ឬក៏កម្រិតរបស់ប្រព័ន្ធ។ បច្ចេកវិទ្យាទាំងនេះរួមមានដូចខាងក្រោម៖

១. **ហោ**ស្យលិខសាស្ត្រ - ផងដែរសំដៅលើការបំលែងតួអក្សរទៅកាន់អក្សរដែលមិនអាចមើលយល់ដោយមនុស្ស (encryption) ហោស្យលិខសាស្ត្រគឺជាដំណើរការនៃការបកប្រែព័ត៌មានពីទម្រង់ដើមរបស់វាត្រូវបានហៅថា (plaintext) ចូលទៅក្នុងអក្សរសាំញ៉ាំ (encode) ទម្រង់ដែលមិនអាចយល់បានហៅថា (ciphertext) Deryption សំដៅទៅលើដំណើរការនៃការយក ciphertext និងបកប្រែវាចូលទៅទម្រង់ដើមវិញដែលអាចមើលយល់ដោយមនុស្ស។ ហោស្យលិខសាស្ត្រគឺត្រូវបានគេប្រើដើម្បីការពារលើកម្មវិធីផ្សេងៗជាច្រើន។ ព័ត៌មានបន្ថែមអំពីរហោស្យលិខសាស្ត្រ និងបច្ចេកវិទ្យានានា

ដែលមានទំនាក់ទំនងជាមួយវា (IPSec, SSH, SSL, VPN, OTP, etc) គឺអាចរកបាននៅឯគេហទំព័រដូចខាងក្រោម៖

. IETF RFC (http://www.ietf.org/rfc.html)

. RSA Laboratories'Frequently Asked Question About Today's Cryptography (http://www.rsa.com/rsalabs/node.asp?id=2152)

២. អក្សរកាត់ដែលប្រើបានតែម្តង One-time passwords (OTP) - ដូចដែលឈ្មោះរបស់វា អក្សរសម្ងាត់ដែលប្រើបានតែម្តងអាចត្រូវបានគេប្រើត្រឹមតែមួយដងដែលមិនមានការផ្លាស់ប្តូរលើវា។តាមស្ថិតិនៃការដាក់អក្សរសម្ងាត់អាចត្រូវបានដំណើរការបានដោយងាយស្រួលដោយការលុបនូវអក្សរសម្ងាត់នោះ ការលួចនៅអក្សរសម្ងាត់នោះ ការបំបែកនូវអក្សរសម្ងាត់ក្នុងលក្ខណៈដ៏ថោកទាបនិងសកម្មភាពដូចនេះផ្សេងទៀត។ ហានិភ័យអាចត្រូវបានកាត់បន្ថយយ៉ាងធំធេងដោយការប្តូរទៅអក្សរសម្ងាត់ជាញឹកញាប់ទៅលេ One-time Password (OTP) ។សម្រាប់ហេតុផលនេះ OTP គឺត្រូវបានប្រើដើម្បីរក្សាការធ្វើចរាចរនៃហិរញ្ញវត្ថុតាមប្រព័ន្ធអេឡិចត្រូនិចដូចជាដំណើរធនាគារលើប្រព័ន្ធ Online ។

៣. Firewall (ជញ្ជាំងភ្លើង) – Firewall ធ្វើឲ្យមានរបៀបរាបរយលើដំណើរហូរចូលនៃចរាចររវាងបណ្តាញកុំព្យូទ័រនៃភាពផ្សេងគ្នាតាមកម្រិតដែលគួរឲ្យទុកចិត្តបានដូចជាធ្វើឡើងរវាងប្រព័ន្ធអ៊ីនធើរណិត ដែលជាតំបន់ដែលមិនគួរឲ្យទុកចិត្ត និងប្រព័ន្ធបណ្តាញខាងក្នុងដែលជាប្រព័ន្ធមានការទុកចិត្តខ្ពស់។ តំបន់ដែលមានកម្រិតនៃការទុកចិត្តជាមធ្យមគឺជាតំបន់ដែលតាំងនៅរវាងប្រព័ន្ធអ៊ីនធើរណិត និងបណ្តាញខាងក្នុងដែលមានភាពទុកចិត្តបាន ជាញឹកញាប់វាសំដៅទៅលើ 'perimeter network' ឬក៏តំបន់ដែលមិនមានទំព។

៤. ឧបករណ៍ធ្វើការវិភាគលើភាពដែលងាយរងគ្រោះ – ដោយសារការកើនឡើងនៅចំនួនយុទ្ធវិធីលើការវាយប្រហារជាច្រើន និងភាពងាយរងគ្រោះជាច្រើនក្នុងពេលបច្ចុប្បន្ននៅក្នុងការប្រើប្រាស់នៅកម្មវិធីយ៉ាងសាមញ្ញមួយចំនួន។ វាគឺចាំបាច់ដោយកំណត់ពេលបានប្រមាណមើលនៅភាពរងគ្រោះនានារបស់ប្រព័ន្ធ។ នៅក្នុងសន្តិសុខកុំព្យូទ័រ ភាពងាយរងគ្រោះគឺជាភាពទន់ខ្សោយដែលអនុញ្ញាតឲ្យអ្នកវាយលុកអាចវាយប្រហារលើប្រព័ន្ធ។ភាពងាយស្រួលអាចមកពីលេខសម្ងាត់ មិន

មានលក្ខណៈរឹងមាំ Software bugs (សត្វល្អិតរបស់ផ្នែកទន់) មេរោគកុំព្យូទ័រ Script code, injection, SQL injection or malware។ ឧបករណ៍វិភាគលើភាពងាយរងគ្រោះគឺចាប់នៅភាពដែលងាយរងគ្រោះទាំងនេះ។ពួកគេអាចរកបានយ៉ាងងាយស្រួលនៅលើ Online និងគឺមានក្រុមហ៊ុនជាច្រើនដែលផ្តល់នៅសេវាកម្មលើការវិភាគនេះ។ទោះបីជាយ៉ាងណាក៏ដោយ ការប្រើសេវាកម្មយ៉ាងសេរីលើការវិភាគនោះអាចត្រូវបាននាំទៅរកការប្រើនៅគេហទំព័រ ឬវិភាគខុសដែលធ្វើឡើងដោយអ្នកវាយលុកទៅវិញ។ សំរាប់ព័ត៌មានបន្ថែមសូមមើលខាងក្រោម៖

- INSECURE Security Tool (http://sectools.org)
- FrSIRT Vulnerability Archive (http://www.frsirt.com/english)
- Secunia Vulnerability Archive (http://secunia.com)
- SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)

ឧបករណ៍វិភាគលើភាពងាយរងគ្រោះរបស់បណ្តាញទៅលើភាពងាយស្រួលរងគ្រោះនានានៃប្រភពដើមជាច្រើនរបស់បណ្តាញដូចជា៖ Router, Firewalls និង Server។

ឧបករណ៍វិភាគលើភាពងាយរងគ្រោះរបស់ម៉ាស៊ីនមេគឺធ្វើវិភាគលើភាពងាយរងគ្រោះនានាដូចជាលេខសម្ងាត់ដែលមានភាពខ្សោយ ភាពទន់ខ្សោយខាងការរៀបចំ និងការខុសឆ្គងលើការអនុញ្ញាតដែលស្ថិតនៅខាងក្នុងប្រព័ន្ធ។ឧបករណ៍វិភាគលើភាពងាយរងគ្រោះរបស់ម៉ាស៊ីនមេគឺផ្តល់នៅលទ្ធផលដែលមានភាពសុក្រិតជាងការធ្វើវិភាគភាពងាយរងគ្រោះលើបណ្តាញពីព្រោះថាវាវិភាគនៅលើចំនុចដែលងាយរងគ្រោះជាច្រើននៅផ្នែកខាងក្នុងប្រព័ន្ធ។

ឧបករណ៍វិភាគលើភាពងាយរងគ្រោះសម្រាប់គេហទំព័រគឺធ្វើការវិភាគលើភាពងាយរងគ្រោះទាំងឡាយនៃកម្មវិធីនានាដែលដំណើរការលើគេហទំព័រដូចជា XSS និង SQL Injection ដែលបានប្រើបង្ហោះនៅលើគេហទំព័រ។សម្រាប់ព័ត៌មានបន្ថែមសូមមើល Open Web Application Security Project នៅឯគេហទំព័រ http://www.owasp.org/index.php/Top_10_2007

បច្ចេកទេសខាងចាប់

បច្ចេកទេសខាងចាប់គឺត្រូវបានគេប្រើដើម្បីចាប់ និងតាមដាននៅការប្រកាសខុសធម្មតានានានិងការឈ្លានពានចូលទៅក្នុងប្រព័ន្ធបណ្តាញ ឬចូលទៅកាន់ប្រព័ន្ធសំខាន់មួយចំនួន។បច្ចេកទេសខាងចាប់រួមមានដូចខាងក្រោម៖

១. កម្មវិធីប្រឆាំងមេរោគ - កម្មវិធីប្រឆាំងនឹងមេរោគគឺជាកម្មវិធីកុំព្យូទ័រសម្រាប់កំនត់ ការប្រឆាំងឬការកំចាត់ចោលនៅកូដប្រកបដោយគ្រោះថ្នាក់ (malicious code) ដែលរួមមាន Worm , phishing attacks, tootkits, Trojan horses និង malware ដ៏ទៃទៀត។[13]

២. ប្រព័ន្ធនៃការចាប់នៅការឈ្លានពាន (IDS)- IDS ប្រមូល និងវិភាគនៅព័ត៌មានស្តីពីតំបន់មេរោគទាំងឡាយដែលស្ថិតនៅក្នុងកុំព្យូទ័រ ឬក៏បណ្តាញដើម្បីកំនត់នៅភាពប្រេះបែកលើសន្តិសុខដែលអាចកើតមាន។ តួនាទីរបស់ការចាប់នៅការឈ្លានពាន (IDS) រួមទាំងការវិភាគនៅគំរូសកម្មភាពខុសប្រក្រតីនានា និងមានសមត្ថភាពស្គាល់នៅគំរូវាយប្រហារជាច្រើន។

៣. ប្រព័ន្ធការពារការលុកលុយ (IPS) - ការពារការលុកលុយគឺប៉ុនប៉ងដើម្បីកំនត់នៅសក្តានុពលនៃការគំរាមកំហែងនានា និងឆ្លើយតបចំពោះពួកគេវិញមុនដែលការលុកលុយនោះត្រូវធ្វើការវាយប្រហារមក។ IPS ត្រួតពិនិត្យមើលនៅរាល់ចរាចរលើបណ្តាញ និងធ្វើសកម្មភាពប្រឆាំងតបតភ្លាមៗទៅនឹងការគំរាមកំហែងដែលប្រកបដោយសក្តានុពលដោយយោងទៅតាមច្បាប់ដែលបានបង្កើតឡើងដោយរដ្ឋបាលបណ្តាញ។ ឧទាហរណ៍: ISP ប្រហែលជាទប់ស្កាត់នៅចរាចរណ៍ដែលមកពី IP address ដែលគួរឲ្យសង្ស័យ។[14]

13 Wikipedia, "Antivirus software," Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Antivirus_software.
14 SearchSecurity.com, "Intrusion prevention," TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00.html.

ការបញ្ចូលគ្នានៃបច្ចេកវិទ្យា

ការបញ្ចូលគ្នានៃបច្ចេកវិទ្យាគឺជាការបញ្ចូលគ្នានៅមុខងារសំខាន់ៗជាច្រើនសម្រាប់សន្តិសុខព័ត៌មាននៃទ្រព្យសម្បត្តិស្នូល ដូចជាការប្រមើរមើល ការចាប់ និងការតាមដានការឈ្លានពាន។ការបញ្ចូលគ្នានៃបច្ចេកវិទ្យាមានដូចខាងក្រោម:

១. ការគ្រប់គ្រងសន្តិសុខនៃសហគ្រាស (ESM) - ប្រព័ន្ធ ESM ធ្វើការគ្រប់គ្រង ធ្វើការត្រួតពិនិត្យ និងអនុវត្តន៍លើដំណោះស្រាយនៃសន្តិសុខព័ត៌មានដូចជា IDS និង ISP ដោយផ្តែកទៅលើគោលការណ៍ច្បាប់យ៉ាងម៉ឺងម៉ាត់។ វាគឺត្រូវបានប្រើយុទ្ធសាស្ត្រដើម្បីធ្វើលើសមាសភាពទន់ខ្សោយនានានៃដំណោះស្រាយដ៏ទៃដោយការប្រើនៅភាពសំខាន់ជាច្រើននៃដំណោះស្រាយលើសន្តិសុខប្រព័ន្ធនិមួយៗ និងបង្កើតនៅប្រសិទ្ធិភាពនៃសន្តិសុខព័ត៌មានឲ្យស្ថិតក្នុងកម្រិតអតិបរមាដែលនៅក្រោមគោលការណ៍ច្បាប់ដ៏រឹងមាំ។

ESMs ដែលអាចគ្រប់គ្រងលើបច្ចេកវិទ្យាសន្តិសុខដែលមានស្រាប់ហើយនោះបានក្លាយខ្លួនជាអ្នកសង្គ្រោះនៅក្នុងពេលថ្មីនេះពីព្រោះការខ្វះខាតនៅធនធានមនុស្សដើម្បីអនុវត្តន៍នៅបច្ចេកវិទ្យាសន្តិសុខ។ការកើនឡើងនៅក្នុងការវាយប្រហារថ្មីៗដូចជាយុទ្ធសាស្ត្រវាយប្រហាររួមបញ្ចូលគ្នាតែមួយ និងការផុសចេញនៅឧបករណ៍ប្រហារនានាដែលជាការពិបាកក្នុងការចាប់ពួកគេ។ ជាមួយ ESM ការគ្រប់គ្រងប្រកបដោយប្រសិទ្ធិភាពគឺបានងើបឡើង និងវិធានការយ៉ាងសកម្មគឺត្រូវបានបង្កើតឡើង។

២. ការគ្រប់គ្រងលើឧបទ្ទវហេតុនៃសហគ្រាស (ERM) – ERM គឺជាប្រព័ន្ធដែលជួយប៉ាន់ប្រមើរមើលទៅលើរាល់ឧបទ្ទវហេតុដែលកើតឡើងលើអង្គការនានារួមទាំងតំបន់ជាច្រើនដែលស្ថិតនៅខាងក្រៅសន្តិសុខព័ត៌មាន និងប្រើនៅវិធានការរៀបចំឡើងវិញដោយស្វ័យប្រវត្តិ។ ការប្រើ ERM ដើម្បីការពារព័ត៌មានតម្រូវថាត្រូវមាននៅគោលបំណងដ៏ប្រាកដមួយនៃការគ្រប់គ្រងលើហានិភ័យ និងការរៀបសម្រាប់ការអភិវឌ្ឍន៍លើប្រព័ន្ធត្រូវបានគេកំណត់យ៉ាងចំៗចំពោះការធ្វើនោះ។ អង្គការភាគច្រើនកសាង និងធ្វើឲ្យមានសុទិដ្ឋិនិយមដំពោះ ERMs ផ្ទាល់ខ្លួនរបស់អង្គការពួកគេតាមរយៈភ្ញាក់

ងារប្រឹក្សាដែលមានជំនាញខាងសន្តិសុខព័ត៌មានជំនួសការធ្វើនៅ ERMs នោះដោយខ្លួនពួកគេផ្ទាល់។

សំនួរត្រិះរិះ

១. តើការគំរាមកំហែងមួយណាលើសន្តិសុខព័ត៌មានរបស់អង្គការរបស់អ្នក ដែលអ្នកគិតថាវាធ្វើឲ្យប្រព័ន្ធសន្តិសុខព័ត៌មានរបស់អ្នកងាយរងគ្រោះ? ហេតុអ្វី?

២. តើដំណោះស្រាយបច្ចេកវិទ្យាលើសន្តិសុខព័ត៌មានមួយនា ដែលអង្គការរបស់អ្នកប្រើ?

៣. តើអង្គការរបស់អ្នកមានច្បាប់ យុទ្ធវិធី និងសេចក្តីណែនាំនានារបស់សន្តិសុខព័ត៌មានដែរឬទេ?ប្រសិនបើមាន តើវាគ្រប់គ្រាន់ដើម្បីទប់ស្កាត់នៅការគំរាមកំហែងនានាដែលបង្កឲ្យសន្តិសុខព័ត៌មានអង្គការអ្នកងាយរងគ្រោះ? ប្រសិនបើមាន តើអ្វីដែលអ្នកបានផ្តល់ជាអនុសាសន៍ស្តីអំពីច្បាប់ យុទ្ធវិធី និងសេចក្តីណែនាំនានារបស់សន្តិសុខព័ត៌មានសម្រាប់អង្គការអ្នក?

សាកល្បងខ្លួនអ្នក

១. ហេតុអ្វីបានជាការអនុវត្តន៍នៅការវិភាគលើនិន្នាការគំរាមកំហែងសន្តិសុខព័ត៌មានមានសារសំខាន់?

២. ហេតុអ្វីការគ្រប់គ្រងធនធានមនុស្សគឺជាកត្តាដ៏សំខាន់ក្នុងការអនុវត្តន៍នានាលើសន្តិសុខព័ត៌មាន?
តើអ្វីគឺជាសកម្មភាពដ៏សំខាន់ផ្សេងៗនៅក្នុងការគ្រប់គ្រងធនធានមនុស្សសម្រាប់សន្តិសុខព័ត៌មាន?

៣. ពន្យល់ពីគំរូសន្តិសុខព័ត៌មានដែលមានឈ្មោះថា Defense-In-Depth។តើវាធ្វើការដូចម្តេច?

៣. សកម្មភាពផ្សេងៗរបស់សន្តិសុខព័ត៌មាន

នៅត្រង់ចំនុចនេះចង់បង្ហាញពី៖

- ការឲ្យនៅឧបករណ៍អំពីសកម្មភាពផ្សេងៗរបស់សន្តិសុខព័ត៌មាននៃប្រទេសផ្សេងៗដែលត្រូវប្រើដូចជាការនាំផ្លូវមួយនៅក្នុងការបង្កើតគោលការណ៍ច្បាប់សន្តិសុខព័ត៌មាន។ និង
- បង្ហាញពីផ្នែកសំខាន់ៗលើសហប្រតិបត្តិការជាអន្តរជាតិនៅក្នុងការអនុវត្តន៍គោលការណ៍ច្បាប់សន្តិសុខព័ត៌មាន។

៣.១ សកម្មភាពផ្សេងៗរបស់សន្តិសុខព័ត៌មាន

យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានឆៃសហរដ្ឋអាមេរិក

បន្ទាប់ពីរងការវាយប្រហារភេរវកម្មនៅថ្ងៃទី ១១ ខែកញ្ញា ឆ្នាំ ២០០១ រដ្ឋាភិបាលរបស់សហរដ្ឋអាមេរិកបានបង្កើតស្ថាប័នសន្តិសុខផ្ទៃក្នុងដើម្បីពង្រឹងសន្តិសុខជាតិដែលមិនត្រឹមតែប្រយុទ្ធប្រឆាំងការគំរាមកំហែងក្នុងលក្ខណៈរូបភាពពិត ប៉ុន្តែប្រយុទ្ធប្រឆាំងនឹងរលកសញ្ញាគំរាមកំហែងនានាផងដែរ។ សហរដ្ឋអាមេរិកអនុវត្តន៍នៅសកម្មភាពផ្សេងរបស់សន្តិសុខព័ត៌មានប្រកបដោយប្រសិទ្ធិភាព និងមានភាពយ៉ាងទូលំទូលាយតាមរយៈប្រព័ន្ធមន្ត្រីសន្តិសុខព័ត៌មាន។ យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានរបស់វារួមមានយុទ្ធសាស្ត្រជាតិសម្រាប់សន្តិសុខផ្ទៃក្នុង យុទ្ធសាស្ត្រជាតិសម្រាប់សន្តិសុខលើលក្ខណៈរូបភាពពិតនៃហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ និងទ្រព្យសម្បត្តិដ៏មានតម្លៃផ្សេងទៀត និងយុទ្ធសាស្ត្រជាតិដើម្បីរក្សារលកសញ្ញាគ្មានដែនកំនត់ផ្សេងទៀត។

យុទ្ធសាស្ត្រជាតិដើម្បីរលកសញ្ញាគ្មានដែនកំនត់[15]បង្កើតបានជាគំនិតនៃសន្តិសុខរលកសញ្ញា និងការការពារនៃហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ និងទ្រព្យសម្បត្តិដ៏ទៃទៀត។វាកំនត់នៅគោលបំនង និងសកម្មភាពជាក់លាក់នានាសម្រាប់ទប់ស្កាត់ការវាយប្រហារជារលកសញ្ញាប្រឆាំងនឹងហេដ្ឋារចនាសម្ព័ន្ធ និងទ្រព្យសម្បត្តិ

15 The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, 2003), http://www.whitehouse.gov/pcipb.

ផ្សេងៗអាទិភាពប្រាំត្រូវបានកំនត់នៅក្នុងសន្តិសុខជាតិដើម្បីរក្សានៅរលកសញ្ញាគ្មានដែនកំនត់មាន ដូចជា៖

- ប្រព័ន្ធទទួលខុសត្រូវលើសន្តិសុខរលកសញ្ញាគ្មានដែនកំនត់
- កម្មវិធីកាត់បន្ថយភាពងាយរងគ្រោះ និងការគំរាមកំហែងលើសន្តិសុខរលកសញ្ញាគ្មានដែនកំនត់ជាតិ
- កម្មវិធីហ្វឹកហ្វឺន និងរៀបចំខ្លួនសម្រាប់សន្តិសុខរលកសញ្ញាគ្មានដែនកំនត់ជាតិ
- ការរក្សាសន្តិសុខរលកសញ្ញាគ្មានដែនកំនត់របស់រដ្ឋាភិបាល
- កិច្ចសហប្រតិបត្តិការលើសន្តិសុខជាតិ និងសន្តិសុខរលកសញ្ញាគ្មានដែនកំនត់ជាតិ

ការតបស្តីឆលើច្បាប់សន្តិសុខព័ត៌មាន

Cyber Security Enhancement Act of នៃឆ្នាំ ២០០២[16] (CSEA) ដាក់បញ្ចូលមាត្រា២នៃច្បាប់សន្តិសុខផ្ទៃក្នុងៗវាផ្តល់សម្រាប់មាត្រានានាធ្វើការកាត់សេចក្តីណែនាំលើឧក្រិដ្ឋកម្មកុំព្យូទ័រជាក់លាក់ណាមួយ ការប្រកាសអាសន្នអំពីភាពខុសប្រក្រតី ការលើកលែងសច្ចៈភាពល្អៗ ការផ្សព្វផ្សាយនៅការយោសនាខុសច្បាប់លើប្រព័ន្ធអ៊ីនធើរណិត និងការពារនៃឯកជនភាព ព្រមទាំងអ្វីៗទៀតៗ

Emergency Disclosure Exception : មុនថ្ងៃទី ៩ ខែវិច្ឆិកា Electronic Communications Privacy Act (ECPA) បានផ្សព្វផ្សាយពីអ្នកផ្តល់សេវាកម្មខាងគមនាគមន៍អេឡិចត្រូនិចនានាដូចជា (ISP) ជាការបើកបង្ហាញឲ្យមានទំនាក់ទំនងគ្នារបស់អ្នកប្រើប្រាស់ (ដូចជាតាមរយៈសារសម្លេង សារអេឡិចត្រូនិច និងការភ្ជាប់ឯកសារនានាជាមួយការផ្ទើរ)។ Emergency Disclosure Exception អនុញ្ញាតឲ្យ ISPs ចែករំលែកព័ត៌មាននៃសារអេឡិចត្រូនិច ឬការទំនាក់ទំនងតាមប្រព័ន្ធអេឡិចត្រូនិចជាមួយភ្នាក់ងារអនុវត្តន៍ច្បាប់ដោយមិនបាច់មានការអនុញ្ញាតដោយយោងទៅតាម USA Patriot Act ដែលបានចូលជាធរមានមន្ទាប់ពីថ្ងៃទី ១១ ខែកញ្ញា ឆ្នាំ២០០១។ករណីលើកលែងណាមួយនៃការបើកមើលនូវព័ត៌មាននៅក្នុងករណីបន្ទាន់មួយត្រូវបានចែងនៅក្នុង CSEA។ ភ្នាក់ងារនានារបស់រដ្ឋាភិបាលដែលទទួលបានព័ត៌មានគួរឲ្យសង្ស័យគឺត្រូវស្នើឲ្យរាយការណ៍ និងក្នុងរយៈពេល ៩០ថ្ងៃបន្ទាប់ពីចេញផ្សាយ បញ្ជូនទៅឲ្យស្មាក្តីទូទៅ (Attomey General) នៅថ្ងៃចេញផ្សាយផ្នែកនានាដែលមានការជាប់ពាក់ព័ន្ធ ផ្សព្វផ្សាយព័ត៌មាន និង

16 Computer Crime and Intellectual Property Section, SEC. 225. *Cyber Security Enhancement Act of 2002* (Washington, D.C.: Department of Justice, 2002), http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm.

ចំនួននៃអ្នកប្រើប្រាស់ដែលមានទំនាក់ទំនងនានាជាមួយព័ត៌មាននោះ និងចំនួននៃការទំនាក់ទំនងទាំងនោះ។

Good Faith Exception: CSEA ប្រកាស់យ៉ាងម៉ឺងម៉ាត់លើការលើកលែងការចោទប្រកាន់ដោយច្បាប់ព្រហ្មទណ្ឌ និងរដ្ឋប្បវេណីនៅក្នុងករណីមានការលួចស្តាប់នៅព័ត៌មានរបស់អ្នកប្រើប្រាស់ម្នាប់ដែលត្រូវបានស្នើរដោយម្ចាស់កុំព្យូទ័រ ឬអ្នកអនុវត្តដែលធ្វើការលើបញ្ហាសន្តិសុខនេះ។

Prohibition of Internet advertising of illegal devices: (**ការហាមឃាត់នៅការយោសនានៅឧបករណ៍ខុសច្បាប់លើប្រព័ន្ធអ៊ីនធើរណិត**) ECPA ហាមឃាត់ផ្សព្វផ្សាយផលិតកម្ម ការចែកចាយទ្រព្យសម្បត្តិ និងការផ្សព្វផ្សាយលើ Online តាមរយៈតេឡេក្រាម ដោយផ្តាល់មាត់ និងឧបករណ៍ដែលរារាំងការទំនាក់ទំនងនៃប្រព័ន្ធអេឡិចត្រូនិចនានា។ ឧបករណ៍ដែលប្រើប្រាស់សម្រាប់ការលួចស្តាប់តាមប្រព័ន្ធអេឡិចត្រូនិចប្រហែលជាត្រូវបានផ្សព្វផ្សាយ។ ទោះបីជាយ៉ាងណាក៏ដោយអ្នកយោសនាតម្រូវឲ្យដឹងពីព័ត៌មាននានាលើការយោសនា។

Reinforcing punishment for computer offences: (**ពង្រឹងការដាក់ទណ្ឌកម្មសម្រាប់ការប្រព្រឹត្តដ៏ថោកទាបណាមួយដល់កុំព្យូទ័រ**) នៅក្រោមច្បាប់ US Computer Froud and Abuse Act បានថ្លែងថារាល់ការចរាចរណ៍ចូលទៅលើប្រព័ន្ធកុំព្យូទ័រហើយបណ្តាលឲ្យមានការខូចខាតដោយច្បាប់ណាមួយអនុញ្ញាតឲ្យ គឺត្រូវបានគិតថាជាទង្វើខុសច្បាប់។ មុនថ្ងៃទី ៩ ខែវិច្ឆិកា បុគ្គលណាម្នាក់ត្រូវបានរកឃើញថាមានកំហុសឆ្គងណាមួយនៅក្នុងបទឧក្រិដ្ឋគឺត្រូវបានផ្តន្ទាទោសឲ្យជាប់ពន្ធនាគារតិចជាងប្រាំឆ្នាំសម្រាប់កំហុសលើកទី១ និងតិចជាង១០ឆ្នាំសម្រាប់កំហុងលើកទី២។ប៉ុន្តែបន្ទាប់ពីថ្ងៃទី ៩ ខែវិច្ឆិកា ការដាក់ទណ្ឌកម្មសម្រាប់ការប្រព្រឹត្តនេះត្រូវបានកែប្រែដោយបុគ្គណាដែលត្រូវបានរកឃើញនៅកំហុសលើកទី១ និងត្រូវផ្តន្ទាទោសតិចជាង១០ឆ្នាំ និងសម្រាប់កំហុងលើកទី២គឺមិនច្រើនជាង ២០ឆ្នាំ។ មានមាត្រាបន្ថែមនៅ CSEA ប្រកាសថាអ្នកប្រព្រឹត្តអាចត្រូវផ្តន្ទាទោសមិនច្រើនជាង២០ឆ្នាំប្រសិនបើអ្នកប្រព្រឹត្តនោះបង្ក ឬប៉ុនប៉ងធ្វើឲ្យគ្រោះថ្នាក់ធ្ងន់ធ្ងរលើរាងកាយ ប៉ុន្តែអ្នកទាំងនោះអាចត្រូវបានកាត់ទោសឲ្យជាប់ព័ន្ធនាគារពេញមួយជីវិត ប្រសិនបើពួកគេបង្ក ឬក៏ប៉ុនប៉ងបណ្តាលរហូតដល់មានការបាត់បង់ជីវិតនោះ។

Exemption of Assistants responsibility (**ការលើកលែងចំពោះការឆ្លើយតបនានាដែលជាជំនួយទៅដល់ការចាប់ខ្លួន**): ECPA លើកលែងការចោទប្រកាន់នៃបទឧក្រិដ្ឋលើអ្នកផ្តល់សេវាកម្មខាងទំនាក់ទំនងនានាដែលជួយនៅក្នុងការរារាំងដល់ការទំនាក់ទំនងខុសច្បាប់ ឬក៏អ្នកដែលផ្តល់ព័ត៌មានចំពោះអ្នកប្រព្រឹត្តខុសច្បាប់។

Federal Information Security Management Act (FISMA)[17] បានដាក់ចូលមាត្រា៣នៅក្នុង e-government Act នៅឆ្នាំ ២០០២។ ច្បាប់នេះការពារហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញជាក់លាក់ និងទាមទារឲ្យមានការខិតខំប្រឹងប្រែងដើម្បីការពារសន្តិសុខព័ត៌មានពីរាល់ជាតិសាសន៍ ភ្នាក់ងារសន្តិសុខជាតិ និងភ្នាក់ងារអនុវត្តន៍ច្បាប់នានា។ គោលបំណងដ៏សំខាន់នៃការគ្រប់គ្រងសន្តិសុខព័ត៌មានសហព័ន្ធគឺ ១.ផ្តល់នៅគម្រោងការណ៏ដ៏ទូលំទូលាយសម្រាប់ពង្រឹងការគ្រប់គ្រងលើសន្តិសុខព័ត៌មាននៅលើការអនុវត្តន៍ និងទ្រព្យសម្បត្តិនានា។ ២. ធ្វើការអភិវឌ្ឍន៍ការត្រួតពិនិត្យដ៏សមរម្យ និងថែរក្សាគម្រោងនានាសម្រាប់ការគាំពារព័ត៌មាន ប្រព័ន្ធព័ត៌មាន រួមទាំងផ្តល់នៅគ្រឿងយន្តដើម្បីពង្រឹងការគ្រប់គ្រងនៃកម្មវិធីនានារបស់សន្តិសុខព័ត៌មាន។

យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានរបស់សហគមន៍អ៊ឺរ៉ុប

នៅក្នុងគមនាគមន៍មួយដែលបានចុះនៅខែមេសា ឆ្នាំ២០០៦,[18] គណៈកម្មាធិការអ៊ឺរ៉ុបបានពិពណ៌នាស្តីពីយុទ្ធសាស្ត្ររបស់សហគមន៍អឺរ៉ុបថ្មីៗទៅលើសន្តិសុខព័ត៌មានដែលរួមមានវិធានការប្រកបដោយឯករាជភាពមួយចំនួនដែលជាប់ពាក់ព័ន្ធនឹងភាគហ៊ុនជាច្រើន។ វិធានការទាំងនោះរួមមានការបង្កើតនៅគម្រោងការនិយតករសម្រាប់ទំនាក់ទំនងលើប្រព័ន្ធអេឡិចត្រូនិចនានានៅក្នុងឆ្នាំ២០០២ ការនិយាយអំពី i២០១០ ដំបូងសម្រាប់ការបង្កើតសង្គមព័ត៌មានអឺរ៉ុប ការបង្កើតនៃភ្នាក់ងារសន្តិសុខព័ត៌មាននិងបណ្តាញរបស់អឺរ៉ុប (ENISA) នៅក្នុងឆ្នាំ២០០៤។ យោងទៅតាមគមនាគមន៍ វិធានការទាំងនោះជះត្រឡប់នៅដំណោះស្រាយបីយ៉ាងចំពោះបញ្ហានានាលើផ្នែកសន្តិសុខនៅក្នុងសង្គមព័ត៌មានរួមមានវិធានការផ្សេងៗនៃប្រភេទបណ្តាញ និងសន្តិសុខព័ត៌មាន (NIS) គម្រោងនិយតករសម្រាប់គមនាគមន៍លើប្រព័ន្ធអេឡិចត្រូនិចដែល

17 Office of Management and Budget, *Federal Information Security Management Act: 2004 Report to Congress* (Washington, D.C.: Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.

18 Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

រួមមានបញ្ហាឯកជនភាព និងសន្តិសុខទិន្នន័យទាំងឡាយ ព្រមទាំងការប្រយុទ្ធប្រឆាំងរលកសញ្ញាឧក្រិដ្ឋកម្ម។

គមនាគមន៍ធ្វើការកត់សម្គាល់លើការវាយប្រហារទៅលើប្រព័ន្ធព័ត៌មាន ការរីកដុះដាលនៅការប្រើប្រាស់ទូរស័ព្ទដៃ ការច្នៃប្រឌិតស្រោមដោយភាពវៃឆ្លាត (ambient intellegente) ការធ្វើឲ្យប្រើប្រាស់នៅកម្រិតយល់ដឹងរបស់អ្នកប្រើប្រាស់ដូចជាបញ្ហាសន្តិសុខសំខាន់ៗដែលគណៈកម្មាធិការអឺរ៉ុបមានបំណងធ្វើបទបង្ហាញតាមរយៈការសន្ទនា តាមរយៈភាពជាដៃគូ និងតាមរយៈការផ្តល់សិទ្ធិ។យុទ្ធសាស្ត្រទាំងនេះត្រូវបានពិពណ៌នានៅគមនាគមន៍ដូចខាងក្រោម:

ការសន្ទនា (dialogue)

គណៈកម្មាធិការស្នើឲ្យមានវិធានការជាបន្តបន្ទាប់ដែលត្រូវបានរៀបចំឡើងដើម្បីបង្កើតនៅការសន្ទនាជាលក្ខណៈចំហរ និងក្នុងនាមជាពហុភាគហ៊ុន:

- ដាក់នៅលំហាត់ដែលមានលក្ខណៈគំរូមយយសម្រាប់គោលការណ៏ច្បាប់ជាតិនានាដែលទាក់ទងជាមួយបណ្តាញ និងសន្តិសុខព័ត៌មានដើម្បីកំណត់ឲ្យបាននៅការអនុវត្តផ្សេងៗប្រកបដោយប្រសិទ្ធិភាពបំផុតដូច្នេះបន្ទាប់មកពួកគេអាចត្រូវបានចែកចាយទៅលើចំនុចសំខាន់ៗយ៉ាងទូលំទូលាយនៅគ្រប់ផ្នែកសហគមន៍អឺរ៉ុប។ ជាពិសេសលំហាត់នេះនឹងកំនត់នៅការអនុវត្តន៍ដ៏ល្អបំផុតចំពោហាការធ្វើឲ្យប្រសើរឡើងនៅចន្លោះសម្រាប់សហគ្រាសធុនតូចនិងមធ្យម រួមទាំងប្រជាពលរដ្ឋទូទៅនៃហានិភ័យនានា និងការបង្កបញ្ហាជាមួយបណ្តាញនិងសន្តិសុខព័ត៌មានរួមទាំង
- ពហុភាគហ៊ុនជជែកវែកញែកទៅលើរបៀបណាដែលគួរធ្វើឲ្យល្អបំផុតចំពោះការធ្វើអាជីវកម្មលើឧបករណ៍និយតករដែលមានស្រាប់នានា។ការពិភាក្សាវែកញែកនេះនិងត្រូវបានរៀបចំធ្វើឡើងនៅក្នុងបរិបទនៃសន្និសីទ និងសិក្ខាសាលាទាំងឡាយ។

>>

>>

ភាពជាដៃគូ (Partnership)

ការបង្កើតគោលការណ៍ច្បាប់ដែលប្រកបដោយប្រសិទ្ធិភាពស្នើឲ្យយល់ដឹងឲ្យបានច្បាស់នៅធម្ម ជាតិនៃបញ្ហានានាដែលត្រូវដោះស្រាយជាមួយ ក៏ដូចជាភាពដែលគួរឲ្យទុកចិត្តបាន ឲ្យទាន់ សភាពការចំពោះទិន្នន័យនៃសេដ្ឋកិច្ច និងស្ថិតិទិន្នន័យ។ ព្រោះហេតុនេះ គណៈកម្មាធិការនឹងស្នើ ENISA ធ្វើការ:

- កសាងនៅភាពជាដៃគូគួរឲ្យទុកចិត្តមួយជាមួយរដ្ឋជាសមាជិកនិងភាគហ៊ុននានាដើម្បីធ្វើការ អភិវឌ្ឍន៍ឡើងនៅគម្រោងដ៏សមរម្យមួយសម្រាប់ប្រើប្រាស់ក្នុងការប្រមូលទិន្នន័យ និង
- ត្រួតពិនិត្យនៅភាពអាចធ្វើទៅបាននៃការចែកចាយព័ត៌មានរបស់អឺរ៉ុប និងប្រព័ន្ធដ៏រំលាត ដើម្បីជួយសម្រួលនៅការឆ្លើយតបដ៏មានប្រសិទ្ធិភាពលើការគំរាមកំហែងផ្សេងៗ។ ប្រព័ន្ធ នេះនឹងចង្អុលបង្ហាញជាលក្ខណៈដោយប្រើលើសពីមួយភាសាចំពោះអឺរ៉ុបក្នុងការផ្តល់ព័ត៌ មានមុតស្រួចទៅការគំរាមកំហែង ហានិភ័យ និងប្រកបកដោយរំលាត។

ដូចគ្នានេះគណៈកម្មាធិការដឹងអញ្ជើញរដ្ឋជាសមាជិកនានា វិស័យឯកជន និងសហគមស្រាវជ្រាវ ធ្វើការរួមគ្នាបង្កើតនៅជាភាពដៃមួយដើម្បីធានាថាភាពអាចរកបាននៅទិន្នន័យដែលជាប់ទាក់ទង ទៅនឹងឧស្សាហកម្មសន្តិសុខ ICT។

ការផ្តល់សិទ្ធិ (Empowerment)

ការផ្តល់សិទ្ធិឲ្យភាគហ៊ុននានាគឺលើកតម្កើងចំណេះដឹងរបស់ពួកគេស្តីពីសេចក្តីត្រូវការ និងហានិ ភ័យនានាទាក់ទងនឹងសន្តិសុខ។សម្រាប់ហេតុផលនេះ សមាជិករដ្ឋទាំងឡាយត្រូវបានអញ្ជើញ ឲ្យចូលរួម:

- ជាសមាជិកដែលធ្វើការអនុវត្តន៍មុនគេនៅក្នុងការឆ្លើយលំហាត់គំរូដែលត្រូវបានឡើងស្តីពី គោលការណ៍ច្បាប់នានា។

>>

>>

- ជំរុញនៅក្នុងសហប្រតិបត្តិការជាមួយ ENISA ឃោសនាពីចំណេះដឹងលើអត្ថបទប្រយោជន៍នៃការទទួលយកនៅបច្ចេកវិទ្យាសន្តិសុខ ការអនុវត្តន៍ និងឥរិយាបទប្រកបដោយប្រសិទ្ធិភាព
- ជាកំណល់នៅការដាក់ចេញនៅសេវាកម្ម e-government ដើម្បីជំរុញឲ្យមានការប្រតិបត្តិខាងសន្តិសុខដ៏ល្អ។ និង
- លើកទឹកចិត្តឲ្យមានការអភិវឌ្ឍន៍ទៅលើកម្មវិធីបណ្តាញ និងសន្តិសុខព័ត៌មាននានាជាផ្នែកនៃកម្មវិធីសិក្សាជាន់ខ្ពស់

ភាគហ៊ុនផ្នែកឯកជនគឺត្រូវបានលើកទឹកចិត្តផងដែរនៅក្នុងការធ្វើសកម្មភាពមុនគេលើ:

- ការកំណត់ឲ្យបានច្បាស់លាស់ទៅលើការទទួលខុសត្រូវនានា សម្រាប់អ្នកផលិតកម្មវិធី Software និង ISPs ដែលទាក់ទងទៅនឹងការផ្តល់ឲ្យបានគ្រប់គ្រាន់ព្រំទាំងត្រួតត្រានៅរាល់កម្រិតនៃសន្តិសុខ
- ជំរុញនៅផ្នែកផ្សេងទៀត មានភាពស្មោះត្រង់ អន្តរប្រតិបត្តិ ភាពអាចប្រើការបាន និងការប្រកួតប្រជែងគឺជាចំនុចឆ្ពោះទៅមុខយ៉ាងសំខាន់សម្រាប់សន្តិសុខ និងលើកតម្កើងលើការពង្រីកបន្ថែមលើផលិតផល និងសេវាកម្មសន្តិសុខនានាដើម្បីប្រឆាំងនឹងការលួចបន្លំ ID និងការវាយប្រហារដទៃទៀតលើផលប្រយោជន៍ឯកជន
- ចែកចាយនៅការអនុវត្តន៍ដ៏ល្អនានានៃសន្តិសុខសម្រាប់អ្នកប្រតិបត្តិបណ្តាញ អ្នកផ្តល់សេវាកម្ម និង SMEs
- ជំរុញឲ្យមានកម្មវិធីហ្វឹកហ្វឺនផ្សេងៗនៅក្នុងវិស័យឯកជនដើម្បីផ្តល់ឲ្យនិយោជិកជាមួយចំណេះដឹង និងជំនាញនានាដ៏ចាំបាច់ក្នុងដំណើរលើការអនុវត្តន៍សន្តិសុខនានា
- ធ្វើការឆ្ពោះទៅរកគម្រោងការណ៍នៃការផ្តល់នូវិញ្ញាបណ្ណប័ត្រលើសន្តិសុខថាមានភាពពេញលេញសម្រាប់ផលិតផល ម្ចាស់កម្មសិទ្ធិ និងសេវាកម្មនានាដែលនឹងដូចទៅនឹងសេចក្តីចង់បានរបស់ EU

>>

>>

- ជាប់ទំនាក់ទំនងលើផ្នែកធានារ៉ាប់រងនៅក្នុងការអភិវឌ្ឍន៍នៅវិធីគ្រប់គ្រងហានិភ័យ និងយុទ្ធវិធីផ្សេងៗ

Source: Abridged from Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

សន្ធិបាតក្រុមប្រឹក្សានៃប្រទេសអឺរ៉ុបលើឧក្រិដ្ឋកម្ម

បន្ថែមលើការប្រកាសឲ្យប្រើដោយសហគមន៍អឺរ៉ុបនៅក្នុងឆ្នាំ ២០០១ សន្ធិបាតគណៈរដ្ឋមន្ត្រីអឺរ៉ុបទៅលើឧក្រិដ្ឋកម្ម (CECC) "បានលើកឡើង នៅសេចក្តីណែនាំនានាសម្រាប់រាស់រដ្ឋាភិបាលណាដែលកំពុងមានសេចក្តីប្រាថ្នាដើម្បីអភិវឌ្ឍន៍ច្បាប់ប្រឆាំងឧក្រិដ្ឋកម្ម" និង "ផ្តល់នៅគម្រោងសម្រាប់សហប្រតិបត្តិការណ៍ជាអន្តរជាតិនៅក្នុងការអភិវឌ្ឍន៍នេះ"។ ៣៩ប្រទេសនៅអឺរ៉ុបបានចុះហត្ថលេខាលើសន្ធិសញ្ញានេះដូចជាប្រទេសកាណាដា ជប៉ុន អាហ្រិកខាងត្បូង និងសហរដ្ឋអាមេរិក។ ការចុះហត្ថលេខាបានឲ្យ CECC ចូលជាធរមាននៅក្នុងខែកក្កដា ឆ្នាំ២០០៤ "គឺត្រឹមតែជាការបញ្ចូលនោសន្ធិសញ្ញាអន្តរជាតិទៅលើប្រធានបទនោះហើយត្រូវបានអនុវត្តចាប់ពីពេលនោះមក"។[19]

បណ្តាញសន្តិសុខព័ត៌មាន និងភ្នាក់ងារអឺរ៉ុប

ENISA ត្រូវបានបង្កើតឡើងដោយសភាអឺរ៉ុប និង គណៈរដ្ឋមន្ត្រីសហគមន៍អឺរ៉ុបនៅថ្ងៃទី២០ ខែមីនា ឆ្នាំ ២០០៤ "ដើម្បីជួយពង្រីកបណ្តាញនិងសន្តិសុខព័ត៌មាននៅក្នុងសហគមន៍អឺរ៉ុប និងជំរុញឲ្យមានការបញ្ចូលនៃវប្បធម៌បណ្តាញ និងសន្តិសុខព័ត៌មានសម្រាប់ផលប្រយោជន៍ប្រជាជន អ្នកប្រើប្រាស់ ការធ្វើជំនួញ ព្រមទាំងស្ថាប័នលើវិស័យសាធារណៈនានា"។

19 Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.

ក្រុមហ៊ុនអចិន្ត្រៃយ (PSG) ជាចក្ខុវិស័យសម្រាប់ ENISA[20] បានប្រកាសយ៉ាងច្បាស់នៅក្នុងខែឧសភា ឆ្នាំ ២០០៦ ថា ENISA ជាមជ្ឈមណ្ឌលមួយយ៉ាងល្អបំផុតនៅក្នុងបណ្តាញ និងសន្តិសុខព័ត៌មាន នៅក្នុងវេទិកាសម្រាប់ភាគហ៊ុន NIS នានា និងជាអ្នកដឹកនាំនៅចំណោះដឹងអំពីសន្តិសុខព័ត៌មានសម្រាប់ប្រជាជនសហគមន៍អឺរ៉ុប។ ចុងបញ្ចប់នេះ សកម្មភាពរយៈពេលវែងនានាដែលបានលើកឡើងដូចខាងក្រោមគឺសម្រាប់ ENISA នឹងត្រូវបានប្រកាសនៅក្នុងចក្ខុវិស័យ PSG (រូបភាពទី៦)

រូបភាពទី៦.សកម្មភាពរយៈពេលវែងសម្រាប់ ENISA

(Source: Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf)

20 Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

១. អាជ្ញាធរសន្តិសុខព័ត៌មាន និងបណ្តាញព្រៃជាតិរបស់រដ្ឋជាសមាជិកដើម្បីសម្របសម្រួល និងសហប្រតិបត្តិការ

សហប្រតិបត្តិការរវាងជាតិ និងជាតិគឺស្ថិតក្នុងកម្រិតតាបនៅពេលនេះ។ គេអាចធ្វើឲ្យមានភាពល្អច្រើនលើសហប្រតិបត្តិការដោយការលើកតម្កើងនៅការពង្រីកនៃផ្នែកទំនាក់ទំនងនិងសហប្រតិបត្តិការរវាងភ្នាក់ងារជាតិនានា ជាពិសេសទៅលើការចែករំលែកនៅការប្រតិបត្តិដ៏ល្អបំផុតពីភ្នាក់ងារសំខាន់ៗទៅឲ្យបុគ្គលិកទាំងឡាយណាដែលដំពុងតែទើបនឹងចាប់ផ្តើម។

២. សហប្រតិបត្តិការជាមួយវិទ្យាស្ថានស្រាវជ្រាវនានា

គោលបំណងរបស់ ENISA គួរតែត្រង់ទៅរកការស្រាវជ្រាវជាលក្ខណៈមូលដ្ឋាន និងការអភិវឌ្ឍន៍ខាងបច្ចេកវិទ្យាណាដែលត្រូវបានកំនត់យកដើម្បីផ្តោតទៅលើគុណប្រយោជន៍ដ៏អស្ចារ្យសម្រាប់តំបន់នានាក្នុងការគ្រប់គ្រងនៅហានិភ័យដ៏ពិតប្រាកដនៅក្នុងប្រព័ន្ធពិតៗ។ ENISA មិនផ្តល់ការគាំទ្រលើរបៀបវារៈស្រាវជ្រាវដោយខ្លួនវាផ្ទាល់ ប៉ុន្តែធ្វើការលើការរៀបចំដំណើរការ និងភាពជាអទិភាពដែលមានស្រាប់របស់កម្មវិធីដែលកំពុងមានវត្តមានរួចមកហើយផងដែរ។

៣. សហប្រតិបត្តិការជាមួយអ្នកលក់ Hardware និង Software

អ្នកលក់ Software និង Hardware គឺជាអ្នកប្រកួតប្រជែង និងវាអាចជាការពិបាកសម្រាប់ពួកគេចំពោះធ្វើនៅសេចក្តីយល់ព្រមយ៉ាងចំហរឲ្យមានការអនុវត្តរវាងគ្នាទៅវិញទៅមក។ ENISA អាចផ្តល់នៅគំនិតជាកណ្តាល និងបង្កើតនៅវេទិការពិភាក្សានានាដែលប្រកបដោយការយោគយល់ដើម្បីជាអ្នកថែរក្សាឲ្យកិរិយាប្រឆាំងតបតណាមួយស្ថិតនៅក្នុងសេចក្តីយោគយល់គ្នា។

ទស្សនៈវិស័យរយៈពេលវែងរបស់ ENISA គួរតែផ្តោតឲ្យបានច្រើនទៅលើការបង្កើតនៅបច្ចេកវិទ្យាព័ត៌មាន និងបណ្តាញដែលគួរឲ្យទុកចិត្តបានដែលជាការប្រឆាំងតទល់ទៅនឹង Worm និងបណ្តាញដទៃទៀតជំនួសទៅលើការពង្រីកនៅនិន្នាការសន្តិសុខផ្សេងៗទៀត។ កិច្ចការនេះអាចសម្រេចទៅបានដោយធ្វើការជំរុញនៃបច្ចេកវិទ្យានានាសម្រាប់ការអភិវឌ្ឍន៍ដ៏ត្រឹមត្រូវ រក្សាសន្តិសុខ រួមទាំងមាននៅ Software និងស្ថាបត្យករដែលគួរឲ្យពឹងពាក់បាន។

៤. ការចូលរួមនៃការបង្កើតតួខ្លួនគំរូនានា

ជាមួយការសំឡឹងមើលការផ្តើមគំនិតដែលមានភាពស្របគ្នា និងការផ្សព្វផ្សាយប្រកបដោយគុណតម្លៃដ៏អស្ចារ្យនោះ ENISA គួរតែតាមដាន និងឃ្លាំមើលអត្ថបទនានាដែលទាក់ទងជាមួយ NIS នៅក្នុងការបង្កើតតួគំរូនានាដោយរួមទាំងធ្វើការជាបន្តបន្ទាប់ទៅលើលិខិតបញ្ជាក់ពីសន្តិសុខដែលអាចរកបាន និងតួខ្លួនគំរូណាដែលប្រកបដោយភាពគួរឲ្យទុកចិត្តបាន។

៥. ចូលរួមនៅក្នុងដំណើរការនៃច្បាប់តាមរយៈការបញ្ចេះបញ្ចូល និងផ្តល់នៅទស្សនៈនានា

ENISA គួរតែធ្វើការជាអ្នកផ្តល់នៅការប្រឹក្សាដ៏គួរឲ្យទុកចិត្តដែលត្រូវធ្លាប់បានដឹងលឺពីមុនៗមក ចំពោះដំណើរការនៅសេចក្តីព្រាង សេចក្តីស្នើ និងបញ្ហាច្បាប់ផ្សេងៗទៀតដែលមានទំនាក់ទំនងនៅក្នុង NIS ។

៦. ធ្វើការជាមួយអ្នកប្រើប្រាស់តាមស្ថាប័ននានា

ជាញឹកញាប់អ្នកប្រើប្រាស់តាមស្ថាប័នផ្សេងៗគឺមិនមែនជាអ្នកតំណាងដ៏ល្អក្នុងការបង្កើតតួគំរូ និងត្រឹមត្រូវទៅច្បាប់ដូចជាអ្នកលក់។ ENISA អាចផ្តល់ឲ្យក្រុមអ្នកប្រើប្រាស់ទាំងនោះជាមួយការយល់ឲ្យច្បាស់ទៅក្នុងការងារដែលមានលក្ខណៈគំរូព្រមទាំងផ្តល់ឱកាសធ្វើជាម្ចាស់អំណាចលើការងារនោះផងដែរ។

៧. ធ្វើឲ្យដូចគ្នា និងជំរុញឲ្យមានការអនុវត្តន៍ដ៏ល្អបំផុតរវាងសមាជិករដ្ឋ និងការប្រើប្រាស់នៅក្នុងឧស្សាហកម្មអ្នកប្រើប្រាស់

ENISA មិនគួរគិតតែពីផលចំណេញខាងជំនួញ ប៉ុន្តែធ្វើឲ្យប្រសើរឡើងនៅទំនុកចិត្តនៅក្នុងការប្រើប្រាស់អ៊ីនធើរណិត និងប្រព័ន្ធផ្សព្វផ្សាយក្នុងលក្ខណៈឌីជីថលរបស់អ្នកប្រើប្រាស់ទាំងនោះ

៨. ធ្វើការសម្រាប់ដោះស្រាយជាលក្ខណៈបច្ចេកទេស និងនយោបាយដើម្បីឲ្យមានភាពដូចគ្នាលើការប្រើប្រាស់

ភាពខ្វះខាតភាពជឿជាក់លើប្រព័ន្ធអ៊ីនធើរណិត គឺជាការរាំងស្ទះដ៏សំខាន់មួយរបស់អ្នកប្រើប្រាស់នៅក្នុងទំហំដ៏ធំមួយក្នុងការងាកបែរទៅរកការប្រើប្រាស់ e-business ។ការត្រួតពិនិត្យយ៉ាងទៀងទាត់ទៅលើភាពជាម្ចាស់នៃតំបន់ណាមួយ ទៅលើអាស័យដ្ឋានរបស់អ៊ីមែល ឬក៏សេវាកម្មតាមប្រព័ន្ធ Online មួយចំនួននោះគឺជាជំហានដ៏ធំក្នុងការធ្វើឡើងវិញ និងបង្កើនឡើងវិញនៅសេចក្តីទុកចិត្តរបស់អ្នកប្រើប្រាស់ធម្មតាលើប្រព័ន្ធអ៊ីនធើរណិត។ ដំណោះស្រាយខាងបច្ចេកវិទ្យានៅក្នុងតំបន់នេះអាចត្រូវបានមើលឃើញតាមរយៈដំណើរការអនុវត្តន៍នានាដែលត្រូវបានដឹកនាំដោយឧស្សាហកម្ម ប៉ុន្តែ ENISA អាចធ្វើការឆ្ពោះទៅរកគោលការណ៍ច្បាប់នានាដែលមានលក្ខណៈយ៉ាងទូលំទូលាយរបស់ EU សម្រាប់បញ្ហាក់នៅភាពពិតនៃអង្គភាព Online ផ្សេងៗ។

៩. ធ្វើឲ្យមានតុល្យភាពរាំងនៅលើបញ្ហាសន្តិសុខ "ព័ត៌មាន" និង "បណ្តាញ"

ENISA គួរតែធ្វើការទំនាក់ទំនងជាមួយអ្នកផ្តល់សេវាកម្មខាងបណ្តាញ និងអ៊ីនធើរណិតដ៏ធំមួយ (ISPs/NSPs) ដើម្បីជួយពួកគេធ្វើឲ្យភាពស្របគ្នា ឲ្យមានការអនុវត្តន៍ដ៏ល្អនានាលើផល

ប្រយោជន៍នៃជំនួញព្រទាំងអ្នកប្រើប្រាស់ឆ្លងកាត់ប្រទេសអឺរ៉ុប។នេះគឺវាសំខាន់ពីព្រោះ ISPs/NSPs អាចដើរតួនាទីយ៉ាងសំខាន់នៅក្នុងការធ្វើឲ្យប្រសើរឡើងនៅសន្តិសុខទៅលើប្រព័ន្ធអ៊ីនធើរណិតក្នុងលក្ខណៈដ៏ធំមួយ។ សកម្មភាពសម្រាប់ការសម្របសម្រួល និងសហប្រតិបត្តិការដែល ISPs កំពុងតែធ្វើគឺមានភាពខ្វះខាតនៅក្នុងពេលឥឡូវ។

Source: Abridged from Paul Dorey and Simon Perry, ed. *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានៃសាធារណរដ្ឋកូរ៉េ

ទោះបីជាសាធារណរដ្ឋកូរ៉េជាប្រទេសមួយក្នុងចំណោមក្រុមនៃប្រទេសដែលមានបច្ចេកវិទ្យាជឿនលឿន ក៏ដោយប៉ុន្តែ ពេលថ្មីៗនេះប្រទេសមួយនេះបានស្រែកហៅនៅសេចក្តីត្រូវការការពារសន្តិសុខព័ត៌មានផងដែល។ នៅក្នុងឆ្នាំ ២០០៤ រដ្ឋាភិបាលកូរ៉េតាមរយៈក្រសួងគមនាគមន៍ព័ត៌មានា (MIC) បានលើកឡើងនៅរឿងស្តីពីផែនទីសម្រាប់សន្តិសុខព័ត៌មានរយៈពេលវែង និងមធ្យមក្នុងគោលបំណងដើម្បីបង្កើតទម្រង់សន្តិសុខមួយដើម្បីធានាឲ្យមានសុវត្ថិភាពខាងបរិស្ថាននៃការតភ្ជាប់សម្រាប់បណ្តាញផ្សព្វផ្សាយរួមបញ្ចូលគ្នាតែមួយ និងអភិវឌ្ឍន៍សន្តិសុខបច្ចេកវិទ្យាប្រឆាំងការលួចចម្លងខុសច្បាប់នៅជំនាន់បន្ទាប់ដោយប្រើប្រាស់ទូរស័ព្ទជាឧបករណ៍។ MIC ផងដែរបានណែនាំអំពីការប៉ាន់ប្រមាណលើផលប៉ះពាល់ឯកជន (PIA) និងបង្កើតនៅមធ្យមភាគមួយសម្រាប់លិខិតបញ្ជាក់ពីភាពពេញវិយដោយការប្រើប្រាស់នៅចំនួននៃការចុះឈ្មោះលើការតាំងទីលំនៅ។ បន្ថែមលើនេះទៀត សាធារណរដ្ឋកូរ៉េបានចុះហត្ថលេខាលើកិច្ចព្រមព្រៀងទីក្រុងសេអ៊ូល និងទីក្រុងមែលប៊ិន ដើម្បីបង្កើតនូវការសហការក្នុងចំណោមប្រទេសនានានៅតំបន់អាស៊ីប៉ាស៊ីហ្វិកប្រឆាំងទប់ទល់នឹង Spam តាមរយៈការប្រតិបត្តិនៃប្រព័ន្ធត្រួតពិនិត្យ Spam មួយ ការឆ្លើយតបលក្ខណៈបច្ចេកវិទ្យាផ្តល់ចំណេះដឹងការហ្វឹកហ្វឺនអ្នកប្រើប្រាស់ ការធ្វើឲ្យប្រសើរឡើងលើកិច្ចសហប្រតិបត្តិការនៃឯកជន និងរដ្ឋ ដោយការចែករំលែកនៅព័ត៌មានរវាងប្រទេសនានារួមទាំងការផ្លាស់ប្តូរនៅធនធានមនុស្ស។

គោលបំណងដ៏ពិតប្រាកដនៃផែនទីសន្តិសុខព័ត៌មានគឺ ១. ធានាសុវត្ថិភាពនៃរាល់ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ ២. ធានានៅភាពដែលអាចគួរឲ្យពឹងពាក់បាននៃឧបករណ៍ និងសេវាកម្មថ្មីៗរបស់ IT ។ ៣. ជំរុញភាពជាមូលដ្ឋាននៃសន្តិសុខព័ត៌មាននៅក្នុងសាធារណរដ្ឋកូរ៉េ។ ការអនុវត្តន៍នៃផែនទីមួយនេះតម្រូវឲ្យប្រើប្រាស់គម្រោងនៃប្រាប់បំណាច់ថវិការចំនួន ៤ឆ្នាំ ប្រមាណជាង ២៤៧.៨៩ រយកោដិដុល្លា (៤៣ រយកោដិដុល្លានៅក្នុងឆ្នាំ ២០០៥ ៥៥.៥ រយកោដិដុល្លានៅក្នុងឆ្នាំ ២០០៦ និង ៨០.១ រយកោដិដុល្លានៅក្នុងឆ្នាំ ២០០៨)។

ធានាសុវត្ថិភាពនៃរាល់ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ: យោងតាមផែនទីសន្តិសុខព័ត៌មាន សុវត្ថិភាពនៃរាល់ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញគឺត្រូវបានធានាកោយការអភិវឌ្ឍន៍នៅគម្រោងទម្រង់សន្តិសុខព័ត៌មានសម្រាប់សមាហរណកម្ម និងការចាក់ស្រេះឆ្លងកាត់បណ្តាញកុំព្យូទ័រផ្សេងៗ។ កសាងនូវការគ្រប់គ្រងសន្តិសុខ DNS ជំនាន់បន្ទាប់ និងការអភិវឌ្ឍន៍បណ្តាញមួយបែកចេញពីគ្រឿងយន្តដើម្បីការពារការបំផ្លាញនៅក្នុងបរិស្ថានបណ្តាញផ្សព្វផ្សាយរួមបញ្ចូលគ្នាតែមួយពីការរាលដាលទៅកាន់បណ្តាញឯកជន ឬត្រឡប់ច្រាសមកវិញ។

ធានានៅភាពដែលអាចគួរឲ្យពឹងពាក់បាននៃឧបករណ៍ និងសេវាកម្មថ្មីរបស់ IT អនុលោមតាមការប៉ាន់ប្រមាណលើផលប៉ះពាល់លើសន្តិសុខព័ត៌មានមួយដែលអាចស្ទង់មើលលើភាពងាយរងគ្រោះ និងការគំរាមកំហែងលក្ខណាពិត ជាលក្ខណៈបច្ចេកទេស និងជាលក្ខណៈរដ្ឋបាលនានានឹងត្រូវបានធ្វើការអភិឌ្ឍន៍ដើម្បីរារាំងប្រកបដោយប្រសិទ្ធិភាព ចំពោះការប្រព្រឹត្តល្មើសលើផ្នែកសន្តិសុខព័ត៌មាននៅក្នុងសេវាកម្មរបស់ IT។ នីតិវិធីលើការបញ្ជាក់សម្រាប់ការវាយតម្លៃនៅគ្រប់កម្រិតនៃសន្តិសុខព័ត៌មាននឹងត្រូវបានគេទុកនៅនឹងកន្លែង។ សម្រាប់សេវាកម្មនានារបស់ IT ជំនាន់បន្ទាប់ទៀត ការបញ្ជាប់លើប្រព័ន្ធដំណើរការនឹងត្រូវបានធ្វើការផ្លាស់ប្តូរដោយរួមបញ្ចូលទាំងការបញ្ជាក់ពីលើបុគ្គលអ្នករកស៊ី ច្បាប់ដែលអនុញ្ញាត បញ្ជីនៃការធ្វើជំនួញ និងអ្វីដែលទាក់ទងនឹងបញ្ហានេះផ្សេងទៀត។

ច្រើនជាងនេះទៀត គម្រោងសម្រាប់ការអភិវឌ្ឍន៍បច្ចេកវិទ្យាសន្តិសុខព័ត៌មានត្រូវបានបង្កើតចេញជារូបមន្តដែលរួមមាន ការអនុញ្ញាតនៅបច្ចេកវិទ្យាមានលក្ខណៈសមរម្យមួយសម្រាប់បណ្តាញប្រចាំផ្ទះនានា

អត្តសញ្ញាណចុងក្រោយរបស់បច្ចេកវិទ្យាសម្រាប់ការការពារនៅដំណើរការខុសច្បាប់ សន្តិសុខបច្ចេកវិទ្យាសម្រាប់រូបយន្តសេវាកម្មជំនាន់បន្ទាប់ និងសន្តិសុខបច្ចេកវិទ្យាសម្រាប់ព័តមានពីជំនាន់ក្រោយទៀត។

ការបង្កើតនៃភាពជាមូលដ្ឋានសន្តិសុខព័ត៌មាន: ផែនទីសន្តិសុខព័ត៌មានប្រទេសកូរ៉េមាននៅការផ្តល់ផ្សេងៗសម្រាប់ការធ្វើឲ្យប្រសើរឡើងលើភាបត្រឹមត្រូវតាមច្បាប់ ដើម្បីឲ្យត្រូវទៅតាមការស្នើរសុំនានានៃការផ្លាស់ប្តូរបរិស្ថានគមនាគមន៍ព័ត៌មាន និងការរៀបចំសម្រាប់ការគំរាមកំហែងដទៃៗទៀតក្នុងថ្ងៃអនាគត ។ ទីមួយ មជ្ឈមណ្ឌលសេវាកម្មឆ្លើយតបនឹងឧប្បទ្ទវហេតុលើប្រព័ន្ធអ៊ីនធើរណិតគួរត្រូវបានធ្វើឲ្យប្រសើរឡើងដោយការដោះស្រាយជាមួយទម្រង់ដ៏រំលាត និងមានភាពប្រសើរដ៏ខ្ពង់ខ្ពស់នៃព័ត៌មានក្នុងស្រុក និងបរទេសគួរត្រូវបានពង្រឹង និងធ្វើការគាំទ្រចំពោះប្រព័ន្ធទាំងនោះចំពោះសន្តិសុខព័ត៌មានដែលមានភាពទន់ខ្សោយ។ ទីពី២ បច្ចេកវិទ្យាផ្សេងៗដែលមានការទំនាក់ទំនងដូចជាច្បាប់ការពារឯកជនភាពគួរត្រូវបានអភិវឌ្ឍន៍ និងមជ្ឈមណ្ឌលសេវាកម្មឆ្លើយតបលើ Spam គួរត្រូវបានដំណើរការ។ ទីបី ច្បាប់ថ្មីៗស្តីអំពីសន្តិសុខព័ត៌មានគួរត្រូវបានធ្វើឲ្យប្រសើរឡើងដើម្បីជួបនៅសេចក្តីត្រូវការនៅគ្រប់ទីកន្លែង។ ដូច្នេះការយល់ដឹងពីសន្តិសុខព័ត៌មានគួរត្រូវបានជំរុញតាមរយៈយុទ្ធនាការ និងកម្មវិធីហ្វឹកហ្វឺនរបស់ជំនាញនានារបស់សន្តិសុខព័ត៌មាន។

យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានឧស្សាហកម្មជប៉ុន[21]

នៅក្នុងការរក្សាជាមួយនឹងគោងបំណងរបស់ខ្លួននៃការក្លាយជា "ជាតិដែលមានភាពរីកចំរើននៅសន្តិសុខព័ត៌មាន"[22] ប្រទេសជប៉ុនបានបញ្ចេញឲ្យឃើញច្បាស់នៅការបង្កើតឡើងក្នុងទម្រង់សម្ពិតនៃគោលបំណងនានា គោលគំនិតគ្រឹះ និងគម្រោងផ្សេងៗទៀតនៅក្នុងតំបន់នៃសន្តិសុខព័ត៌មាន។ក្រុមប្រឹក្សាច្បាប់សន្តិសុខព័ត៌មាន និងមជ្ឈមណ្ឌលសន្តិសុខព័ត៌មានជាតិ (NISC) គឺជាស្ថាប័នកណ្តាលក្នុងការត្រួតត្រាមើលទៅលើការងារដែលជាប់ពាក់ព័ន្ធរាស់សន្តិសុខព័ត៌មាននៅក្នុងប្រទេស។ នៅក្នុងតំបន់នៃការស្រាវជ្រាវទៅលើរលកសញ្ញាគំរាមកំហែងនានា មជ្ឈមណ្ឌលសំអាតរលកសញ្ញា (Cyber clean Center) ត្រូវបានបង្កើតឡើងដើម្បីវិភាគលើលក្ខណៈនៃ Bots និងបង្កើតជារូបមន្តយ៉ាងមានប្រសិទ្ធិភាពមួយព្រមទាំងយុទ្ធវិធីឆ្លើយតបយ៉ាងមានសុវត្ថិភាព។

21 This section is drawn from NISC, *Japanese Government's Efforts to Address Information Security Issue* (November 2007), http://www.nisc.go.jp/eng/.

22 Information Security Policy Council, *The First National Strategy on Information Security* (2 February 2006), 5. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

យុទ្ធសាស្ត្រសន្តិសុខព័ត៌មានរបស់ប្រទេសជប៉ុនត្រូវបានចែកចេញជាពីរផ្នែក: ១. យុទ្ធវិធីជាតិមួយលើសន្តិសុខព័ត៌មានដែលត្រូវបានដាក់ឲ្យប្រើប្រាស់ជាទូទៅ និង ២. ជប៉ុនមាំមួន YYYY។ យុទ្ធវិធីជាតិទីមួយលើសន្តិសុខព័ត៌មានរៀបចំនៅសេចក្តីត្រូវការសម្រាប់រាល់ "អង្គភាពទាំងអស់" នៅក្នុងសង្គម IT[23] ចូលរួមនៅក្នុងការបង្កើតបរិស្ថានមយយសម្រាប់ប្រើប្រាស់ប្រកបដោយសុវត្ថិភាពនៃ IT ។ យុទ្ធសាស្ត្ររៀបចំឲ្យស្ថាប័នទាំងអស់ "ថាពិតជាបានទទួលយក និងអនុវត្តន៍នៅគ្រប់វិធានដែលជាធាតុរបស់សង្គម IT"។ "ការអនុវត្តន៍នសអង្គភាពទាំងអស់" នេះគឺត្រូវបានបែងចែកជាបួន: ការគ្រប់គ្រងថ្នាក់តំបន់ និងកណ្តាល ហេដ្ឋារចនាសម្ព័ន្ធពិសេសៗ ជំនួញ និងឯកត្តជន។ ផ្នែកនិមួយៗត្រូវបានស្នើបង្កើតនៅតួនាទីផ្ទាល់ខ្លួន និតប្រតិបត្តិការពួកគេ (តារាងទី៤)

តារាងទី៤. តួនាទី និងគម្រោងនានាសម្រាប់ផ្នែកនិមួយៗផ្នែករលើយុទ្ធសាស្ត្រជាតិទីមួយនៃសន្តិសុសព័ត៌មាន

ផ្នែក	តួនាទី	គម្រោង
ការគ្រប់គ្រងថ្នាក់កណ្តាល និងតំបន់	ការឲ្យនៅ ការអនុវត្តន៍ដ៏ល្អបំផុតសម្រាប់វិធានការនានារបស់សន្តិសុខព័ត៌មាន	គំរូសម្រាប់វិធានការនានា
ហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ	ការធានាឲ្យមានការផ្គត់ផ្គង់ដោយស្ថិរភាពនៃសេវាកម្មផ្សេងៗរបស់ពួកគេដូចជាមូលដ្ឋានគ្រឹះនៃការរស់នៅក្នុងសង្គមរបស់ប្រជាជន និងសកម្មភាបនានានៃសេដ្ឋកិច្ច	គម្រោងសកម្មភាពហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ
ជំនួញផ្សេងៗ	ការអនុវត្តន៍នៅវរធានការផ្សេងៗរបស់សន្តិសុខព័ត៌មានដូច្នេះវាត្រូវបានមើលឃើញនៅតម្លៃយ៉ាងខ្ពស់ដោយទីផ្សារ។	វិធានការទាំងនេះត្រូវបានជំរុញឲ្យអនុវត្តន៍ដោយក្រសួង និងភ្នាក់ងារទាំងឡាយ

23 Ibid., 11.

ឯកត្តជនម្នាក់ៗ	លើលឡើងនៅការយល់ដឹងថាជាអ្នកដើរតួនាទីដ៏សំខាន់នៃសង្គម IT	វិធានការទាំងនេះត្រូវបានជំរុញឲ្យអនុវត្តន៍ដោយក្រសួង និងភ្នាក់ងារទាំងឡាយ

Source: NISC, *Japanese Government's Efforts to Address Information Security Issues* (November 2007), http://www.nisc.go.jp/eng/.

គោលការណ៍ច្បាប់នានាដែលត្រូវអនុវត្តន៍ពីយុទ្ធវិធីជាតិទីមួយនៅលើសន្តិសុខព័ត៌មានគឺត្រូវបានរៀបរាប់ដូចខាងក្រោម:ៗ

- ការជំរុញលើបច្ចេកវិទ្យាសន្តិសុខព័ត៌មាន - ការអភិវឌ្ឍន៍បច្ចេកវិទ្យានានាបានចង្អុលបង្ហាញចំពោះការគ្រប់គ្រងលើការប្រើប្រាស់ និងជំរុញឲ្យមានការអភិវឌ្ឍន៍បច្ចេកវិទ្យាដែលហៅថា "ការប្រកួតប្រជែងដ៏សំខាន់" នៃការបញ្ចូលនូវរបៀបថ្មីខាងបច្ចេកទេសដែលជាមូលដ្ឋានគ្រឹះជាមួយនឹងទស្សន:ដ៏វែងឆ្ងាយ។
- ការជំរុញការសហការ និងសហប្រតិបត្តិការជាអន្តរជាតិ - ជាការជួយឲ្យបង្កើតឡើងនៅទីតាំងជាអន្តរជាតិនានាសម្រាប់សន្តិសុខព័ត៌មាន និងការធានា៉ាប់រង និងការបង្កើតនៅវិភាគទានជាអន្តរជាតិផ្សេងដែលដឹកនាំដោយប្រទេសជប៉ុន។
- ការអភិវឌ្ឍន៍លើធនធានមនុស្ស - ការអភិវឌ្ឍន៍ធនធានប្រកបដោយជំនាញលើការអនុវត្តន៍ និងភាពប៉ិនប្រសប់ ព្រមទាំងសមត្ថភាពនៅកិច្ចការជាច្រើនផ្សេងទៀត រួមទាំងរបៀបនៃការរៀបចំប្រព័ន្ធប្រកបដោយគុណភាពសម្រាប់សន្តិសុខព័ត៌មាន និង
- ត្រួតពិនិត្យលើឧក្រិដ្ឋកម្ម និងវិធានការនសការបង្កា ការពារសម្រាប់សិទ្ធិ និងផលប្រយោជន៍ ពង្រឹងលើការត្រួតពិនិត្យឧក្រិដ្ឋកម្ម និងការអភិវឌ្ឍន៍មូលដ្ឋានស្របច្បាប់ដែលពាក់ព័ន្ធនានារួមទាំងការអភិវឌ្ឍន៍សម្រាប់ការធ្វើឲ្យប្រសើរឡើងនៃសន្តិសុខនៅក្នុងរលកសញ្ញាគ្មានព្រំដែន

សន្តិសុខប្រទេសជប៉ុន YYYY (Secure Japan YYYY) គឺជាគម្រោងប្រចាំឆ្នាំសម្រាប់សន្តិសុខព័ត៌មាន។ សន្តិសុខជប៉ុនឆ្នាំ ២០០៧ រួមមានការអនុវត្តន៍នៅវិធាកការសន្តិសុខព័ត៌មានចំនួន ១៥៩ និងទិសដៅនៃគម្រោងជាផ្លូវការជាអាទិភាពមានចំនួន ២៤ សម្រាប់ឆ្នាំ ២០០៧ ទាំងនេះបានសង្ខេបដូចខាងក្រោម:

- ការធ្វើឲ្យប្រសើរឡើងនៃវិធានការសន្តិសុខព័ត៌មាននានាសម្រាប់ភ្នាក់ងារគ្រប់គ្រង់ថ្នាក់កណ្តាល

- ផ្សព្វផ្សាយនៃវិធានការនានាសម្រាប់ផ្នែកខ្លះដែលកំពុងរត់តាមពីក្រោយនៅក្នុងការទទួលយកនៅវិធានការទាំងនោះដើម្បីធានានៅសន្តិសុខព័ត៌មាន ដូចជាផ្នែកសាធារណៈទូទៅ និង
- បង្កើនៅកិច្ចខំប្រឹងប្រែងឆ្ពោះទៅរកភាពរឹងប៉ឹងលើទម្រង់សន្តិសុខព័ត៌មាន

សំនួរត្រិះរិះ

១. តើវាខុសច្បាប់ដូចម្តេចរវាងសកម្មភាពសន្តិសុខព័ត៌មាននានានៅក្នុងប្រទេសរបស់អ្នកទៅនឹងអ្វីដែលបានពិពណ៌នាពីខាងលើ?

២. តើសកម្មភាពសន្តិសុខព័ត៌មានទាំងឡាយដែលត្រូវបានអនុវត្តន៍នៅក្នុងប្រទេសជាច្រើនដែលត្រូវបានពិពណ៌នានៅក្នុងចំនុចនេះ ហើយមិនត្រូវបាន ឬក៏ មិនត្រូវគ្នាទៅនឹងការអភិវឌ្ឍន៍ក្នុងប្រទេសរប់អ្នក? ប្រសិនបើដូច្នោះតើវិធានការមួយណា និងហេតុផលអ្វីដែលសកម្មភាពទាំនោះត្រូវបានអនុវត្តន៍ និងមានភាពត្រូវគ្នាក្នុងការអភិវឌ្ឍន៍ដោយប្រទេសរបស់អ្នក ។

៣.២ សកម្មភាពសន្តិសុខព័ត៌មានអន្តរជាតិ

សកម្មភាពសន្តិសុខព័ត៌មាននៃសហរដ្ឋអាមេរិក

នៅក្រោមការគាំទ្រដោយអង្គការសហប្រជាជាតិ **ជំនួបប្រជុំពិភពលោកស្តីអំពីសន្តិសុខព័ត៌មាន** (WSIS) [24]ធ្វើការប្រកាសមួយអំពីគោលគំនិតនានា និងគម្រោងនៃសកម្មភាពសម្រាប់ការធ្វើឲ្យរីកចម្រើនប្រកបដោយប្រសិទ្ធិភាពនៃសង្គមព័ត៌មាន និងការខិតទៅរក "ការបែងចែកព័ត៌មាន" ដែលត្រូវបានធ្វើឡើង។ គម្រោងនៃសកម្មភាពផ្តល់នៅអត្ថន័យទៅតាមសកម្មភាពដូចខាងក្រោម:

24 World Summit on the Information Society, "Basic Information: About WSIS," http://www.itu.int/wsis/basic/about.html.

- តួនាទីនៃរដ្ឋាភិបាល និងរាល់ម្ចាស់ភាគហ៊ុនជាអ្នកជំរុញនៅ ICT សម្រាប់ធ្វើការអភិវឌ្ឍន៍
- ហេដ្ឋារចនាសម្ព័ន្ធគមនាគមន៍ និងព័ត៌មានជាមូលដ្ឋានដ៏សំខាន់សម្រាប់ការរាប់បញ្ចូលទៅក្នុងសន្តិសុខព័ត៌មាន
- ការទទួលយកព័ត៌មាន និងចំណេះដឹង
- កសាងសមត្ថភាព
- កសាងនៅភាពជឿជាក់ និងសន្តិសុខនៅក្នុងការប្រើប្រាស់ ICTs
- [ការបង្កើត]នៅបរិស្ថានមួយ[ដែលអាចធ្វើទៅបាន]
- ICT អនុវត្តន៍នៅរាល់ភាពដូចគ្នានៃវប្បធម៌ ភាពផ្សេងគ្នាខាងភាសា និងព័ត៌មានក្នុងតំបន់
- ការផ្សព្វផ្សាយ
- ការលើកកំពស់សីលធម៌នៃសន្តិសុខព័ត៌មាន
- សហប្រតិបត្តិការនៃតំបន់ និអន្តរជាតិ[25]

វេទិការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធើរណិត (IGF)[26] គឺជាការគាំទ្រចំពោះស្ថាប័ននៃអង្គការសហប្រជាជាតិសម្រាប់បញ្ហាលើការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធើរណិតនានា។ វាត្រូវបានបង្កើតក្រោយពេលមានកិច្ចប្រជុំលើកទី២ នៃWSIS នៅប្រទេសទុយនេស៊ីដែលធ្វើការពិភាក្សាលើបញ្ហាមួយចំនួនដែលទាក់ទងទៅនឹងការគ្រប់គ្រងលើប្រព័ន្ធអ៊ីនធើរណិត។ វេទិការលើកទី២របស់ IGF ត្រូវបានធ្វើនៅក្នុងទីក្រុង Rio de Janeiro នៅថ្ងៃទី ១២ដល់ថ្ងៃទី ១៥ ខែវិច្ឆិកា ឆ្នាំ ២០០៧ ដោយបានផ្តោតលើបញ្ហាផ្សេងៗរបស់សន្តិសុខព័ត៌មាន ដូចជារលកសញ្ញាភេរវកម្ម រលកសញ្ញាឧក្រិដ្ឋកម្ម និងសុវត្ថិភាពនៃកុមារលើប្រព័ន្ធអ៊ីនធើរណិត។

សកម្មភាពសន្តិសុខព័ត៌មានឆានែ OECD[27]

អង្គភាពសម្រាប់ការអភិវឌ្ឍន៍ និងកិច្ចសហប្រតិបត្តិការនៃសេដ្ឋកិច្ច OECD គឺជាវេទិការតែមួយគត់ដែលរដ្ឋាភិបាលនៃទីផ្សារសេរីជាង ៣០ ធ្វើការរួមគ្នាជាមួយលើផ្នែកជំនួញ និងសង្គមស៊ីវិលសំដៅយកការពិភាក្សាស្តីពីសេដ្ឋកិច្ច សង្គម បរិស្ថាន និងការគ្រប់គ្រងក្នុងការប្រកួតប្រជែងទប់ទល់នឹងការបង្រួបបង្រួមសេដ្ឋកិច្ចទាំងពិភពលោក។ នៅក្នុង OECD ការងារជាក្រុមលើសន្តិសុខព័ត៌មាន និងឯកជន WPISP ធ្វើ

25 World Summit on the Information Society, *Plan of Action* (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/poa.html.
26 Internet Governance Forum, http://www.intgovforum.org.
27 This section is drawn from WPISP, "Working Party on Information Security and Privacy" (May 2007).

ការនៅក្រោមការឧបត្ថម្ភនានានៃគណៈកម្មធិការសម្រាប់គោលការណ៍ច្បាប់ព័ត៌មាន កុំព្យូទ័រ និងគមនាគមន៍ដើម្បីផ្តល់នៅការរីភាគនៅភាពប៉ះពាល់នៃ ICT ទៅលើសន្តិសុខព័ត៌មាន និងឯកជនព្រមទាំងអភិវឌ្ឍន៍នៅអនុសាសន៍នានារបស់គោលការណ៍ដោយផ្អែកលើការយល់ស្របរួមគ្នាចំពោះការគាំទ្រទៅលើសេចក្តីទុកចិត្តនៅក្នុងសេដ្ឋកិច្ចអ៊ីនធើរណិត។

WPISP ធ្វើការនៅលើសន្តិសុខព័ត៌មាន: នៅក្នុងឆ្នាំ ២០០២ OECD បានបង្កើតឡើង "នៅសេចក្តីណែនាំនានាសម្រាប់សន្តិសុខនៃបណ្តាញ និងប្រព័ន្ធព័ត៌មាន ការឆ្ពោះទៅរកវប្បធម៌នៃសន្តិសុខ"[28] ដើម្បីជំរុញ"សន្តិសុខនៅក្នុងការអភិវឌ្ឍន៍បណ្តាញ និងប្រព័ន្ធព័ត៌មានរួមទាំងការទទួលយកនៃមធ្យោបាយថ្មីៗចំពោះការគិត និងឥរិយាបថនៅពេលដេលមានការប្រើប្រាស់ព្រមទាំងអន្តរកម្មទៅវិញទៅមកនៅក្នុងបណ្តាញ និងប្រព័ន្ធព័ត៌មាន"។[29]

ចែករំលែកបទពិសោធន៍ និងការអនុវត្តន៍នានានៅក្នុងសន្តិសុខព័ត៌មាន វេទិកាជាសាកលមួយនិយាយអំពីសន្តិសុខបណ្តាញ និងប្រព័ន្ធព័ត៌មានត្រូវបានធ្វើឡើងនៅក្នុងឆ្នាំ២០០៣ និងសិក្ខាសាលារបស់ OECD-APEC ស្តីពីសន្តិសុខនៃបណ្តាញ និងប្រព័ន្ធព័ត៌មាននៅក្នុងឆ្នាំ ២០០៥។

WPISP ធ្វើការលើឯកជនភាព: "សេចក្តីណែនាំផ្សេងៗទៅលើការការពារឯកជនភាព និងការហូរចូលហួសព្រំដែននៃទិន្នន័យផ្ទាល់ខ្លួន" ដែលបានធ្វើឡើងនៅក្នុងឆ្នាំ ១៩៨០ ដែលតំណាងឲ្យការស្របគ្នាជាអន្តរជាតិមួយចំពោះការប្រើព័ត៌មានឯកជននៅលើវិស័យឯកជន និងសាធារណៈ។ "Online ជាលក្ខណៈឯកជនភាព: សេចក្តីណែនាំរបស់ OECD ទៅលើគោលការណ៍ច្បាប់ និងការអនុវត្តន៍" ដែលបានធ្វើឡើងនៅក្នុងឆ្នាំ២០០២ ដោយផ្តោតទៅលើបច្ចេកវិទ្យាផ្សេងៗក្នុងការផ្លាស់ប្តូរជាលក្ខណៈឯកជនភាព គោលការណ៍ច្បាប់ឯកជន Online ការប្រតិបត្តិ និងការកែតម្រូវរួមទាំងអ្វីៗផ្សេងៗទៀតដែលជាប់ទាក់ទងចំពោះ e-commerce។ នៅពេលបច្ចុប្បន្ន WPISP គឺកំពុងធ្វើការចំពោះកិច្ចសហប្រតិបត្តិការនៅការអនុវត្តន៍ច្បាប់ឯកជនភាព។

28 OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Paris: OECD, 2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
29 Ibid., 8.

ការងារដទៃទៀត: នៅក្នុងឆ្នាំ ១៩៩៨ OECD បានលើកឡើងនូវ "សេចក្តីណែនាំស្តីពីច្បាប់រហស្សលិខសាស្ត្រ" ដែលប្រព្រឹត្តឡើងដោយការប្រកាសនៃក្រសួងអូតាវ៉ា ទៅលើភាពត្រឹមត្រូវតាមច្បាប់សម្រាប់ការធ្វើពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិច។ "ការពិនិត្យមើលនៃភាពស្របច្បាប់ និងគម្រោងលើគោលការណ៍ច្បាប់នានាស្តីអំពីភាពត្រឹមត្រូវទៅតាមច្បាប់នៅសេវាដែលដើរនៅលើប្រព័ន្ធអេឡិចត្រូនិច និងការចុះហត្ថលេខាតាមប្រព័ន្ធអេឡិចត្រូនិចសម្រាប់ប្រទេសជាសមាជិករបស់ OECD" គឺត្រូវបានធ្វើនៅរវាងឆ្នាំ ២០០២ ទៅឆ្នាំ ២០០៣។ ហើយនៅក្នុងឆ្នាំ ២០០៥ "ការប្រើប្រាស់នៅភាពស្របច្បាប់ឆ្លងកាត់ព្រំដែននៃប្រទេសជាសមាជិករបស់ OECD" គឺត្រូវបានប្រកាសឲ្យប្រើ។

នៅក្នុងឆ្នាំ ២០០៤ "បច្ចេកវិទ្យាផ្សេងៗដែលផ្តែកលើលក្ខណៈជីវសាស្ត្រ" គឺត្រូវបានចងក្រងឡើង ហើយនៅក្នុងឆ្នាំ ២០០៥ ដោយក្រុមការងាររួមមួយដែលធ្វើកិច្ចការទៅលើ Spam នោះត្រូវបានបង្កើតឡើង។ ព្រមទាំងការងារបន្តបន្ទាប់ដទៃទៀតដែលទាក់ទងលើការរកឃើញរបៀបគ្រប់គ្រងតាមលក្ខណៈឌីជីថល Malware ការកំនត់អត្តសញ្ញាណនៃកម្រិតហ្វ្រេកង់របស់វិទ្យុដែលបានរីករាលដាល ឧបករណ៍ត្រួតពិនិត្យ និងបណ្តាញ ព្រមទាំងគម្រោងការសាមញ្ញៗសម្រាប់ការអនុវត្តន៍នៅសន្តិសុខព័ត៌មាន និងឯកជនភាព។

សកម្មភាពសន្តិសុខព័ត៌មានឆានារបស់ APEC[30]

សហប្រតិបត្តការសេដ្ឋកិច្ចអាស៊ីប៉ាស៊ីហ្វិក (APEC) គឺកំពុងប្រើប្រាស់នៅសកម្មភាពខាងសន្តិសុខព័ត៌មាននានានៅក្នុងតំបន់អាស៊ីប៉ាស៊ីហ្វិកតាមរយៈក្រុមការងារព័ត៌មាន និងទូរគមនាគមន៍ (TEL) ដែលរួមមាន៣ទិសដៅនៃក្រុមផ្សេងៗគ្នា: ក្រុមធ្វើការលើទិសដៅសេរីភាវូបនីយកម្ម ក្រុមធ្វើការលើទិសដៅអភិវឌ្ឍន៍ ICT និង ក្រុមការងារលើទិសដៅកម្មសិទ្ធិ និងសន្តិសុខ។

ជាពិសេសចាប់តាំងពីមានកិច្ចប្រជុំនៃក្រសួងលើកទី៦របស់ APEC ស្តីអំពីទូរគមនាគមន៍ និងឧស្សាហកម្មព័ត៌មានដែលបានធ្វើនៅក្នុងទីក្រុង Lima របស់ប្រទេសប៉េរ៉ូនៅខែ មិថុនា ឆ្នាំ ២០០៥ ក្រុមធ្វើការលើទិសដៅកម្មសិទ្ធិ និងសន្តិសុខបានបោះជំហានទៅរកការពិភាក្សានានាស្តីអំពីរលកសញ្ញាសន្តិសុខ និងរលកសញ្ញាឧក្រិដ្ឋកម្ម។ យុទ្ធសាស្ត្រសន្តិសុខដែលប្រើរលកសញ្ញារបស់ APEC ដែលរួមទាំងការពង្រឹងនៅភាព

30 This section is drawn from APEC, "Telecommunications and Information Working Group," http://www.apec.org/apec/apec_groups/som committee on economic/working groups/telecommunications and information.html

ទុកចិត្តរបស់អ្នកប្រើប្រាស់ទៅលើ e-commerce បានបម្រើឲ្យនៅការបង្រួបបង្រួមលើកិច្ចប្រឹងប្រែងផ្សេងៗនៃសេដ្ឋកិច្ចខុសៗគ្នា។ កិច្ចខិតខំប្រឹងប្រែងទាំងនោះរួមមានការអនុម័ត និងការអនុវត្តន៍ច្បាប់ស្តីពីរលកសញ្ញាសន្តិសុខដែលជាផ្នែកមួយជាប់ជាមួយការសម្រេចរបស់សភាទូទៅនៃអង្គការសហប្រជាជាតិ ៥៥/៦៣[31] សន្និបាតស្តីពីរលកសញ្ញាឧក្រិដ្ឋកម្ម។[32] ច្បាប់ដំបូងនៃរលកសញ្ញាឧក្រិដ្ឋកម្មរបស់ TEL និងគម្រោងកសាងនោសមត្ថភាពប្រកបដោយជាពមាំមួន និងធ្វើការគាំទ្ររាល់ស្ថាប័នណាដែលអនុវត្តន៍នៅច្បាប់ថ្មីៗទាំងនោះ។

APEC កំពុងធ្វើការរួមគ្នាដើម្បីអនុវត្តន៍ជាក្រុមទទួលខុសត្រូវបន្ទាន់លើកុំព្យូទ័រ (CERTs) ផងដែរ ដូចជាធ្វើការព្រមានមួយក្នុងកិច្ចការពារប្រព័ន្ធប្រឆាំងនឹងរលកសញ្ញាវាយប្រហារនានា។ សាធារណៈរដ្ឋកូរ៉េកំពុងផ្តលើនៅវគ្គហ្វឹកហ្វឺនចំពោះប្រទេសកំពុងអភិវឌ្ឍន៍ដែលជាសមាជិក និងសេចក្តីណែនាំទាំងឡាយសម្រាប់ការបង្កើត និងអនុវត្តន៍នៅ CERTs ដែលត្រូវបានគេអភិវឌ្ឍន៍ជាបន្តបន្ទាប់មក។

ការការពារនៃ SMEs និងអ្នកប្រើប្រាស់តាមផ្ទះពីរលកសញ្ញាវាយប្រហារ និងមេរោគផ្សេងៗគឺត្រូវបានគិតថាជាបញ្ហាចំបងរួមទាំងការបង្កើតនៅចំនួនឧកបរណ៍ដទៃទៀតដើម្បីប្រើនៅក្នុងការទប់ទល់នេះ។ព័ត៌មានគឺបាននឹងកំពុងផ្តល់ឲ្យទៅលើរបៀបប្រើប្រាស់អ៊ីនធើរណិតប្រដោយសន្តិសុខ និងទៅលើបញ្ហាសុវត្តិភាពមួយចំនួនដែលមានទំនាក់ទំនងទៅនឹងការប្រើប្រាស់បច្ចេកវិទ្យា Wireless និងការផ្លាស់ប្តូរអ៊ីមែល ដោយសុវត្តិភាព។

កាត់បន្ថយការប្រើប្រាស់ច្រឡំទៅលើព័ត៌មានរបស់ឧក្រិដ្ឋកម្មតាមរយៈព័ត៌មានដែលបានកំពុងចែកចាយធ្វើការអភិវឌ្ឍន៍ទៅវិធានការ និងជំនួញការផ្នែកច្បាប់ រួមទាំងវិធានការដទៃៗទៀតដើម្បីការពារកិច្ចការជំនួញ និងប្រជាជនជាច្រើនផ្សេងទៀតដែលទាំងអស់នេះនឹងបន្តក្លាយជាបញ្ហាចំបងរបស់ APECTEL ក្នុងដំណើរការលើវា។ ជាផ្នែកមួយនៃរបៀបវារៈរបស់វាស្តីពីបញ្ហាសន្តិសុខនានា APECTEL បានយល់ព្រមនៅក្នុងឆ្នាំ ២០០៧ ឲ្យមាន "ការណែនាំមួយស្តីពីវិធីសាស្ត្រខាងបច្ចេកវិទ្យា និងច្បាប់ប្រឆាំងតប នឹង Botnet" និងព្រមទាំងបានធ្វើសិក្ខាសាលាមួយស្តីពីរលកសញ្ញាសន្តិសុខណា និងហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានសំខាន់ៗ។

31 'Combating the criminal misuse of information', which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.

32 An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity. See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

សកម្មភាពសន្តិសុខព័ត៌មានរបស់ ITU[33]

ITU គឺជាភ្នាក់ងាររបស់ UN លើការដឹកនាំសម្រាប់ ICTs យោងតាមកិច្ចព្រមព្រៀងនៅក្នុង Geneva នៃប្រទេស Swithzerland។ ITU មាន ១៩១រដ្ឋជាសមាជិក និងច្រើនជាង ៧០០ ផ្នែកដែលជាសមាជិកនិងសមាគមន៍។

តួនាទីរបស់ ITU គឺជាការជួយគមនាគមន៍ពិភពលោកលើផ្នែកស្ទួលបី។ ផ្នែកគមនាគមន៍វិទ្យុ (ITU-R) គឺត្រូវបានផ្តោតទៅលើការគ្រប់គ្រងវិសាលគមប្រេកង់វិទ្យុជាអន្តរជាតិ និងប្រភពគោចររបស់ផ្កាយរណប។ ផ្នែកគំរូការូបនីយកម្ម (ITU-T) ផ្តោតទៅលើគំរូការូបនីយកម្មនៃបណ្តាញគមនាគមន៍ព័ត៌មាន និងសេវាកម្មផ្សេងៗ។ ផ្នែកធ្វើការអភិវឌ្ឍន៍ (ITU-D) គឺត្រូវបានបង្កើតឡើងដើម្បីជួយផ្សាយនៅភាពសមធម៌ ការទ្រទ្រង់ និងភាពល្មមគ្រប់គ្រាន់លើដំណើរការចំពោះ ICT ក្នុងអត្ថន័យមួយនៃការលើកទឹកចិត្តនៃការអភិវឌ្ឍន៍សេដ្ឋកិច្ច និងសង្គមឲ្យកាន់តែទូលំទូលាយ។ ITU រៀបចំនៅព្រឹត្តការណ៍នានារបស់ TELECOM និងគឺជាអ្នកដឹកនាំលើការរៀបចំភ្នាក់ងារនៃ WSIS ផងដែរ។

នៅក្នុងតំបន់រលកសញ្ញាសន្តិសុខ អ្នកផ្តើមគំនិតសំខាន់របស់ ITU រួមមាន WISS Action Line C.5 ITU Globle Cybersecurity Agenda និង ITU Cybersecurity Gateway។

សកម្មភាពសំខាន់ៗរបស់ WSIS Action Line C.5 គឺមាន:

- ការការពារហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានសំខាន់ៗ (CIIP)
- ជំរុញនៅវប្បធម៌ជាសាកលនៃរលកសញ្ញាឧក្រិដ្ឋកម្ម
- ការធ្វើឲ្យមានភាពចុះសម្រុងគ្នាលើវិធីសាស្ត្រស្របច្បាប់ជាតិនានា ការសហការណ៍ និងកិច្ចខំប្រឹងប្រែងប្រកបដោយភាពត្រឹមត្រូវជាអន្តរជាតិ។
- ការប្រឆាំងតបតនឹង Spam
- ធ្វើការអភិវឌ្ឍន៍លើការតាមដាន ការព្រមាន និងសមត្ថភាពឆ្លើយតបចំពោះឧប្បទ្ទវហេតុនានា
- ចែករំលែកព័ត៌មានពីយុទ្ធសាស្ត្រជាតិ ការអនុវត្តន៍ដ៏ល្អ និងសេចក្តីណែនាំផ្សេងៗ រួមទាំង
- ការការពារឯកជនភាព ទិន្នន័យ និងអ្នកប្រើប្រាស់

33 This section is drawn from ITU, "About ITU," http://www.itu.int/net/about/index.aspx.

ITU Global Cybersecurity Agenda (GCA) គឺជាគម្រោងរបស់ ITU មួយសម្រាប់កិច្ចសហប្រតិបត្តិការជាអន្តរជាតិដែលមានគោលបំណងចំពោះសេចក្តីស្នើសុំដំណោះស្រាយផ្សេងៗដើម្បីបន្ថែមនៅភាពគួរឲ្យទុកចិត្ត និងប្រកបដោយសន្តិសុខនៅក្នុងសង្គមព័ត៌មានមួយ។ GCA មានយុទ្ធសាស្ត្រគោល៥គឺ: គម្រោងស្របច្បាប់ វិធានការខាងបច្ចេកវិទ្យានានា គ្រោងអង្គភាពនានា ការកសាងសមត្ថភាព និងកិច្ចសហប្រតិបត្តិការជាអន្តរជាតិ។ យុទ្ធវិធីទាំងនេះគឺត្រូវបានពិនិត្យពិច័យតាមរយៈគោលដៅទាំងឡាយដូចខាងក្រោម៖

- អភិវឌ្ឍន៍នៅច្បាប់លើរលកសញ្ញាឧក្រិដ្ឋកម្មដែលដាក់ឲ្យអនុវត្តន៍ជាសាកល និងធ្វើនៅអន្តរប្រតិបត្តិជាមួយវិធានការច្បាប់នៃតំបន់ជាតិដែលមានស្រាប់រួចហើយ។
- បង្កើតនៅគ្រោងដែលត្រូវបានទទួលស្គាល់តាមតំបន់ និងថ្នាក់ជាតិរួមទាំងច្បាប់នានាស្តីអំពីរលកសញ្ញាឧក្រិដ្ឋកម្ម។
- បង្កើតនៅតំបន់សន្តិសុខអប្បបរមាដែលមានការទទួលយល់ព្រមជាសាកល និងគ្រោងការណ៍នានាប្រកបដោយការជឿជាក់សម្រាប់ដំណើរការ Software និងប្រព័ន្ធផ្សេងៗ។
- បង្កើតគម្រោងជាសាកលមួយសម្រាប់ការឃ្លាំមើល ការព្រមាន និងឆ្លើយតបចំពោះឧប្បទ្វវហេតុដើម្បីធានាចំពោះកិច្ចសហប្រតិបត្តឆ្លងកាត់តាមតំបន់និមួយៗ
- បង្កើត ទទួលស្គាល់ទៅតាមប្រភេទ កំនត់យកជាប្រព័ន្ធប្រើនៅឌីជីថលជាសាកល និងគ្រោងការណ៍នានាដែលទទួលស្គាល់ជាចាំបាច់ដើម្បីធានានៅការរៀបចំនៃភាពជឿជាក់លើឌីជីថលសម្រាប់បុគ្គលម្នាក់ៗធ្វើការឆ្លងកាត់តាមព្រំដែនភូមិសាស្ត្រ។
- អភិវឌ្ឍន៍យុទ្ធសាស្ត្រជាសាកលមួយជួយសម្រួលលើការកសាងសមត្ថភាពមនុស្ស និងវិទ្យាស្ថានក្នុងការបន្ថែមនៅចំណេះដឹង និងដឹងពីរបៀបធ្វើដំណើរការលើផ្នែកនិមួយៗ និងនៅគ្រប់តំបន់ដែលបានពិពណ៌នាមក
- ផ្តល់ដំបូន្មានចំពោះគម្រោងដ៏មានសក្តានុភាពណាមួយជាយុទ្ធសាស្ត្រពហុភាគហ៊ុនជាសាកលក្នុងកិច្ចសហប្រតិបត្តិការជាអន្តរជាតិ ការចរចារសហការណ៍នៅគ្រប់តំបន់ដែលបានពិពណ៌នាមក

ITU Cybersecurity Gateway មានគោលបំណងផ្តល់នៅភាពងាយស្រួលប្រើប្រាស់ទៅលើប្រភពព័ត៌មានដែលមានទំនាក់ទំនងទៅនឹងរលកសញ្ញាសន្តិសុខជាតិ និងអន្តរជាតិ។ វាគឺអាចរកបានដោយប្រជាជនរដ្ឋាភិបាល អ្នកជំនួញ និងអង្គការអន្តរជាតិនានា។ សេវាកម្មទាំងនោះបានផ្តល់ដោយ Gateway រួមមាន

ការចែករំលែកនៅព័ត៌មាន ការឃ្លាំមើល និងការព្រមាន ច្បាប់ និងភាពស្របច្បាប់ ឯកជនភាព និងការការពារ ព្រមទាំងគំរូរបស់ឧស្សាហកម្ម និងដំណោះស្រាយនានា។

ITU-D បានត្រួតមើលផងដែរទៅលើកម្មវិធីការងាររលកសញ្ញាសន្តិសុខរបស់ ITU ដែលត្រូវបង្កើតឡើងដើម្បីជួយដល់ប្រទេសជាច្រើនធ្វើការអភិវឌ្ឍន៍បច្ចេកវិទ្យាសម្រាប់ឲ្យមាននៅសន្តិសុខកម្រិតខ្ពស់របស់រលកសញ្ញាគ្មានដែនកំណត់។ វាផ្តល់នៅជំនួញទៅលើការងារដែលពាក់ព័ន្ធដូចការងារខាងក្រោមនេះ៖

- ការបង្កើតយុទ្ធសាស្ត្រជាតិ និងសមត្ថភាពនានាសម្រាប់រលកសញ្ញាសន្តិសុខ និង CIIP
- ការបង្កើតភាពសមរម្យសម្រាប់ច្បាប់រលកសញ្ញាឧក្រិដ្ឋកម្ម និងការអនុវត្តន៍នៅគ្រឿងយន្តនានា
- ការបង្កើតនៅការឃ្លាំមើល ការព្រមាន និងសមត្ថភាពឆ្លើយតបនឹងឧបទ្ទវហេតុ
- ប្រយុទ្ធប្រឆាំងនឹង Spam រួមទាំងការគំរាមកំហែងនានាដែលជាប់ពាក់ព័ន្ធ
- ធ្វើការដកស្រង់នៅចន្លោះប្រហោងរបស់គំរូការូបនីយកម្មដែលជាប់ពាក់ព័ន្ធនឹងសន្តិសុខរវាងប្រទេសជឿនលឿន និងប្រទេសកំពុងអភិវឌ្ឍន៍។
- ការបង្កើតបញ្ជីសៀវភៅ CIIP រលកសញ្ញាសន្តិសុខរបស់ ITU ភ្ជាប់ជាមួយតំបន់រក្សាទុកទិន្នន័យ (Database) និងនរណាជាអ្នកផ្សព្វផ្សាយ
- បង្កើតនៅអ្នកចង្អុលប្រាប់លើរលកសញ្ញាសន្តិសុខ
- ធ្វើការគាំទ្រលើកិច្ចសហប្រតិបត្តិការក្នុងតំបន់
- ចែករំលែកនៅព័ត៌មាន និងគាំទ្រលើ ITU Cybersecurity Gatesay
- ឈោងចាប់ និងជំរុញនៅរាល់សកម្មភាពនានាដែលជាប់ទាក់ទង

សកម្មភាពផ្សេងទៀតរបស់ ITU ដែលជាប់ទាក់ទងជាមួយរលកសញ្ញាសន្តិសុខគឺជាការបញ្ចូលរួមគ្នាជាមួយសកម្មភាព StopSpam Alliance.org ដូចជាសកម្មភាពកសាងសមត្ថភាពរបស់តំបន់ស្តីអំពីកិច្ចខំប្រឹងប្រែង និងច្បាប់រលកសញ្ញាឧក្រិដ្ឋកម្ម ការអភិវឌ្ឍន៍ និងការបែងចែកនៅឧបករណ៍សម្រាប់បន្ទូរនៅការវាយលុករបស់ Botnet[34] ការផ្សព្វផ្សាយនានាទាក់ទងនឹងរលកសញ្ញាឧក្រិដ្ឋកម្ម[35] រលកសញ្ញាសន្តិសុខឧបករណ៍សម្រាប់គំរូច្បាប់រលកសញ្ញាឧក្រិដ្ឋកម្មសម្រាប់ប្រទេសកំពុងអភិវឌ្ឍន៍ ឧបករណ៍ធ្វើការប៉ាន់ប្រមាណផ្ទាល់ខ្លួននៅរលកសញ្ញាសន្តិសុខជាតិ។[36]

34 Suresh Ramasubramanian and Robert Shaw, "ITU Botnet Mitigation Project: Background and Approach" (ITU presentation, September 2007), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.
35 ITU-D Applications and Cybersecurity Division, "Publications," ITU, http://www.itu.int/ITU-D/cyb/publications/.
36 ITU-D Applications and Cybersecurity Division, "ITU National Cybersecurity / CIIP Self-Assessment Tool," ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

សកម្មភាពសន្តិសុខព័ត៌មានឆានាឆៃ ISO/IEC

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន (ISMS) ដូចទៅនឹងឈ្មោះដែលបានគេហៅវាគឺជាប្រព័ន្ធមួយសម្រាប់គ្រប់គ្រងលើសន្តិសុខព័ត៌មាន។ វារួមមាននៅការដំណើរការ និងប្រព័ន្ធនានាដើម្បីធានារក្សានោភាពសម្ងាត់ សុច្ចរិកភាព និងភាពប្រើប្រាស់យ៉ាងមានប្រយោជន៍នៃទ្រព្យសម្បត្តិព័ត៌មានខណៈពេលហានិភ័យគឺស្ថិតនៅក្នុងកម្រិតអប្បបរមា។ លិខិតបញ្ជាក់ពីភាពត្រឹមត្រូវរបស់ ISMS គឺកំពុងមានប្រជាប្រិយយ៉ាងច្រើននៅជុំវិញពិភពលោក ហើយឆ្នាំ ២០០៥គឺជាចំនុចត្រឡប់ទៅក្នុងប្រវត្តិសាស្ត្រគំរូ ISMS ទទួលស្គាល់ជាលក្ខណៈអន្តរជាតិពីព្រោះការប្រកាសដាក់ឲ្យប្រើជាផ្លូវការនៅពីរគំរូ: IS ២០០៧ ប្រើសម្រាប់សេចក្តីស្នើសុំលើការបង្កើត ISMS និង IS ១៧៧៩៩:២០០០ ដែលត្រូវបានផ្សព្វផ្សាយប្រើប្រាស់ជា IS ១៧៩៩៩:២០០៥ សម្រាប់អនុវត្តន៍ទៅលើ ISMS។

គំរូ ISMS គឺត្រូវបានក្លាយជា BS ៧៧៩៩ ដែលនេះគឺដោយសារវាត្រូវបានធ្វើការអភិវឌ្ឍន៍ជាដំបូងដោយវិទ្យាស្ថានគំរូរបស់អង់គ្លេស (BSI) នៅក្នុងឆ្នាំ ១៩៩៥ ជាការអនុវត្តនៅលើកូដសម្រាប់ការគ្រប់គ្រងលើសន្តិសុខព័ត៌មាន។ នៅក្នុងឆ្នាំ ១៩៩៨ ដោយមានការស្នើសុំចំពោះមុខ វាត្រូវបានអភិវឌ្ឍន៍ដោយយោងតាមគំរូ “ការអនុវត្តនៅលើកូដសម្រាប់ការគ្រប់គ្រងលើសន្តិសុខព័ត៌មាន” ត្រូវបានផ្លាស់ប្តូរទៅជាផ្នែកទី១ ហើយសេចក្តីស្នើសុំនានាលើការបង្កើតឡើងនៅ ISMS ត្រូវបានចាត់ទុកជាផ្នែកទី២។ ផ្នែកទី១ ធ្វើការយ៉ាងជាក់លាក់លើការត្រួតពិនិត្យសម្រាប់ការគ្រប់គ្រងលើសន្តិសុខព័ត៌មាន ខណៈដែលផ្នែកទី២ ប្រើសម្រាប់ការស្នើសុំលើការបង្កើតនៅ ISMS ព្រមទាំងការពិពណ៌នាពីដំណើរការលើសន្តិសុខព័ត៌មាន (Plan-Do-Check-Act Cycle) ដើម្បីបន្តការធ្វើឲ្យប្រសើរឡើងនៃការគ្រប់គ្រងទៅលើហានិភ័យ។

ផ្នែកទី១ត្រូវបានបង្កើតជា IS 17799 ដោយ ISO/IEC JTC 1/SC27 WG1 នៅក្នុងឆ្នាំ ២០០០ បន្ទាប់ចាប់តាំងពី IS 17999 ត្រូវបានពិនិត្យឡើងវិញ (ជាមួយការប្រើប្រាស់នៅពាក្យបញ្ជាច្រើនជាង ២០០០) រួមទាំងការបន្ថែមបន្ថយនោះ ជំនាន់ក្រោយបំផុតត្រូវបានចុះក្នុងបញ្ជីចំពោះការទទួកស្គាល់ជាគំរូអន្តរជាតិនៅក្នុងខែវិច្ឆិកា ឆ្នាំ២០០៥។ IS 17799:2000 ផ្តល់នៅ ១២៦ ត្រួតពិនិត្យបញ្ជីនានាដែល ១០ត្រួតពិនិត្យលើការគ្រប់គ្រងតាមតំបន់នានា។ IS 17799 បានបន្ថែមបន្ថយទៀតនៅក្នុងឆ្នាំ ២០០៥ ដែលផ្តល់នៅ ១១

ត្រួតពិនិត្យជាលក្ខណៈរដ្ឋបាលលើតំបន់ត្រួតត្រាផ្សេងៗ (Domains) ព្រមទាំង ១៣៣ លើការត្រួតពិនិត្យដទៃៗទៀត។

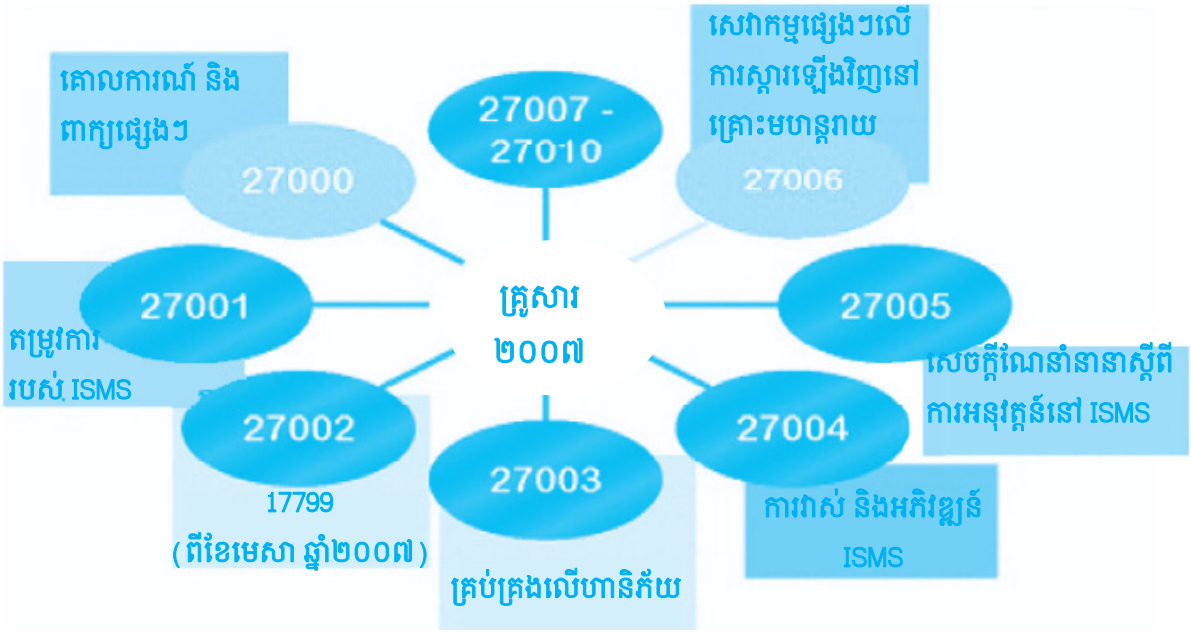
ផ្នែកទី២នៃ BS 7799 ត្រូវបានបង្កើតឡើងនៅក្នុងឆ្នាំ ១៩៩៩ ហើយត្រូវបានប្រើប្រាស់ជាគំរូសម្រាប់បញ្ជាក់ពី ISMS ។ វាត្រូវបានកែតម្រូវនៅក្នុងខែកញ្ញា ឆ្នាំ២០០២ ដើម្បីឲ្យត្រូវគ្នាជាមួយ ISO 9001 ISO 14001 និងចំណោមគំរូផ្សេងៗទៀត។ ISO បានទទួលយក BS 7799 ជាផ្នែកទី ២ នៅឆ្នាំ ២០០២ តាមរយៈការប្រើនៅយុទ្ធសាស្ត្រតាមផ្លូវដ៏លឿនបំផុតសម្រាប់ការថតចម្លងជាមួយជាមួយសេចក្តីស្នើសុំសម្រាប់ ISMS ជាគំរូអន្តរជាតិ និងបានចុះឈ្មោះវាជាគំរូអន្តរជាតិ ISO27001 ដោយគ្រាន់តែមានការកែលើវាបន្តិចបន្តួចក្នុងរយៈពេលដ៏ខ្លី។ ការផ្លាស់ប្តូរប្រកបដោយភាពលេខធ្លោនោះរួមមានការបន្ថែមនៅមាតិការអំពីប្រសិទ្ធិភាព និងការកែប្រែលើសេចក្តីបន្ថែម។

ពីព្រោះតែជាគំរូដ៏សំខាន់ពីរដែលមានទំនាក់ទំនងទៅនឹង ISMS ត្រូវបានកំនត់ជាគំរូតាមស្តង់ដារអន្តរជាតិនោះ គ្រួសារមួយនៃគំរូសន្តិសុខអន្តរជាតិនានាបានលេចចេញឡើងក្រោមគម្រោងស៊េរីលេខ ២៧០០០ ដែលគឺមានភាពដូចគ្នានេះទៅនឹងប្រព័ន្ធគ្រប់គ្រងផ្សេងៗទៀត (គុណភាពជំនួញ ៩០០០ ស៊េរី ការគ្រប់គ្រងបរិស្ថាន ១៤០០០ស៊េរី)។ IS 27001 ត្រូវបានកែប្រែពីជំនាន់របស់ IS 17799:2005 តំណាងឲ្យការស្នើសុំនានាសម្រាប់ការអនុវត្តន៍នៃ ISMS គំរូសម្រាប់ការគ្រប់គ្រងលើហានិភ័យសន្តិសុខព័ត៌មាន និងប្រព័ន្ធសន្តិសុខព័ត៌មានគ្រប់គ្រងលើរង្វាស់ និងការអភិវឌ្ឍន៍ ត្រូវបានអភិវឌ្ឍន៍ឡើងដោយ JTC1 SC27 គឺស្ថិតនៅក្នុងស៊េរី 27001។

រូបរាងលេខ៧: បង្ហាញពីគ្រួសារនៃគំរូដែលទាក់ទងនឹង ISMS។ សកម្មភាព ISMS នានាកំពុងផ្តល់សិទ្ធិនៅលើកម្លាំងអភិវឌ្ឍន៍ និងវាគឺត្រូបានរំពឹងថាគំរូ ISMS ឬសេចក្តីណែនាំផ្សេងៗដែលមានលក្ខណៈសមស្របនឹងឧស្សាហកម្មជាក់លាក់នានាគឺបាននឹងកំពុងអភិវឌ្ឍន៍ដោយផ្អែកលើភាពសាមញ្ញរបស់ ISMS សម្រាប់ប្រើប្រាស់លើប្រព័ន្ធទូទៅ។ ជាឧទាហរណ៍គឺកិច្ចខិតខំប្រឹងប្រែងនានាដើម្បីអភិវឌ្ឍន៍នៅសេចក្តីណែនាំរបស់ ISMS ជៈឥទ្ធិពលលើលក្ខណៈនៃឧស្សាហកម្មគមនាគមន៍។

រូបលេខ៧. គ្រួសារ ISO/IEC 27001

(ANSIL, Roadmap ISO/IEC 2700x, ISMS, Forum Eurosec 2007, http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf)



សំនួរត្រិះរិះ

តើសកម្មភាពសន្តិសុខព័ត៌មានដែលបានទទួលស្គាល់ដោយស្ថាប័នអន្តរជាតិបានដឹងឬកំពុងត្រូវបានអនុវត្តន៍នៅក្នុងប្រទេសរបស់អ្នក? តើពួកគេបានដឹងកំពុងត្រូវអនុវត្តន៍យ៉ាងដូចម្តេច?

សកម្មភាពខ្លួនឯង

១. តើអ្វីគឺជាភាពប្រហាក់ប្រហែលគ្នាក្នុងចំណោមសកម្មភាពសន្តិសុខព័ត៌មានកំពុងត្រូវបានអនុវត្តន៍ដោយប្រទេសជាច្រើនដែលបានពិពណ៌នានៅក្នុងចំនុចនេះ? អ្វីគឺជាភាពផ្សេងគ្នារបស់ពួកគេ?

២. អ្វីគឺជាភាពសំខាន់ចំបងៗរបស់សន្តិសុខព័ត៌មាននៃស្ថាប័នអន្តរជាតិនានាដែលបានរៀបរាប់នៅក្នុងចំនុចនេះ?

៤. វិធីវិទ្យាសន្តិសុខព័ត៌មាន

នៅក្រង់ចំនុចនេះមានគោលបំណងពិពណ៌នាវិធីវិទ្យាសន្តិសុខព័ត៌មានដែលជាលក្ខណៈបច្ចេកទេស លក្ខណៈពិត និងតាមលក្ខណៈរដ្ឋបាល

៤.១ វិធីវិទ្យាសន្តិសុខព័ត៌មាន

វិធីវិទ្យាសន្តិសុខព័ត៌មានមានគោលបំណងបង្រួមនៅការបំផ្លាញឲ្យនៅតូចនិងធ្វើការថែរក្សានិរន្តន៍ភាពលើការគិតគូរអំពីភាពគំរាមកំហែង និងភាពងាយរងគ្រោះដែលអាចកើតឡើងចំពោះទ្រព្យសម្បត្តិព័ត៌មាន។ ដើម្បីធានានិរន្តន៍ភាពខាងជំនួញ វិធីវិទ្យាសន្តិសុខព័ត៌មានខាងក្នុង។ នេះជាប់ពាក់ព័ន្ធទៅលើដំណើរការនៃវិធីសាស្ត្រសម្រាប់ការប៉ាន់ប្រើមើរមើលលើហានិភ័យ និងការត្រួតពិនិត្យនានា។ ជាពិសេសអ្វីដែលជាតម្រូវការគឺគម្រោងការដ៏ល្អមួយដែលគ្របដណ្តប់លើទ្រង់ទ្រាយជាលក្ខណៈបច្ចេកទេស លក្ខណៈពិត និងលក្ខណៈរដ្ឋបាលនៃសន្តិសុខព័ត៌មាន។

ទ្រង់ទ្រាយតាមលក្ខណៈរដ្ឋបាល

គឺមាននៅ ISMS ជាច្រើនដែលផ្តោតទៅលើទ្រង់ទ្រាយតាមលក្ខណៈរដ្ឋបាល។ ISO/IEC 27001 គឺមួយក្នុងចំណោមគំរូដែលត្រូវបានគេប្រើប្រាស់យ៉ាងសាមញ្ញបំផុតក្នុងទ្រង់ទ្រាយមួយនេះ។

ISO/IEC 27001 ជាគំរូ ISMS អន្តរជាតិ គឺសំដៅទៅលើ BS 7799 ដែលត្រូវបានបង្កើតឡើងដោយ BSI ។ BS7799 គឺការអនុវត្តន៍ និងការគ្រប់គ្រងលើ ISMS តម្រូវឲ្យមានចំពោះជាគំរូដ៏សាមញ្ញដែលត្រូវបានប្រើប្រាស់ចំពោះគំរូសន្តិសុខនានានៃស្ថាប័នផ្សេងៗរួមទាំងការគ្រប់គ្រងលើសន្តិសុខទាំងនោះប្រកបដោយប្រសិទ្ធិភាពផងដែរ។ ផ្នែកទី១ នៃ BS7799 ពិពណ៌នាពីតម្រូវការលើសកម្មភាពសន្តិសុខនានាដោយត្រូវបានផ្តែកទៅរកការឲ្យមាននៅការអនុវត្តន៍ដ៏ល្អបំផុតនៃសកម្មភាពសន្តិសុខទាំងនោះនៅក្នុងស្ថាប័ននានា ។ ផ្នែកទី២ ដែលបានក្លាយជាការពិពណ៌នាតំណាងឲ្យ ISO/IEC27001 ស្នើឲ្យមានតម្រូវការអប្បបរមា

សម្រាប់ការប្រតិបត្តិ និងការប៉ាន់ប្រមាណរបស់ ISMS នៃសន្តិសុខព័ត៌មាន។ សកម្មភាពសន្តិសុខព័ត៌មាននានានៅក្នុង ISO/IEC27001 មាន១៣៣នៃការត្រួតពិនិត្យ និងលើដែនត្រួតត្រា (តារាងលេខ៥)

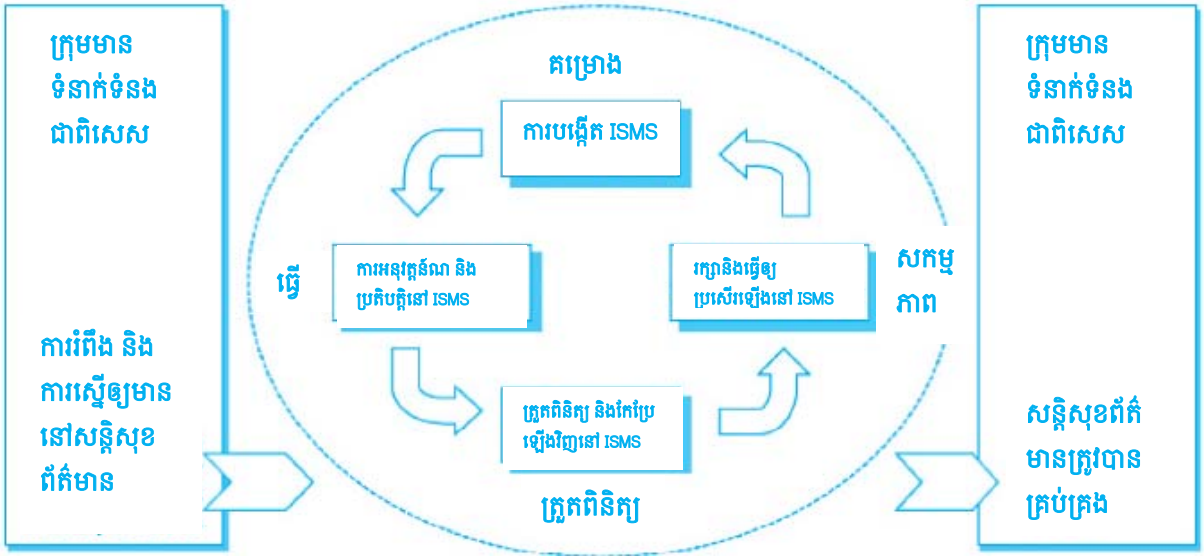
តារាងលេខ៥. ការត្រួតពិនិត្យនៅក្នុង ISO/IEC27001

ដែនត្រួតត្រា	ការពិពណ៌នា
A5	គោលការណ៍ច្បាប់សន្តិសុខ
A6	ស្ថាប័ន អង្គភាពនៃសន្តិសុខព័ត៌មាន
A7	ការគ្រប់គ្រងលើទ្រព្យសម្បត្តិព័ត៌មាន
A8	សន្តិសុខធនធានមនុស្ស
A9	សន្តិសុខបរិស្ថាន និងលក្ខណៈពិត
A10	ការគ្រប់គ្រងលើការអនុវត្តន៍ និងការទំនាក់ទំនងនានា
A11	ដំណើរការលើការត្រួតពិនិត្យ
A12	ការទទួលយកនៅប្រព័ន្ធព័ត៌មាន ការអភិវឌ្ឍន៍ថែរក្សា
A13	ការគ្រប់គ្រងលើឧប្បទ្ទវហេតុសន្តិសុខព័ត៌មាន
A14	ការគ្រប់គ្រងលើសុច្ចរិតភាពនៃជំនួញ
A15	ការគោរពតាម

ISO/IEC27001 ទទួលយកនៅគំរូដំណើរការរបស់ Plan_Do_Check_Act ដែលត្រូវបានប្រើប្រាស់ដើម្បីធ្វើឲ្យមានរចនាសម្ព័ន្ធទៅរាល់ដំណើរការរបស់ ISMS។ នៅក្នុង ISO/IEC27001 វាស់ភ័ស្តុតាងនៃដំណើរការលើការប៉ាន់ប្រមាណមើលរបស់ ISMS គួរត្រូវបានធ្វើជាឯកសារ។ រាល់លិខិតបញ្ជាក់គួរត្រូវបានធ្វើសារនកម្មជាលក្ខណៈខាងក្រៅក្នុងរយៈពេលប្រាំមួយខែម្តង និងរាល់ដំណើរការទាំងអស់នេះគួរត្រូវបានធ្វើសារឡើងវិញម្តងទៀតបន្ទាប់ពីរយៈពេល៣ឆ្នាំដើម្បីគ្រប់គ្រងប្រកបដោយនិរន្តន៍ភាពលើ ISMS។

រូបលេខ៨. គំរូដំណើរការ Plan_Do_Check_Act **ត្រូវបានប្រើលើដំណើរការនានារបស់** ISMS

(Source: ISO/IEC JTC 1/SC 27)



ការត្រួតពិនិត្យលើសន្តិសុខគួរត្រូវបានគ្រោងដោយគិតពិចារណាលលើសេចក្តីស្នើឲ្យមាននៅសន្តិសុខ។ ធនធានមនុស្ស រួមមានអ្នកផ្គត់ផ្គង់ អ្នកចុះកុងត្រា អ្នកប្រើប្រាស់ និងអ្នកដែលមិនមែនជាអ្នកជំនាញនានាគួរចូលរួមក្នុងសកម្មភាពទាំងនេះ។ ការបង្កើតឡើងនៅសេចក្តីស្នើសុំឲ្យមានសន្តិសុខគឺត្រូវបានផ្អែកលើកត្តាបីដូចខាងក្រោម៖

- ការប៉ាន់ប្រមាណមើលលើឧប្បទ្ទវហេតុ
- ការស្នើសុំដែលត្រឹមត្រូវតាមច្បាប់ និងការប្រកាសរបស់កិច្ចសន្យា
- ដំណើរការព័ត៌មានសម្រាប់ការអនុវត្តន៍តាមស្ថាប័ន (អង្គភាព) មួយ

ការវិភាគលើចន្លោះប្រហោង (Gap analysis) សំដៅទៅលើដំណើរការនៃការវាស់ស្ទង់លើកម្រិតសន្តិសុខព័ត៌មានក្នុងពេលថ្មីៗនេះ និងការបង្កើតនៅទិសដៅអនាគតនៃសន្តិសុខព័ត៌មាន។ លទ្ធផលនៃការវិភាគលើចន្លោះប្រហោងគឺបានមកពីសំនួររបស់ម្ចាស់ទ្រព្យសម្បត្តិព័ត៌មានដែលបានសួរទៅចំនុចត្រួតត្រាទាំង ១៣៣ និងតំបន់គ្រប់គ្រងទាំង ១១។ម្តងទៀតសម្រាប់តំបន់ដែលមានភាពខ្វះខាតគឺត្រូវបានកំនត់តាមរយៈការវិភាគលើភាពចន្លោះប្រហោងនេះ ហើយការត្រួតពិនិត្យដ៏សមរម្យនានាលើតំបន់មួយអាចត្រូវបានបង្កើតឡើង។

ការប៉ាន់ប្រមាណមើលហានិភ័យៈ គឺត្រូវបានបែងចែកចូលទៅក្នុងការប៉ាន់ប្រមាណមើលលើតម្លៃនៃទ្រព្យសម្បត្តិព័ត៌មាន និងការប៉ាន់ប្រមាណមើលនៃភាពងាយរងគ្រោះ និងការគំរាមកំហែងនានា។ ការប៉ាន់ប្រមាណលើតម្លៃទ្រព្យសម្បត្តិគឺជាការវាយតម្លៃលើបរិមាណនៃទ្រព្យសម្បត្តិព័ត៌មាន។ ការប៉ាន់ប្រមាណលើការគំរាមកំហែងជាប់ពាក់ពាន់និងអត្រាការគំរាមកំហែងនានាទៅលើភាពសម្ងាត់ និរន្តន៍ភាព និងភាពអាចរកបាននៃព័ត៌មាន។ ឧទាហរណ៍ខាងក្រោមបង្ហាញពីការគណនាដែលមានការជាប់ពាក់ព័ន្ធទៅលើការប៉ាន់ប្រមាណល់ហានិភ័យ។

ឈ្មោះទ្រព្យសម្បត្តិ	តម្លៃ ទ្រព្យសម្បត្តិ	ភាពគំរាមកំហែង			ភាពងាយរងគ្រោះ			ហានិភ័យ		
		C	I	A	C	I	A	C	I	A
ឈ្មោះទ្រព្យសម្បត្តិ #1	2	3	3	1	3	1	1	8	6	5

- តម្លៃទ្រព្យសម្បត្តិ + ភាពគម្រាមគំហែង + ភាពងាយរងគ្រោះ = ហានិភ័យ
- ភាពរក្សាការសម្ងាត់ៈ តម្លៃទ្រព្យសម្បត្តិ(២) + ការគំរាមកំហែង(៣) + ភាពងាយរងគ្រោះ(៣)= ហានិភ័យ(៨)
- និរន្តន៍ភាពៈ តម្លៃទ្រព្យសម្បត្តិ(២) + ការគំរាមកំហែង(៣) + ភាពងាយរងគ្រោះ(១)= ហានិភ័យ(៦)
- ភាពដែលអាចរកបានៈ តម្លៃទ្រព្យសម្បត្តិ(២) + ការគំរាមកំហែង(១) + ភាពងាយរងគ្រោះ(១)= ហានិភ័យ(៥)

ដំណើរការនៃការត្រួតពិនិត្យនានាៈ តម្លៃនសហានិភ័យនិមួយៗនឹងមានភាពផ្សេងៗពីគ្នាអាស្រ័យទៅលើលទ្ធផលពីការប៉ាន់ប្រមាណលើហានិភ័យ . ទាមទារឲ្យមានការសម្រេចមួយចំនួនដើម្បីប្រើប្រាស់លើការត្រួតពិនិត្យដ៏សមរម្យចំពោះទ្រព្យសម្បត្តិដែលត្រូវបានកំណត់តម្លៃផ្សេងៗពីគ្នា។ ហានិភ័យទាំងនោះគួរត្រូវបានចែកចេញជាហានិភ័យដែលអាចទទួលយកបាន និងមិនអាចទទួលយកបានយោងទៅតាមលក្ខខណ្ឌរបស់<<កម្រិតនៃការធានារ៉ាប់រង>>។ ទ្រព្យសម្បត្តិព័ត៌មានដែលមានហានិភ័យប៉ុន្តែហានិភ័យនោះអាចទទួលយកបានដោយមិនមានបង្កគ្រោះថ្នាក់ធំដុំនោះទេ អាចតម្រូវឲ្យមានការត្រួតពិនិត្យលើវា។ ការត្រួតពិនិត្យនោះត្រូវបានធ្វើដោយផ្អែកលើការត្រួតពិនិត្យនានារបស់ ISO/IEC ប៉ុន្តែវារឹតតែមានប្រសិទ្ធិភាពទៀតប្រសិនបើការត្រួតពិនិត្យនោះត្រូវបានធ្វើឡើងដោយផ្អែកលើភាពពិតរបស់ស្ថាប័ន។

ប្រទេសនិមួយៗមានលិខិតបញ្ជាក់លើការប្រើប្រាស់ ISO/IEC27001 ។តារាងលេខ៦រាយនៅចំនួនលិខិតបញ្ជាក់នៃប្រទេសទាំងនោះ៖

តារាងលេខ៦.ចំនួននៃលិខិតបញ្ជាក់សម្រាប់ប្រទេសមួយ

ជប៉ុន	2863	ញ៉ូដឺឡែន	11	ប៉ុលហ្គារី	2
ឥណ្ឌា	433	សិង្ហបូរី	11	កាណាដា	2
អង់គ្លេស	368	ហ្វីលីពីន	10	ជីប្រាដាល់	2
តៃវ៉ាន់	202	សោឌីអារ៉ាប់	10	អាយស្វីអូហ្វមេន	2
ចិន	174	ប៉ាគីស្ថាន	10	មួរូកូ	2
អាល្លឺម៉ង់	108	សហព័ន្ធរុស្សី	10	អូម៉ាង	2
សហរដ្ឋអាមេរិក	82	បារាំង	10	កាតា	2
ហុងគ្រី	74	កូឡុំប៊ី	9	យេមែន	2
សាធារណរដ្ឋកូរ៉េ	71	សូវេនី	7	អាលមានី	1
សាធារណរដ្ឋក្រិច	66	ស្វីតដែន	7	បង់ក្លាដេស	1
អ៊ីតាលី	54	ស្លូវ៉ាគី	7	ប៊ែលសិក	1
ហុងកុង	38	ក្រូអាតទី	6	អេហ្ស៊ីប	1
ប៉ូឡូញ	36	ក្រិច	5	អ៊ីរ៉ង់	1
អូស្ត្រាលី	28	អាហ្វ្រិកខាងត្បូង	5	កាស្សាស្ថាន	1
ទួរគី	26	បារ៉ែន	5	លីបាន់	1
អ៊ីឡង់	26	ឥណ្ឌូនេស៊ី	4	លីធូនី	1
ម៉ាឡេស៊ី	26	គុយវ៉ែត	4	ឡុចហ្សំបួរ	1
អេស្ប៉ាញ	26	ន័រវែស	4	ម៉ាសេដូនី	1
ប្រេស៊ីល	20	ស្រីលង្កា	4	មូដូវ៉ា	1
មិចស៊ិចកូ	20	ស្វីសហ្ស៊ឺឡែន	4	ញ៉ូវហ្ស៊ីឡែន	1
ថៃ	17	ឈីលី	3	អ៊ុយក្រែន	1
រូម៉ានី	16	ម៉ាការ	3	អុយរុយហ្គាយ	1
ទួគី	15	ប៉េរូ	3	កៀហ្គាស្ថាន	1
សហព័ន្ធអារ៉ាប់	14	ព័រទុយហ្គាល់	3	ប៉ាន់ប្រមាណលើការសរុប:	4997
អាយឡែន	11	វៀតណាម	3	ចំនួនសរុបពិត:	4987

Note: The number of certificates shown here are as of 21 December 2008.
Source: International Register of ISMS Certificates, "Number of Certificates per Country," ISMS International User Group Ltd., http://www.iso27001certificates.com.

ទ្រង់ទ្រាយដែលមានលក្ខណៈពិត

នៅពេលបច្ចុប្បន្នគឺមិនមែនមានប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានលើរូបរាងពិតជាអន្តរជាតិ។ភ្នាក់ងារគ្រប់គ្រងស្ថានការបន្ទាន់របស់របស់សហព័ន្ធ (FEMA) ៤២៦[37] ដែលគឺជាគំរូសម្រាប់រូបរាងពិត ISMS នៅក្នុងសហរដ្ឋអាមេរិក និងដែលប្រទេសជាច្រើនប្រើជាយុទ្ធវិធីមួយ និងត្រូវបានពិពណ៌នានៅក្នុងទីនេះ។

FEMA ៤២៦ ផ្តល់នៅសេចក្តីណែនាំនានាសម្រាប់ការការពារអាគារនានាប្រឆាំងនឹងការវាយប្រហារភេរវកម្ម។ វាគឺត្រូវធ្វើដោយត្រង់ចំពោះ “ការកសាងសហគមន៍វិទ្យាសាស្ត្រនៃស្ថាបត្យករ និងវិស្វករ ដើម្បីកាត់បន្ថយការបំផ្លាញនៅរូបរាងពិតទៅលើអាគារ ហេដ្ឋារចនាសម្ព័ន្ធដែលពាក់ព័ន្ធ និងប្រជាជនដែលបង្កឡើងដោយការឈ្លានរបស់ឯកជន”។[38] ស៊េរីដែលជាប់ពាក់ព័ន្ធនៃសេចក្តីណែនាំនោះគឺ FEMA ៤២៧ (“របៀបដំបូងលើការរៀបចំអាគារឧស្សាហកម្មនានាដើម្បីប្រឆាំងតបតនឹងការវាយប្រហាររបស់ភេរវជន”), FEMA ៤២៨ (“របៀបដំបូងចំពោះគម្រោងបង្កើតសាលាសុវត្ថិភាពនៅក្នុងករណីនៃការវាយប្រហាររបស់ភេរវជន”), FEMA ៤២៩ (“របៀបដំបូងស្តីពីការធានារ៉ាប់រងហិរញ្ញវត្ថុ និងភាពស្របច្បាប់សម្រាប់ការគ្រប់គ្រងហានិភ័យនៃភេរវកម្មនៅក្នុងអាគារនានា”), FEMA ៤៣០ (ស្ថាបត្យកម្ម) និង FEMA ៤៣៨ (មុខវិជ្ជាសិក្សា)។

FEMA ៤២៦ គឺវាមិនទាក់ទងផ្ទាល់ដោយត្រង់ៗលើសន្តិសុខព័ត៌មានប៉ុន្តែវាអាចការពារការលេចចេញ ការបាត់បង់ ឬការបំផ្លាញនៃព័ត៌មានពីព្រោះការវាយប្រហារលើអាគារ។ ជាពិសេស FEMA ៤២៦ គឺជាប់ពាក់ព័ន្ធយ៉ាងជិតស្និទ្ធទៅនឹងគម្រោងនិរន្តន៍ភាពនៃជំនួញដែលជាធាតុមួយនៃសន្តិសុខរដ្ឋបាល។ ដោយសង្កេតមើលលើ FEMA ៤២៦ ទ្រង់ទ្រាយរូបភាពពិតនៃគម្រោងនិរន្តន៍ភាពរបស់ជំនួញអាចត្រូវបានការពារ។

ទ្រង់ទ្រាយជាលក្ខណៈបច្ចេកទេស

គឺមិនមាន ISMS សម្រាប់ទ្រង់ទ្រាយជាលក្ខណៈបច្ចេកទេសគំរូអន្តរជាតិសម្រាប់ការវាយតម្លៃដែលមានលក្ខណៈសាមញ្ញៗមានដូចជាលិខិតបញ្ជាក់ពី Common Criteria (CC) ប្រហែលជាត្រូវបានប្រើជំនួស។

37 FEMA, “FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings,” http://www.fema.gov/plan/prevent/rms/rmsp426.

38 Ibid.

លិខិតបញ្ជាក់ពី Common Criteria[39]

លិខិតបញ្ជាក់ពី Common Criteria មាកឫសគល់នៃជំនួញ។ វាត្រូវបានបង្កើតឡើងដើម្បីកត់សម្គាល់ទៅលើចម្ងល់នានាអំពីភាពផ្សេងៗគ្នានៅក្នុងកម្រិតសន្តិសុខនានានៃផលិតផល IT ដែលផលិតដោយប្រទេសផ្សេងៗគ្នា។ គំរូអន្តរជាតិមួយត្រូវបានបង្កើតសម្រាប់ការវាយតម្លៃនៃផលិតផល IT នានាដោយប្រទេសកាណាដា បារាំង អាល្លឺម៉ង់ អង់គ្លេស និងសហរដ្ឋអាមេរិក។

យ៉ាងជាក់លាក់ CC តំណាងឲ្យសេចក្តីស្នើសុំនានាសម្រាប់ឲ្យមានសន្តិសុខ IT នៃផលិតផលឬប្រើប្រព័ន្ធនៅក្រោមផ្នែកផ្សេងៗនៃសេចក្តីស្នើសុំខាងមុខងារ និងការធានាង៉ាប់រង។ សេចក្តីស្នើសុំខាងមុខងាររបស់ CC គឺជាការកំនត់ទៅលើលក្ខណៈសន្តិសុខដែលប្រាថ្នាចង់បានដោយអ្នកប្រើប្រាស់។ សេចក្តីស្នើសុំខាងធានា៉ាប់រងក៏ជាភាគសំខាន់សម្រាប់ការផ្តល់នៅទំនុកចិត្តជារង្វាស់លើសន្តិសុខដែលត្រូវបានប្រកាសឲ្យប្រើប្រាស់នោះគឺប្រកបដោយប្រសិទ្ធិភាព និងអនុវត្តន៍បានយ៉ាងត្រឹមត្រូវ។ មុខងារសន្តិសុខនានារបស់ CC រួមមាន ១៣៦ ធាតុចេញមកពី ១១ក្រុម ដែលបង្កើតបាន ៥៧គ្រួសារ សេចក្តីស្នើសុំខាងធានា៉ាប់រងសំដៅយក ៨៦ធាតុ ចេញមកពី ៩ក្រុម ដែលបង្កើតបាន ៤០គ្រួសារ។

តម្រូវឲ្យមាននៅមុខងាររបស់សន្តិសុខ (Security functional requirement (SFR):) SFRs ពិពណ៌នាយ៉ាងច្បាស់នៅរាល់មុខងាររបស់សន្តិសុខសម្រាប់ទិសដៅនៃការវាយតម្លៃ Target of Evaluation (TOE) ។ តារាងលេខ៧.រាយនៅក្រុមនៃមុខងាររបស់សន្តិសុខដែលត្រូវានបញ្ចូលក្នុង SFRs

តារាងលេខ៧.សមាសភាពនៃក្រុមនៅក្នុង SFRs

ក្រុម		ការពិពណ៌នា
FAU	សាវនកម្មសន្តិសុខ	សំដៅលើមុខងារមួយចំនួនដែលរួមមានការធ្វើសាវនកម្មលើការការពារទិន្នន័យ របៀបថតទុកឯកសារ និងការជ្រើសរើសនៅហេតុតការណ៍ដូចជាឧបករណ៍ប្រើសម្រាប់ការវិភាគ ការប្រកាសពីការរំលោភបំពាន និងការវិភាគចំពោះហេតុការពិតផងដែរ
FCO	គមនាគមន៍	ពិពណ៌នានៅតម្រូវការជាចាំបាច់នានានៃប្រាក់

39 Common Criteria, http://www.commoncriteriaportal.org.

		កំរៃសម្រាប់ TOEs ដែលត្រូវបានគេប្រើប្រាស់ក្នុងការបញ្ជូនព័ត៌មាន
FCS	ការគាំទ្រលើរហស្សលិខសាស្ត្រ	កំណត់យកយ៉ាងច្បាស់លើការប្រើប្រាស់នៃការគ្រប់គ្រងស៊ីសំខាន់លើរហស្សលិខសាស្ត្រ និងការអនុវត្តវា
FDP	ការការពារទិន្នន័យរបស់អ្នកប្រើប្រាស់	តម្រូវការក៏ជាក់លាក់ដែលទាក់ទងនឹងកិច្ចការពារទិន្នន័យរបស់អ្នកប្រើប្រាស់
FIA	អត្តសញ្ញាណ និងយថាភាព (ភាពត្រឹមត្រូវតាមច្បាប់)	និយាយសំដៅលើតម្រូវការនានាសម្រាប់មុខងារផ្សេងៗក្នុងការបង្កើត និងបញ្ជាក់លើអត្តសញ្ញាណរបស់អ្នកប្រើប្រាស់ដែលត្រូវបានអះអាងរួច
FMT	ការគ្រប់គ្រងលើសន្តិសុខ	កំណត់យ៉ាងច្បាស់លើការគ្រប់គ្រងនៃទ្រង់ទ្រាយមួយចំនួនរបស់សន្តិសុខ TOE (TSF): ការកំណត់យកសន្តិសុខផ្សេង ទិន្នន័យ TSF និងមុខងារដទៃៗទៀតរបស់ TSF។
FPR	ឯកជនភាព	ពិពណ៌នាលើតម្រូវការមួយចំនួនដែលអាចត្រូវបានធ្វើឡើងដើម្បីបំពេញនៅសេចក្តីត្រូវការជាឯកជនភាពរបស់អ្នកប្រើប្រាស់។ខណៈពេលតម្រូវការខ្លះបន្តឲ្យមានការអនុញ្ញាតសម្រាប់ប្រព័ន្ធមួយដែលប្រកបដោយភាពបត់បែនក៏ដូចទៅនឹងការថែរក្សាលើការត្រួតពិនិត្យមើលឲ្យបានគ្រប់គ្រាន់ទៅលើការប្រតិបត្តិនៃប្រព័ន្ធ។
FPT	ការការពារនៃ TSF	រួមមានគ្រួសារជាច្រើននៃតម្រូវការខាងមុខងារដែលទាក់ទងទៅនឹងសុចរិតភាព និងការគ្រប់គ្រងនៃគ្រឿងយន្តផ្សេងៗទៀតដែលបង្កើតបានជា TSF និងសុចរិតភាពនៃទិន្នន័យ TSF
FRU	ការប្រើប្រាស់ធនធាន	រួមមានភាពដែលអាចរកបាននៃប្រភពដែលត្រូវការដូចជាសមត្ថភាពនៃការប្រតិបត្តិ និងឬ សមត្ថភាពនៃការរក្សាទុក
FTA	ដំណើរការ TOE	កំណត់យ៉ាងច្បាស់ចំពោះតម្រូវការខាងមុខងារការត្រួតពិនិត្យលើការបង្កើតឡើងនៅសម័យមួយរបស់អ្នកប្រើប្រាស់។

FTP	តំបន់ ឬផ្លូវដែលគួរឲ្យជឿជាក់	ផ្តល់នៅតម្រូវការនានាសម្រាប់ផ្លូវគមនាគមន៍ដ៏គួរឲ្យជឿទុកចិត្តមួយរវាងអ្នកប្រើប្រាស់ទាំងឡាយ និង TSF

Source: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007,CCMB-2007-09-004

សមាសធាតុនានាលើការធានាការពារសន្តិសុខ (SACs) តាមចិត្តសាស្ត្ររបស់ CC ស្នើសុំលើសន្ទិយោគនៃការគំរាមកំហែងសន្តិសុខនានា និងឲ្យមានការផ្តាច់ផ្ទាចិត្តដទៃទៀតចំពោះគោលការណ៍ច្បាប់សន្តិសុខដែលត្រូវបានរៀបចំតាមរយៈវិធានការសន្តិសុខដ៏សមរម្យ និងប្រកបដោយភាពគ្រប់គ្រងលើការធ្វើវា។ វិធានការទាំងនោះដែលត្រូវបានទទួលយកមកគួរត្រូវតែជួយកំនត់នៅភាពងាយស្រួលរងគ្រោះនានាកាត់បន្ថយភវនីយភាពនៃការកេងប្រវ័ញ្ច និងពង្រីកនៅការបំផ្លាញនៅក្នុងហេតុការណ៍មួយដែលភាពងាយរងគ្រោះនានាគឺត្រូវបានគេទាញយកផលប្រយោជន៍ពីវា។[40] តារាងលេខ៨ រាយនៅក្រុមនានាដែលបានដាក់បញ្ចូលក្នុង SACs

តារាងលេខ៨.សមាសភាពបែក្រុមនៅក្នុង SACs

ក្រុម		ការពិពណ៌នា
APE	ការវាយតម្លៃលើការការពារនៃទម្រង់ (PP)	នេះត្រូវបានតម្រូវឲ្យបង្ហាញថា PP គឺជាសម្លេងនិងជាធាតុរឹងប៉ឹងនៃផ្នែកខាងក្នុងហើយប្រសិនបើ PP មួយមានការពឹងផ្អែកលើមួយ ឬក៏ច្រើននៃ PP ដទៃទៀតឬកញ្ចប់ផ្សេងទៀតនោះគឺថា PP មួយនោះជាផ្នែកគ័ត្រឹមត្រូវនៃ PP ទាំងនេះនិងកញ្ចាប់ទាំងនេះ។
ASE	ការវាយតម្លៃលើទិសដៅសន្តិសុខ (ST)	នេះត្រូវបានតម្រូវឲ្យបង្ហាញថា ST គឺជាសម្លេងនិងជាធាតុរឹងប៉ឹងនៃផ្នែកខាងក្នុងហើយប្រសិនបើ ST មួយមានការពឹងផ្អែកលើមួយ ឬក៏ច្រើននៃ PP ដទៃទៀតឬកញ្ចប់ផ្សេងទៀតនោះគឺថា ST មួយនោះជាផ្នែកគ័ត្រឹមត្រូវនៃ PP ទាំងនេះនិងកញ្ចាប់ទាំងនេះ។
ADV	ការអភិវឌ្ឍន៍	នេះផ្តល់ព័ត៌មានអំពី TOE ។ ចំណេះដឹងដែលបានមកគឺត្រូវបានប្រើជាមូលដ្ឋានគ្រឹះសម្រាប់ការអនុវត្តន៍ការវិភាគនៃភាពងាររងគ្រោះ និងការធ្វើសាកល្បងលើ TOE ដូចដែលបានពិពណ៌នារួចមកហើយនៅក្នុង ATE និង ក្រុម AVA ។

40 Common Criteria, *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements* (August 1999, Vesion 2.1), http://www.scribd.com/doc/2091714/NSA-Common-Critira-Part3.

AGD	ឯកសារសម្រាប់ការណែនាំនានា	សម្រាប់ឲ្យសុវត្ថិភាពលើការរៀបចំ និងអនុវត្តន៍លើ TOE វាចាំបាច់ដើម្បីពិពណ៌នានៅរាល់ទ្រង់ទ្រាយដែលជាប់ពាក់ព័ន្ធសម្រាប់ការប្រើនៃ TOE ដោយសុវត្ថិភាព។ក្រុមនានាត្រូវគិតពីការខុសឆ្គងនៃរូបសណ្ឋានដែលអាចកើតមានឬក៏ការខុសឆ្គងលើការប្រើប្រាស់នៃ TOE។
ALC	គាំទ្រវិឌ្ឍកាលនៃអាយុ	នៅក្នុងវិវឌ្ឍកាលនៃអាយុ ដែលរួមមានទាំងសមត្ថភាពនៃការគ្រប់គ្រងលើរូបសណ្ឋាន (CM) CM Scope ការចែកចាយការអភិវឌ្ឍន៍លើសន្តិសុខ ការបង្ហាញនៅការខូចខាត និយមន័យនៃវិវឌ្ឍន៍កាលនៃអាយុ ឧបករណ៍ និងបច្ចេកវិទ្យាវាគឺត្រូវបានធ្វើឲ្យខុសគ្នា ទោះជាវាស្ថិតនៅក្រោមការទទួលខុសត្រូវនានានៃអ្នកអភិវឌ្ឍន៍វាឬក៏អ្នកប្រើប្រាស់វា។
ATE	ការសាកល្បង	ការសង្កត់ធ្ងន់នៅក្នុងក្រុមនេះគឺនៅលើការបញ្ជាក់ថា TSF ប្រតិបត្តិអាស្រ័យលើការពិពណ៌នាលើការរៀបចំរបស់វា។ក្រុមនេះមិននិយាយពីការសាកល្បងដ៏វែឆ្ងាតមួយណាឡើយ។
AVA	ការប៉ាន់ប្រមាណលើភាពងាយរងគ្រោះ	សកម្មភាពប៉ាន់ប្រមាណលើភាពងាយរងគ្រោះគ្របដណ្តប់លើភាពងាយរងគ្រោះផ្សេងៗពីគ្នានៅក្នុងការអភិវឌ្ឍន៍ និងការអនុវត្តន៍នៃ TOE។
ACO	សមាសភាព	កំណត់លើសេចក្តីត្រូវការខាងធានា៉ាប់រងយ៉ាងជាក់ច្បាស់នោះដែលត្រូវបានរៀបចំឡើងដើម្បីផ្តល់នៅភាពជឿជាក់ដែលសមាសភាព TOE និងប្រតិបត្តិការប្រកបដោយសុវត្ថិភាពនៅពេលដែលវាពឹងផ្អែកលើមុខងារដែលបានផ្តល់ឲ្យដោយកម្មវិធី Software Firmware ឬក៏ធាតុរបស់ Hardware នានាដែលធ្លាប់បានវាយតម្លៃកាលពីពេលមុន។

Source: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007,CCMB-2007-09-004

យុទ្ធវិធីវាយតម្លៃនៃ CC

១. ការវាយតម្លៃនៃ PP: PP ពិពណ៌នាពីបណ្តុំនៃដំណើរឯករាជ្យនានានៃតម្រូវការឲ្យមានលើសន្តិសុខសម្រាប់ផ្នែកផ្សេងៗរបស់ TOE និងរួមទាំងបញ្ហាសន្តិសុខដែលផលិតផលដែលត្រូវប្រើប្រាស់លើសន្តិសុខនោះគឺត្រូវត្រៀមខ្លួនចូលរួមដោះស្រាយ។ វាធ្វើឲ្យជាក់លាក់នៅតម្រូវការលើការធានារ៉ាប់រង និងមុខងាររបស់ CC និងផ្តល់នៅសនិទានភាពសម្រាប់ធាតុរបស់ការធានារ៉ាប់រង និងធាតុរបស់មុខងារដែលត្រូវបានជ្រើសរើស។វាគឺត្រូវបង្កើតឡើងយ៉ាងសាមញ្ញដោយអ្នកប្រើប្រាស់ ឬសហគមន៍អ្នកប្រើប្រាស់សម្រាប់តម្រូវការខាងសន្តិសុខ IT។

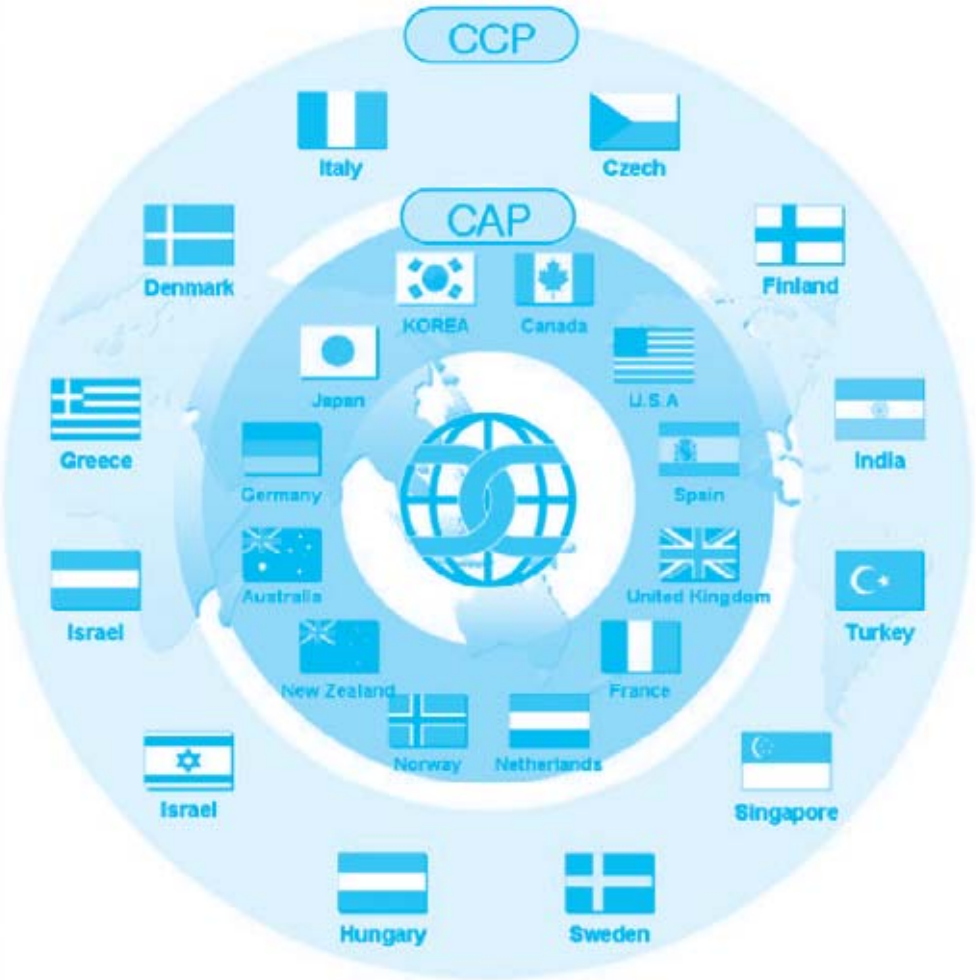
២. ការវាយតម្លៃនៃ ST: ST គឺជាមូលដ្ឋានគ្រឹះសម្រាប់កិច្ចព្រមព្រៀងរវាងអ្នកអភិវឌ្ឍន៍ TOE អ្នកប្រើប្រាស់ អ្នកវាយតម្លៃ និងសិទ្ធិនានាលើការវាយតម្លៃដូចទៅអ្វីដែលសន្តិសុខ TOE ផ្តល់ឲ្យ និងរយៈពេលនៃការវាយតម្លៃ។អ្នកប្រើប្រាស់សម្រាប់ ST ប្រហែលជារួមបញ្ចូលផងដែរទៅលើការគ្រប់គ្រង ការលក់ ការទិញ ការតម្លើង ការបង្កើតនៅរូបសណ្ឋាន ការអនុវត្តន៍ និងការប្រើប្រាស់ TOE។ST មានទាំងដំណើរការលើព័ត៌មានដ៏ជាក់លាក់មួយចំនួនដែលបង្ហាញពីរបៀបដែលផលិតផលមួយនិយាយពីតម្រូវការសន្តិសុខ។វាប្រហែលសំដៅទៅលើមួយ ឬក៏ច្រើន PPs។នៅក្នុងករណីនេះ ST ត្រូវតែបំពេញនៅតម្រូវការសន្តិសុខទៅតាមផ្នែកនិមួយៗដែលត្រូវបានឲ្យនៅក្នុង PPs មួយៗ និងប្រហែលជាកំណត់លើសេចក្តីស្នើសុំនានាដ៏វែងឆ្ងាយទៀត។

កិច្ចព្រមព្រៀងលើកការរៀបចំនៃតំបន់ធម្មតាៗ (*Common Criteria Recognition Arrangement*)

Common Criteria Recognition Arrangement (CCRA) ត្រូវបានរៀបចំឡើងសម្រាប់ការយល់ព្រមលើលិខិតបញ្ជាក់របស់ CC ក្នុងចំណោមជាតិនានា។វាមានគោលបំណងដើម្បីធានាថាការវាយតម្លៃ CC គឺត្រូវបានធ្វើឡើងដើម្បីភាពរឹងមាំរបស់គំរូនានា ការលុបបំបាត់ ឬកាត់បន្ថយទៅលើការវាយតម្លៃជាន់គ្នាលើផលិតផល IT ឬក៏ការការពារលើទម្រង់ផ្សេងៗ និងការធ្វើឲ្យប្រសើរនៅឱកាសសម្រាប់ទីផ្សារសាកលរបស់ឧស្សាហកម្ម IT ដោយការយល់ព្រមឲ្យមានលិខិតបញ្ជាក់ក្នុងចំណោមជាតិដែលជាសមាជិក។

CCRA មាន២៤ជាតិជាសមាជិក ដែល១២ គឺជាអ្នកចូលរួមលើការផ្តល់សិទ្ធិលើលិខិតបញ្ជាក់ (Certificate Authorizing Participants (CAPa)) និង ១២ គឺជាអ្នកចូលរួមនៅការប្រើប្រាស់លើលិខិតបញ្ជាក់លើការវាយតម្លៃ។ពួកគេគឺជាអ្នកគាំទ្រនៃការដើរតាមនៅការប្រតិបត្តិរបស់លិខិតបញ្ជាក់នៅក្នុងប្រទេសរបស់ពួកគេ និងពួកគេជាអ្នកផ្តល់សិទ្ធិលើបញ្ជាលិខិតបញ្ជាក់។ប្រទេមួយត្រូវតែក្លាយជាសមាជិកនៃ CCAR ក៏ដូចជា CCP សម្រាប់រយៈពេលពីរឆ្នាំយ៉ាងតិចបំផុតមុន និងដាក់ពាក្យស្នើសុំជាសមាជិករបស់ CAP ។CCPs គឺជាអ្នកប្រើប្រាស់នៃលិខិតបញ្ជាក់លើការវាយតម្លៃ។ទោះបីជាពួកគេមិនប្រកាន់យកនៅសមត្ថភាពនៃការវាយតម្លៃលើសន្តិសុខព័ត៌មានក៏ដោយ ប៉ុន្តែពួកគេបានបង្ហាញពីចំណាប់អារម្មណ៍ក្នុងការប្រើប្រាស់ផលិតផលដែលមានការបញ្ជាក់ មានសុពលភាព រួមទាំងការការពារលើទម្រង់នានា។ ដើម្បីក្លាយជាសមាជិកនៃ CCRA ប្រទេសមួយគួរតែដាក់ទំរង់ស្នើសុំដែលត្រូវបានសរសេរដោយដៃទៅកាន់គណៈកម្មធិការគ្រប់គ្រង។

រូបលេខ៩. CAPs **និង** CCPs



៤.២ ឧទាហរណ៍នានានៃយុទ្ធវិធីសន្តិសុខព័ត៌មាន

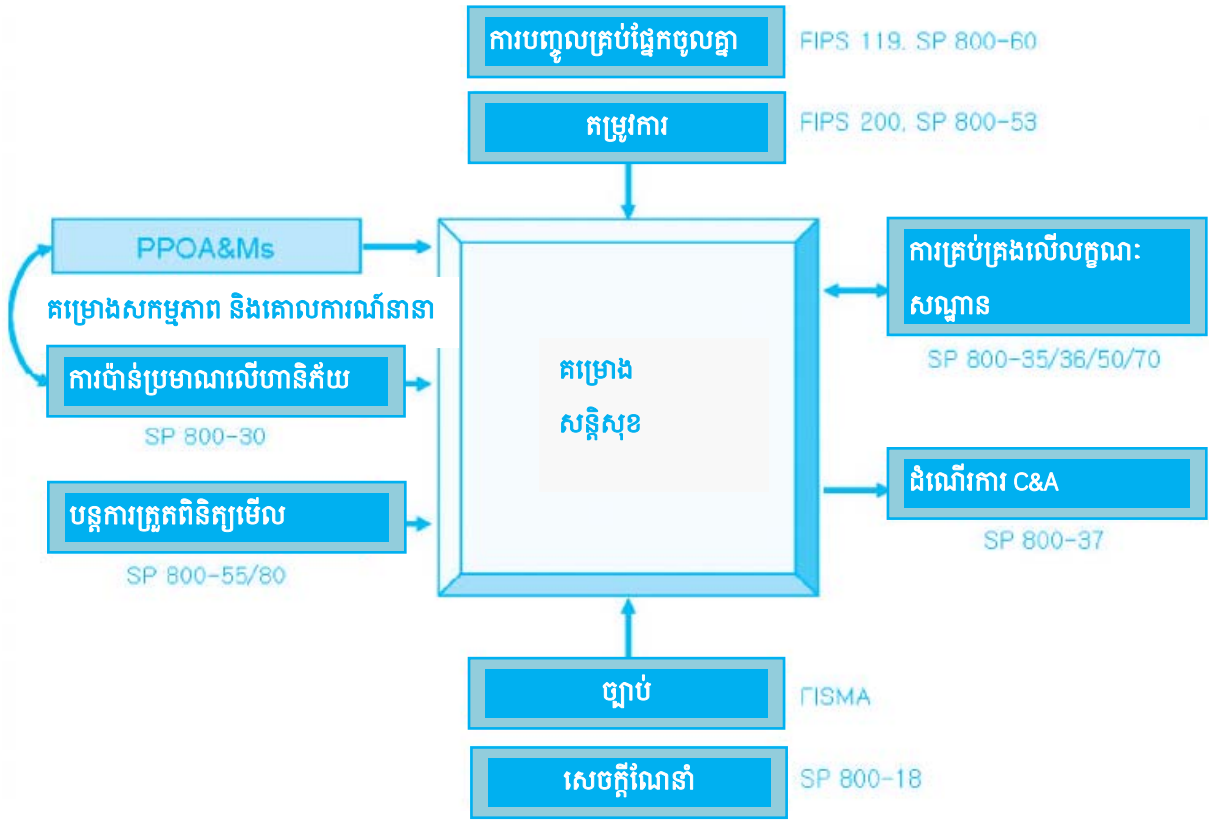
វិទ្យាស្ថានគំរូ និងបច្ចេកវិទ្យាជាតិរបស់សហរដ្ឋអាមេរិក

ផ្អែកលើ FISMA វិទ្យាស្ថានគំរូ និងបច្ចេកវិទ្យាជាតិរបស់សហរដ្ឋអាមេរិក (NIST) បានធ្វើការអភិវឌ្ឍន៍នៅសេចក្តីណែនាំ និងគំរូផ្សេងៗសម្រាប់ពង្រឹងសន្តិសុខនៃព័ត៌មាន និងប្រព័ន្ធព័ត៌មាននានាដែលវិទ្យាស្ថានសហព័ន្ធជាច្រើនអាចប្រើប្រាស់វា។សេចក្តីណែនាំ និងគំរូទាំងនោះមានគោលបំណងក្នុងការ៖

- ផ្តល់នៅភាពប្រាកដប្រជាសម្រាប់ធ្វើឲ្យសេចក្តីស្នើសុំនានារបស់សន្តិសុខក្នុងកំរិតអប្បបរមាដោយការអភិវឌ្ឍន៍នៅគំរូទាំងនោះដែលអាចត្រូវបានប្រើប្រាស់សម្រាប់ការបញ្ចូលគ្នាគ្រប់ផ្នែកនៃប្រព័ន្ធព័ត៌មាន និងព័ត៌មានសហគមន៍។
- អាចឲ្យប្រព្រឹត្តទៅបាននៅការបញ្ចូលគ្នានៅសន្តិសុខព័ត៌មាន និងប្រព័ន្ធ
- ជ្រើសរើស និងធ្វើឲ្យជាក់ច្បាស់នៅរាល់ការត្រួតពិនិត្យសន្តិសុខសម្រាប់ប្រព័ន្ធព័ត៌មានដែលគាំទ្រទៅលើភ្នាក់ងារប្រតិបត្តិនៃរដ្ឋាភិបាលសហព័ន្ធ។
- ត្រួតពិនិត្យនៅភាពវិជ្ជមាន និងប្រកបដោយប្រសិទ្ធិភាពនៃការត្រួតពិនិត្យសន្តិសុខទៅលើភាពងាររងគ្រោះផ្សេងៗ។

សេចក្តីណែនាំដែលទាក់ទងទៅនឹង FISMA គឺត្រូវបានផ្សព្វផ្សាយជាការផ្សព្វផ្សាយពិសេស និងការផ្សព្វផ្សាយលើគំរូនានានៃដំណើរការរបស់ព័ត៌មានសហព័ន្ធ។ គឺមាន២សៀរីនៃការផ្សព្វផ្សាយពិសេសនេះ ៥០០សៀរីសម្រាប់បច្ចេកវិទ្យាព័ត៌មាន និង៨០០ សៀរីសម្រាប់សន្តិសុខកុំព្យូទ័រ។រូបភាងលេខ១០ បង្ហាញនៅដំណើរការដែលភ្នាក់ងាររដ្ឋាភិបាលសហរដ្ឋអាមេរិកធ្វើទៅតាមការបង្កើតរបស់គម្រោងសន្តិសុខរបស់ពួកគេដោយផ្អែកលើគំរូនេះ។

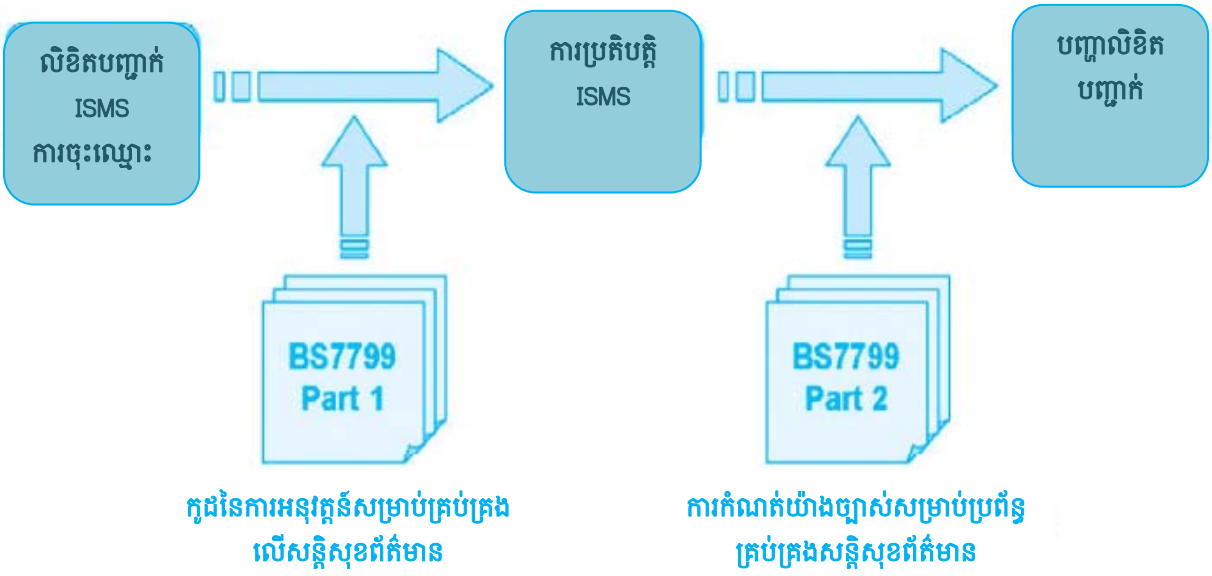
រូបលេខ១០. ដំណើរការចេញចូលលើគម្រោងសន្តិសុខ



ចក្រភពអង់គ្លេស (BS7799)

ដូចអ្វីដែលបានលើកឡើងពីពេលមុននេះ BSI ធ្វើការវិភាគលើសកម្មភាពផ្សេងៗរបស់សន្តិសុខនៃស្ថាប័ននានានៅក្នុងចក្រភពអង់គ្លេស និងឲ្យនៅលិខិតបញ្ជាក់ BS7799 ដែលឥឡូវត្រូវបានអភិវឌ្ឍន៍ទៅកាន់ ISO 27001 (BS7799ផ្នែកទី២) និង ISO 27002 (BS7799ផ្នែកទី១).រូបរាងលេខ ១១ បង្ហាញពីវិធានការដែលត្រូវបានគោរពតាម:

រូបលេខ១១.ដំណើរនៃលិខិតបញ្ជាក់ BS7799

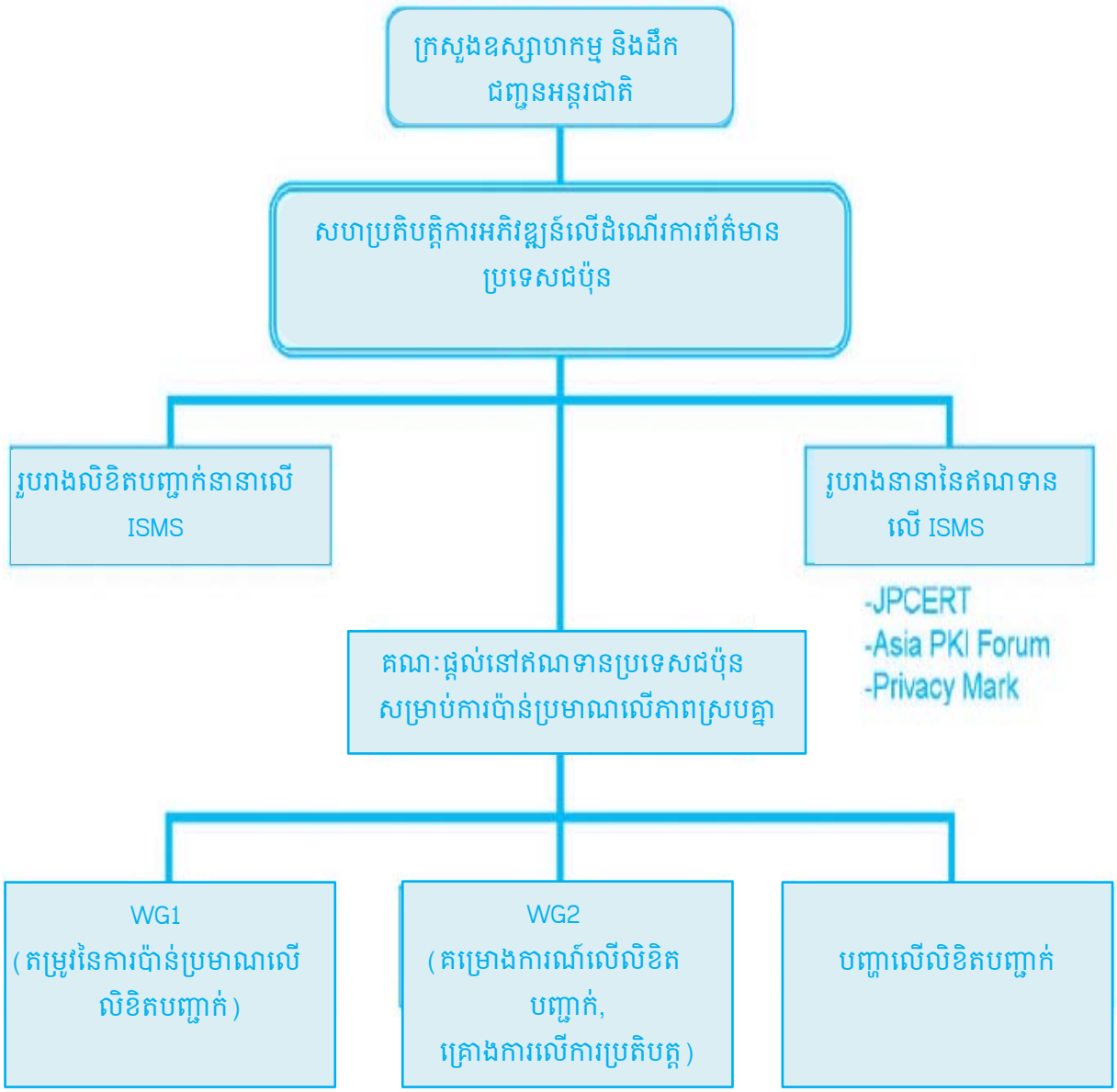


ជប៉ុន (**ពី** ISMS **ជំនាន់** 2.0 **ទៅ** BS7799 **ផ្នែកទី២**:2002)

ISMS ជំនាន់ទី២.0 នៃកិច្ចប្រតិបត្តិការអភិវឌ្ឍន៍លើដំណើរការព័ត៌មានប្រទេសជប៉ុនត្រូវបានអនុវត្តន៍នៅក្នុងប្រទេសជប៉ុនកំឡុងខែមករា ឆ្នាំ ២00២។ វាត្រូវបានជំនួសដោយ BS7799 ផ្នែកទី2:2002 ក្នុងពេលថ្មីៗនេះ។

អាគ្រានៃដំណើរការសម្រាប់វិញ្ញាបណ្ណប័ត្របានកើនឡើងចាប់តាំងពីរដ្ឋាភិបាលកណ្តាលបានជំរុញលើគម្រោងការសន្តិសុខព័ត៌មាន។ គ្រប់គ្រងនៃតំបន់បានផ្តល់លុយសម្រាប់អង្គភាពនានាបាននៅវិញ្ញាប័ណ្ណប័ត្រ ISMS។ទោះបីជាយ៉ាងណាក៏ដោយ ISMS ជំនាន់ 2.0 គ្រាន់តែសង្កត់ធ្ងន់ទៅលើទ្រង់ទ្រាយក្នុងលក្ខណៈរដ្ឋបាល និងមិនរួមបញ្ចូលនៅទ្រង់ទ្រាយខាងបច្ចេកទេសនៃសន្តិសុខព័ត៌មាន។ ច្រើនជាងនេះទៀតអង្គភាពភាគច្រើនគឺចាប់អារម្មណ៍ត្រឹមតែទទួលបាននៅការបញ្ជាក់តែប៉ុណ្ណោះ និងមិនចាំបាច់នៅក្នុងការធ្វើឲ្យប្រសើរឡើងនៅរាល់សកម្មភាពសន្តិសុខព័ត៌មានទាំងឡាយរបស់ពួកគេទេ។ រូបទី១២ បង្ហាញពីប្រព័ន្ធលិខិតបញ្ជាក់ ISMS នៅក្នុងប្រទេសជប៉ុន

រូបលេខ១២. លិខិតបញ្ជាក់លើ ISMS **នៅក្នុងប្រទេសជប៉ុន**

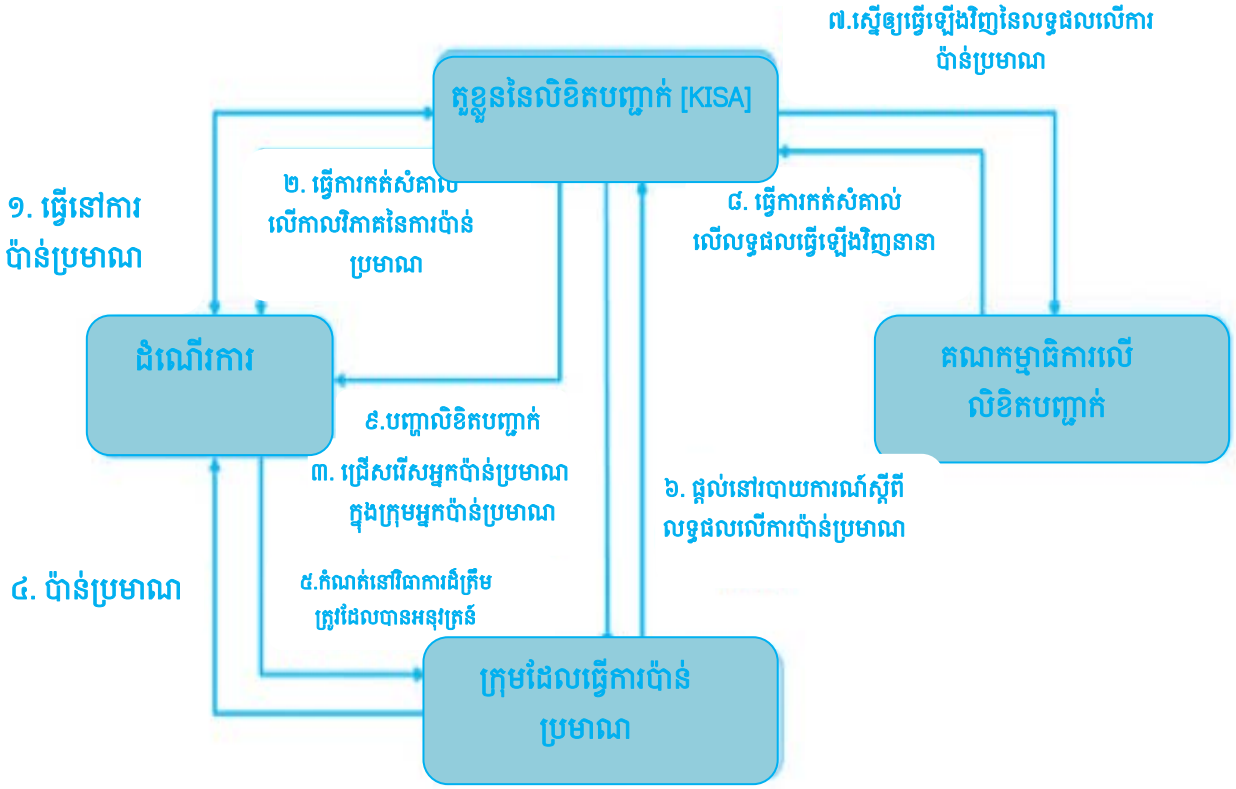


សាធារណរដ្ឋកូរ៉ែ (ISO/IEC 27001 **និង/ឬ** KISA ISMS)

វិញ្ញាប័ណ្ណប័ត្រ ISMS ធ្វើឡើងដោយភ្នាក់ងារសន្តិសុខព័ត៌មានប្រទេសកូរ៉ែ (KISA) បានធ្វើការអភិវឌ្ឍន៍យ៉ាងសំខាន់ដោយ MIC ត្រូវបានប្រើកំឡុងពេល ISO/IEC 27001 បាននឹងកំពុងចែកចាយដោយ BSI-Korea។ ISMS របស់ KISA គឺជាប្រព័ន្ធគ្រប់គ្រងការសង្គ្រោះមួយដែលរួមមានទាំងពង្រឹងនៅតំបន់សន្តិសុខព័ត៌មានបច្ចេកវិទ្យាដែលខ្វះសមត្ថភាពនៅក្នុងការអនុវត្តន៍ ISO/IEC 27001 ជាពិសេសការទទួលយកនៃ <<វិធានការ

សន្តិសុខ>> ជាតម្រូវការមួយនៃវិញ្ញាប័ណ្ណប័ត្រពង្រឹងនៅការរិភាគខាងបច្ចេកទេស។រូបរាងទី១៣ បង្ហាញពីដំណើរការលើលិខិតបញ្ជាក់ ISMS របស់ KISA

រូបលេខ១៣. វិញ្ញាប័ណ្ណប័ត្រ ISMS **នៃ** KISA



អាល្លឺម៉ង់ (IT Baseline Protection Qualification (**គុណសម្បត្តិនៃការការពារ** IT Baseline))

BSI របស់ប្រទេស (Bundesamt for Sichersheit inder informationstechnic) គឺជាភ្នាក់ងារអន្ត្រជាតិសម្រាប់សន្តិសុខព័ត៌មាន។វាផ្តល់សេវាកម្មលើសន្តិសុខ IT ទៅឲ្យរដ្ឋាភិបាលអាល្លឺម៉ង់ ទីក្រុងនានា អង្គភាពនានា និងអ្នកប្រើប្រាស់ម្នាក់ៗនៅក្នុងប្រទេសអាល្លឺម៉ង់។

BSI បានបង្កើតនៅ IT Baseline Protection Qualification ផ្អែកលើស្តង់ដារអន្តរជាតិ ISO Guide 25 [GUI25] និងគំរូរបស់អឺរ៉ុប EN45001 ដែលត្រូវបានទទួលស្គាល់ដោយគណៈកម្មាធិការអឺរ៉ុបសម្រាប់ការសាកល្បង និងធ្វើលិខិតបញ្ជាក់លើ IT។ ប្រភេទលិខិតបញ្ជាក់ទាំងនោះរួមមាន លិខិតបញ្ជាក់លើ

Baseline Protection (Baseline Protection Cerficate) self-declared (IT Baseline Protection higher level) និង self-declard (IT Baseline Protection entry level)។

បន្ថែមលើនេះទៀត ការការពារដែលធ្វើឡើងដោយដៃលើ Baseline (Baseline Protection Manual) (BPM) និងការដែលធ្វើឡើងដោយដៃនៃស៊េរីគំរូ BSI:100-X ត្រូវបានអភិវឌ្ឍន៍រួបរាងផ្សេងទៀតរួមមាន: BSI 100-1 ISMS គំរូ BSI 100-2 BPM Methodology និងគំរូ BSI 100-3 Risk analysis។[41]

ផ្សេងទៀត

តារាងលេខ៩.រាយនៅលិខិតបញ្ជាក់ ISMS ជនៃទៀតដែលមានរួចស្រាប់ហើយ

វិទ្យាស្ថាននានាធ្វើការលើលិខិតបញ្ជាក់		គំរូនានា
ប្រទេសកាណាដា	ការបង្កើតសន្តិសុខគមនាគមន៍នានា	MG-4 ណែនាំចំពោះលិខិតបញ្ជាក់ និងឥណទានសម្រាប់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាននានា
តៃវ៉ាន់	ការរិយាល័យនៃគំរូនានា ឧត្តុនិយម និងការពិនិត្យពិច័្យ	CNS 17799 និង CNS 17800
សិង្ហបូរី	គណៈកម្មធិកាគំរូបច្ចេកវិទ្យាព័ត៌មាននានា	SS493: ផ្នែកទី១(គម្រោងគំរូសន្តិសុខព័តមាន) និង SS493: ផ្នែកទី២ (សេវាកម្មសន្តិសុខនានា) ក្រោមការអភិវឌ្ឍន៍

41 Antonius Sommer, "Trends of Security Strategy in Germany as well as Europe" (presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006), http://www.secure.trusted-site.de/download/newsletter/vortraege/KISA.pdf.

៥. ការការពារនៃភាពឯកជន

ចំនុចនេះមានគោលបំណងចំពោះការ

- **តាមដានការផ្លាស់ប្តូរនៅក្នុងគំនិតឯកជនភាព**
- **ពិពណ៌នានិន្នាការអន្តរជាតិនានានៅក្នុងការការពារឯកជនភាព និង**
- **ឲ្យនៅទស្សនៈ និងឧទាហរណ៍នៃការប៉ាន់ប្រមាណមើលលើផលប៉ះពាល់ឯកជនភាព**

៥.១ គោលគំនិតនៃឯកជនភាព

ព័ត៌មានផ្ទាល់ខ្លួនគឺជាព័ត៌មានដែលទាក់ទងទៅនឹងការកំណត់នៅអត្តសញ្ញាណរបស់បុគ្គលម្នាក់ៗ[42] ឬត្រូវបានកំណត់ ឬក៏ជាលក្ខណៈធម្មជាតិរបស់បុគ្គលនោះដែលត្រូវបានសម្គាល់។[43] វារួមមានព័ត៌មានដូចជា ឈ្មោះ លេខទូរស័ព្ទ អាស័យដ្ឋាន e-mail លេខអាជ្ញាប័ណ្ណនៃយានយន្ត លក្ខណៈនៃរូបរាងរបស់បុគ្គលម្នាក់ (សណ្ឋាននៃមុខ អក្សរសរសេរ)។ល។ លេខកាតធនាគារ និងសម្ព័ន្ធភាពគ្រួសារ។

ការដំណើរការ និងការប្រមូលផ្តុំដែលមិនមានលក្ខណៈសមរម្យ ធ្វើការវិភាគ និងប្រើប្រាស់នៅព័ត៌មានបុគ្គលម្នាក់ៗគឺមានផលប៉ះពាល់ទៅលើបុគ្គលនោះព្រមទាំងជាចុងក្រោយមានផលប៉ះពាល់ជាអវិជ្ជមានទៅលើសុវត្ថិភាព ទ្រព្យសម្បត្តិ និងកិត្តិយសក្នុងសង្គមរបស់គាត់។ដូច្នេះព័ត៌មានផ្ទាល់ខ្លួនគួរត្រូវបានការពារពីដំណើរការប្រមូលផ្តុំ ការវិភាគ ការរក្សាទុក និងការប្រើប្រាស់ដោយមិនត្រឹមត្រូវ។ នៅក្នុងគំនិតនេះដដែល ព័ត៌មានផ្ទាល់ខ្លួនគឺជាកម្មវត្ថុមួយនៃការការពារ។

នៅពេលដែលកម្មវត្ថុនៃការការពារ គឺក្លាយជាសិទ្ធិវាជំនួសឲ្យព័ត៌មានផ្ទាល់ខ្លួនលើខ្លួនវានេះគឺជាគោលគំនិតនៃឯកជនភាព។ គឺមានមធ្យោបាយប្រាំដើម្បីពន្យល់ពីសិទ្ធិឯកជនភាព:

- សិទ្ធិដំណើរការដោយសេរីដែលមិនដំណើរការលើព័ត៌មានផ្ទាល់ខ្លួនអ្នកដទៃ (ឧទាហរណ៍:ដំណើរការជាលក្ខណៈពិត ដំណើរការឆ្លងកាត់សេវាកម្មនៃការផ្ញើរសារ)

42 Cabinet Office, *Privacy and Data-sharing: The way forward for public services* (April 2002), http://www.epractice.eu/resource/626.

43 EurLex, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

- សិទ្ធិមិនអនុញ្ញាតឲ្យយកព័ត៌មានផ្ទាល់ខ្លួនរបស់បុគ្គលម្នាក់ប្រើនៅក្នុងមធ្យោបាយខុសឆ្គងនានា (ឧទាហរណ៍: ការលក់ព័ត៌មាន ការផ្សាយនៃព័ត៌មាន ការផ្ទូរផ្តង)
- សិទ្ធិមិនអនុញ្ញាតឲ្យប្រមូលផ្តុំនៅព័ត៌មានផ្ទាល់ខ្លួនរបស់បុគ្គលណាម្នាក់ដោយមិនបានដឹង ឬក៏យល់ព្រមដោយសាមីខ្លួន (ឧទាហរណ៍:តាមរយៈ CCTV និង Cookies)
- សិទ្ធិមាននៅព័ត៌មានផ្ទាល់ខ្លួនដែលត្រូវបានបញ្ជាក់ប្រកបដោយភាពទៀងត្រង់ និងយ៉ាងត្រឹមត្រូវ (សុច្ចរិតភាព)
- សិទ្ធិទទួលបានរង្វាន់ពីតម្លៃនៃព័ត៌មានផ្ទាល់ខ្លួនរបស់សាមីជននោះ

គោលគំនិតអសកម្មនៃឯកជនភាពរួមមានសិទ្ធិដែលត្រូវបានគេទុកចោលម្នាក់ឯង និងសិទ្ធិនៃធម្មជាតិដែលទាក់ទងទៅនឹងកិត្តិយសក្នុងនាមជាមនុស្ស។ វាត្រូវបានចាត់ទុកថាជាសិទ្ធិដែលល្មើសនឹងច្បាប់ដែលគេបានហាមឃាត់។

គោលគំនិតអសកម្មនៃឯកជនភាពរួមមានការគ្រប់គ្រងដោយខ្លួនឯងនៅព័ត៌មានផ្ទាល់ខ្លួន ឬក៏សិទ្ធិគ្រប់គ្រងត្រួតត្រាព័ត៌មានយ៉ាងមានភាពវិជ្ជមានរួមមានការកែតម្រូវទៅលើលទ្ធផលព័ត៌មានផ្ទាល់ខ្លួនដែលខុស។

៥.២ និន្នាការនានានៅក្នុងគោលការណ៍ឯកជនភាព

សេចក្តីណែនាំនានារបស់ OECD **ទៅលើកិច្ចការពារនៃឯកជនភាព**

នៅក្នុងឆ្នាំ ១៩៨០ OECD បានទទួលយក "សេចក្តីណែនាំនានាទៅលើការការពារនៃឯកជនភាព និងការហូរហួសព្រំដែននៃទិន្នន័យផ្ទាល់ខ្លួន" និងត្រូវបានស្គាល់ផងដែរថាជា "ការអនុវត្តន៍ព័ត៌មានយ៉ាងសុក្រិតភាពរបស់ OECD"។ នៅក្នុងឆ្នាំ ២០០២ "Online ឯកជន: សេចក្តីណែនាំ OECD លើគោលការណ៍ច្បាប់និងការអនុវត្តន៍" គឺត្រូវបានប្រកាសឡើង។[44] សេចក្តីណែនាំនានាអនុវត្តន៍ចំពោះទិន្នន័យផ្ទាល់ទោះជាស្ថិតក្នុងវិស័យឯកជន ឬវិស័យសាធារណៈក៏ដោយដែលបង្កឲ្យមានគ្រោះថ្នាក់ដល់ឯកជនភាព និងសិទ្ធិសេរីភាពរបស់បុគ្គលម្នាក់ៗ ដោយការដំណើរការព័ត៌មាននោះស្ថិតក្នុងឥរិយាបថណាមួយក៏ដោយ។ គោលគំនិតនានារបស់ OECD បានធ្វើការគូសបញ្ជាក់នៅក្នុងចំនុចគោលរបស់សេចក្តីណែនាំ អំពីសិទ្ធិ និង

44 OECD, "Privacy Online: OECD Guidance on Policy and Practice," http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.

កាតព្វកិច្ចរបស់បុគ្គលម្នាក់ៗក្នុងដំណើរការលើទិន្នន័យផ្ទាល់ខ្លួនរួមទាំងកាតព្វកិច្ច និងសិទ្ធិជាប់ពាក់ព័ន្ធលើដំណើរការនោះផងដែរ។ ច្រើនជាងនេះទៀត រាល់គោលគំនិតសំខាន់ៗដែលត្រូវបានសង្ខេបនៅក្នុងសេចក្តីណែនាំនោះគឺត្រូវបានអនុវត្តន៍ទាំងនៅក្នុងកម្រិតថ្នាក់ជាតិ និងអន្តរជាតិទូទៅ។
គោលគំនិតទាំង ៨ដែលបង្កើតបានសេចក្តីណែនាំនានារបស់ OECD ទៅលើការការពារឯកជនភាពគឺ:

១. គោលគំនិតនៃការកំណត់នៅដែនកំណត់សម្រាប់ការប្រមូលផ្តុំ

គឺគួរតែមានដែនកំណត់ដើម្បីការប្រមូលនៅទិន្នន័យជាលក្ខណៈបុគ្គលណាម្នាក់ និងទិន្នន័យខ្លះគួរតែបានធ្វើឡើងប្រកបដោយយុត្តិធម៌ និងស្របតាមច្បាប់ និងដែលមានលក្ខណៈសមរម្យជាមួយការដឹងលឺឬយល់ព្រមពីម្ចាស់ទិន្នន័យ។

២. គោលគំនិតនៃគុណសម្បត្តិទិន្នន័យ

ទិន្នន័យផ្ទាល់ខ្លួនគួរតែជាប់ទាក់ទងចំពោះគោលបំនងនានាដែលទិន្នន័យនោះត្រូវបានប្រើប្រាស់ និងការប្រើប្រាស់វាប្រកបដោយភាពមានប្រយោជន៍យ៉ាងធំធេងទៅលើគោលបំណងទាំងនោះ ហើយវាគួរតែប្រកបដោយភាពត្រឹមត្រូវ ភាពមិនខ្វះខាត ព្រមទាំងទាន់ពេលវេលាទៀតផង។

៣. គោលការណ៍នៅតាមច្បាស់លាស់ចំពោះគោលបំណង

គោលបំណងសម្រាប់ការប្រមូលនៅទិន្នន័យផ្ទាល់ខ្លួនគួរត្រូវតែប្រាកដថាមិនយឺតជាងពេលដែលទិន្នន័យត្រូវបានប្រមូល និងការប្រើប្រាស់នៅទិន្នន័យនោះដើម្បីបំពេញទៅតាមគោលបំណងដែលចង់បាន ឬក៏ដូចជាទិន្នន័យផ្សេងទៀតដែលមិនត្រូវគ្នាចំពោះគោលបំណង និងដូចជាមិនត្រូវបានធ្វើឲ្យជាក់ច្បាស់នៃដំណាក់កាលដែលវាផ្លាស់ប្តូររបស់គោលបំណងទាំងនោះ។

៤. គោលការណ៍លើដែនកំណត់នៃការប្រើប្រាស់

ទិន្នន័យផ្ទាល់ខ្លួនមិនគួរត្រូវបើកចំហ ត្រូវបានធ្វើឲ្យងាយស្រួលលើការយកបាន ឬម្យ៉ាងទៀតវាអាចត្រូវ បានប្រើប្រាស់ទៅលើហេតុផលផ្សេងៗច្រើនជាងការប្រើប្រាស់ទិន្នន័យនោះនៅក្នុងគោលការណ៍ជាក់លាក់ណាមួយ ប៉ុន្តែមានការលើកលែងចំពោះការប្រើប្រាស់ណាដែលមានការអនុញ្ញាតពីម្ចាស់ទិន្នន័យ ឬដោយអាជ្ញាធរច្បាប់។

៥. គោលការណ៍នៅការការពារសន្តិសុខ

ទិន្នន័យផ្ទាល់ខ្លួនគួរត្រូវបានការពារដោយការការពារសុវត្ថិភាពសន្តិសុខប្រកបដោយហេតុផលប្រឆាំងនឹងហានិភ័យដូចជាការបាត់បង់ ការលួចដំណើរនៅទិន្នន័យនោះ ការបំផ្លាញ ការប្រើប្រាស់ ការកែប្រែ ឬការផ្សព្វផ្សាយនៃទិន្នន័យទាំងនោះ។

៦. គោលការណ៍បើកចំហ

គឺគួរមានច្បាប់ទូទៅមួយនៃការបើកចំហសម្រាប់ការអភិវឌ្ឍន៍ ការអនុវត្តន៍ និង គោលការណ៍ច្បាប់នានាដែលទាក់ទងទៅនឹងទិន្នន័យផ្ទាល់ខ្លួន។ ជាមធ្យមវាគួរត្រូវធ្វើឲ្យរួចរាល់នៅភាពដែលអាចរកបានសម្រាប់ការបង្កើតចំពោះទិន្នន័យផ្ទាល់ខ្លួនដែលមានស្រាប់ និងភាពដើមរបស់វា ហើយគោលបំណងសំខាន់នៃការប្រើប្រាស់របស់ពួកគេដូចជាការកំណត់នៅអត្តសញ្ញាណ និងទីតាំងស្ថិតនៅធម្មតានៃឧបករណ៍ត្រួតពិនិត្យទិន្នន័យ។

៧. គោលការណ៍លើសិទ្ធិចូលរួមនៃបុគ្គលម្ចាក់ៗ

បុគ្គលម្នាក់ៗគួរមានសិទ្ធិ

A. ទទួលបានការបញ្ជាក់ពីឧបករណ៍ត្រួតពិនិត្យទិន្នន័យថាតើឧបករណ៍ត្រួតពិនិត្យទិន្នន័យនោះមានទិន្នន័យដែលគាត់ចង់បានដែរឬទេ

B. ទទួលបានការធ្វើទំនាក់ទំនងជាមួយទិន្នន័យដែលគាត់ចង់បាននៅក្នុងពេលវេលាដ៏សមរម្យមួយ ហើយ

C. ទទួលបាននៅហេតុផលនានាប្រសិនបើការស្នើសុំត្រូវបានធ្វើទៅតាមចំនុច (A) និង (B) ប៉ុន្តែ ត្រូវបានបដិសេធនោះ ហើយអាចមានសិទ្ធិតវ៉ាសម្រាប់ការបដិសេធនោះ

D. តវ៉ាចំពោះទិន្នន័យណាដែលគាត់ចង់បាន ហើយប្រសិនបើការតវ៉ានោះបានជោគជ័យគឺត្រូវមានសិទ្ធិក្នុងការសរុប កែប្រែ បំពេញបន្ថែម ឬក៏រៀបចំទៅលើទិន្នន័យនោះ

៨. គោលការណ៍ស្តីពីភាពឧទ្ធលខុសត្រូវ

ឧកបរណ៍ត្រួតពិនិត្យទិន្នន័យគួរតែទទួលខុសត្រូវសម្រាប់ការគោរពតាមវិធានការនានាដែលដូចបានចែងនៅក្នុងគោលកាណ៍ខាងលើ។[45]

សេចក្តីណែនាំរបស់អង្គការសហប្រជាជាតិ ដែលជាប់ពាក់ព័ន្ធទៅនឹងការការពារនៃឯកជនភាព

ចាប់តាំងពីចុងសតវត្សទី៦០មក ពិភពលោកបានគិតគូរចំពោះផលប៉ះពាល់លើឯកជនភាព និងដំណើរការព័ត៌មានដោយគ្មានការអនុញ្ញាត។ ជាពិសេស UNESCO បានបង្ហាញចំណាប់អារម្មណ៍នៅក្នុងឯកជនភាព និងការការពារលើឯកជនភាពចាប់តាំងពី <<សេចក្តីណែនាំនានារបស់អង្គការសហប្រជាជាតិសម្រាប់ភាពស្របច្បាប់ នៃការផ្ទុកទិន្នន័យផ្ទាល់ខ្លួនត្រូវបានធ្វើនៅក្នុងកុំព្យូទ័រ>> ត្រូវបានទទួលយល់ព្រមដោយសភាទូទៅនៅក្នុងឆ្នាំ ១៩៩០។សេចក្តីណែនាំបង្កើតនៅស៊េរីនៃគោលការណ៍ផ្សេងៗអំពីអប្បបរមាលើការធានាទាំងនោះដែលត្រូវបានផ្តល់សម្រាប់ច្បាប់ជាតិ ឬច្បាប់ផ្ទៃក្នុងនៃអង្គការអន្តរជាតិដូចខាងក្រោម:

45 To read the entire document where these principles are listed, see the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

១. គោលការណ៍នៃភាពត្រឹមត្រូវតាមច្បាប់ និងភាពមិនលំអៀង

ព័ត៌មានពីបុគ្គលម្នាក់ៗមិនគួរត្រូវបានគេប្រមូល ឬក៏ធ្វើប្រតិបត្តិលើដោយមធ្យោបាយដែលគ្មានលក្ខណៈស្របច្បាប់គឺស្ថិតក្នុងភាពអយុត្តិធម៌នោះទេ ឬក៏វាត្រូវបានប្រើប្រាស់ដើម្បីបញ្ចប់ជម្លោះចំពោះគោលការណ៍ និងគោលបំណងណាមួយនៃអង្គការសហប្រជាជាតិនោះទេ។

២. គោលការណ៍នៃភាពត្រឹមត្រូវ

បុគ្គលគ្រប់រូបទទួលខុសត្រូវសម្រាប់ការប្រមូលបញ្ចូលគ្នានៃបញ្ជីទិន្នន័យជាច្រើន ឬអ្នកទាំងនោះទទួលខុសត្រូវសម្រាប់ការរក្សាទុកពួកគេហើយមានកាតព្វកិច្ចធ្វើការត្រួតពិនិត្យជារឿយៗ ទៅលើភាពត្រឹមត្រូវ និងភាពជាប់ទាក់ទិនជាមួយទិន្នន័យដែលត្រូវបានថតរក្សាទុកហើយធានាថាទិន្នន័យទាំងនោះអាច រក្សាទុកបានយ៉ាងពេញលេញតាមដែលអាចធ្វើទៅបាន ដើម្បីចៀសវាងពីការខុសឆ្គងនៃការលុបវាចោល ព្រមទាំងធានាថាទិន្នន័យនោះគឺស្ថិតនៅពេលវេលាដែលមិនហួសកំណាត់ឬក៏នៅពេលពួកគេត្រូវបាននឹងកំពុងដំណើរការដោយនរណាម្នាក់នោះ ព័ត៌មានត្រូវតែមាននៅបញ្ជីទិន្នន័យទាំងនោះ។

៣. គោលការន៍នៃការធ្វើឲ្យជាក់ច្បាស់លើគោលបំណង

គោលបំណងក្នុងការរក្សាទុកបញ្ជីទិន្នន័យ និងការប្រើប្រាស់នៅបញ្ជីទិន្នន័យនោះនៅក្នុងកាលកំណត់នៃគោលបំណងទាំងនោះគួរត្រូវបានធ្វើឲ្យមានភាពច្បាស់លាស់ ត្រឹមត្រូវទៅតាមច្បាប់ និងនៅពេលវាត្រូវបានបង្កើត ទទួលបាននៅចំនួនដ៏ទៀងទាត់នៃការផ្សព្វផ្សាយ ឬត្រូវបាននាំយកទៅកាន់សតិកានៃភាពខ្វល់ខ្វាយរបស់បុគ្គលដើម្បីធ្វើឲ្យវាធាចប្រើប្រាស់ជាបន្តបន្ទាប់ក្រោយមក ត្រូវធានាថា:

a. រាល់ទិន្នន័យផ្ទាល់ខ្លួនដែលត្រូវបានប្រមូល និងត្រូវបានថតរក្សាទុកនោះទាមទារឲ្យមានភាពជាប់ទាក់ទង និងភាពគ្រប់គ្រាន់ទៅកាន់គោលគំនិតដែលបានកំណត់យ៉ាងច្បាស់។

b. មិនមានការនិយាយថាទិន្នន័យផ្ទាល់ខ្លួននេះគឺត្រូវបានគេប្រើប្រាស់ ឬក៏ផ្សព្វផ្សាយ ប៉ុន្តែអាចមានករណីលើកលែងចំពោះការប្រើប្រាស់ទិន្នន័យនោះ ក្នុងលក្ខណៈមិនដូចទៅនឹងគោលបំណងទាំងឡាយណាដែលមិនដូចអ្វីដែលបានកំណត់យ៉ាងជាក់ច្បាស់នោះ នៅពេលដែលមានការអនុញ្ញាតពីសាមីខ្លួនរបស់ទិន្នន័យនោះ។

c. រយៈកាលសម្រាប់ទិន្នន័យដែលត្រូវបានរក្សាទុក គឺមិនត្រូវឲ្យហួសពីសមិទ្ធិផលនៃគោលបំណងដូច ដែលត្រូវបានធ្វើឲ្យជាក់ច្បាស់នោះទេ។

៤. គោលការណ៍នៃដំណើរការលើសាមីជន

បុគ្គលរាល់គ្នាដែលផ្តល់ភស្តុតាងនៃអត្តសញ្ញាណជាកម្មសិទ្ធិ មានសិទ្ធិដើម្បីដឹងនៅព័ត៌មាននោះទោះជាព័ត៌មានដែលពួកគេបានដឹងកំពុងដំណើរការក៏ដោយ និងព្រមទាំងទទួលបានវាស្ថិតនៅទម្រង់ដ៏ងាយយល់ថែមទៀតដោយមិនមានការពន្យាពេល ឬចំណាយលើវាច្រើនហួសប្រមាណ ហើយមានសិទ្ធិកែតម្រូវតាមច្បាប់ មិនមានភាពសំខាន់ ឬការបញ្ចូលមិនត្រឹមត្រូវ និងនៅពេលដែលវាត្រូវបានគេទាក់ទងនោះ វាត្រូវបានបញ្ជាក់នៃអាស័យដ្ឋាននានា។

៥. គោលការណ៍នៃភាពមិនមានការរើសអើង

ប្រធានបទចំពោះករណីនានានៃការលើកលែងមួយចំនួនកាត់បន្ថយគិតពីអនាគត គឺត្រូវបានពិភាក្សានៅចំនុចទី៦ ហើយទិន្នន័យដែលទំនងជាឲ្យការងើបឡើងចំពោះភាពមិនត្រឹមត្រូវ ឬក៏ការរំលោភបំពានលើការរើសអើង រួមមានទាំងព័ត៌មានទៅលើការរើសអើងពូជសាសន៍ ជនជាតិដើមពណ៌សំបុរ ជីវិតនៃភេទ គំនិតនានាដែលទាក់ទងនឹងនយោបាយ ចិត្តសាស្ត្រ និងអ្វីផ្សេងៗទៀតដែលជឿជាក់ថាជាប់ពាក់ព័ន្ធ នឹងសមាគមន៍ ឬសហគមន៍ដឹកជញ្ជូនវាគួរត្រូវបានបញ្ចូលរួមគ្នាទេ។

៦. អំណាចធ្វើការលើកលែងនានា

ក្រៅពីគោលការណ៍ ១ ដល់ ៤ អាចត្រូវបានគេផ្តល់សិទ្ធិត្រឹមតែករណីណាដែលទង្វើនោះ គឺមានការចាំបាច់ចំពោះការការពារសន្តិសុខជាតិ តម្រូវការសាធារណៈ សុខមាលភាពសាធារណៈ ឬក៏ទាក់ទង

នឹង គុណធម៌អ្វីៗមួយ ដូចជាសិទ្ធិ និងសេរីភាពនៃបុគ្គលនៃ ជាពិសេសបុគ្គលទទួលរងការធ្វើបាប (ច្បាប់មនុស្សជាតិ) ត្រូវបានផ្តល់ដូចគោលការណ៍ទាំង ៤ដែលត្រូវបានបញ្ជាក់យ៉ាងច្បាស់នៅច្បាប់ ឬការប្រកាសនៃច្បាប់ដែលមានទំនាក់ទំនងជាមួយបញ្ហាទាំងនោះ ដោយយោងជាមួយប្រព័ន្ធច្បាប់ផ្ទៃក្នុងដែល បញ្ជាក់យ៉ាងច្បាស់នៅដែនកំណាត់ និងការបង្កើតការការពារដ៏សមរម្យលើកទី៤។

៧. គោលការណ៍នៃសន្តិសុខ

វិធានការដ៏សាកសមគួរត្រូវបានអនុវត្តន៍ដើម្បីការពារបញ្ជីទិន្នន័យ ប្រឆាំងទៅនឹងគ្រោះមហន្តរាយនានាបណ្តាលមកពីធម្មជាតិដ៏ដូចជាការបំផ្លាញ ឬការបាត់បង់ដោយឧបទ្ទវហេតុដោយសារមនុស្ស ដូចជាការដំណើរការលើទិន្នន័យដោយគ្មានការអនុញ្ញាត ការបន្លំនៃការប្រើប្រាស់ទិន្នន័យក្នុងទិសដៅខុស ឬក៏ការឆ្លងមេរោគលើកុំព្យូទ័រ។

៨. ការគ្រប់គ្រង និងការយល់ព្រម

ច្បាប់នៃប្រទេសនីមួយៗបានបង្កើតនៅអាជ្ញាធរ យោងជាមួយប្រព័ន្ធច្បាប់ផ្ទៃក្នុងដែលមានការទទួលសម្រាប់ការគ្រប់គ្រងលើការគោរពតាមគោលការណ៍ទាំង ៤ខាងលើ។ អាជ្ញាធរនេះ នឹងផ្តល់នៅការធានានៅភាពមិនលំអៀង ឯករាជ្យភាពក្នុងការទទួលខុសត្រូវចំពោះមុខ សម្រាប់ដំណើរការ និងការបង្កើតនៅទិន្នន័យ ព្រមទាំងការប្រកួតប្រជែងខាងបច្ចេកវិទ្យា។ នៅក្នុងហេតុការណ៍នៃការប្រឆាំង និងការអនុវត្តន៍នៅច្បាប់ជាតិចំពោះគោលការណ៍ច្បាប់ដែលបានប្រកាសរួច ច្បាប់ឧក្រិដ្ឋកម្ម ឬក៏ការដាក់ពិន័យផ្សេងៗ គួរធ្វើការរួមគ្នាឲ្យបានល្អជាមួយរបៀបកែខៃដ៏សាកសមដាច់ដោយឡែកពីគ្នា។

៩. ការហូរចូលនៅទិន្នន័យឆ្លងដែនកំណាត់

នៅពេលដែលច្បាប់ប្រទេសមួយ ឬក៏ច្រើនបានត្រូវធ្វើឲ្យខ្វល់ខ្វាយដោយការហូរចូលទិន្នន័យឆ្លងដែន កំណាត់នោះគឺការស្នើឲ្យមានការប្រៀបធៀបនៅការការពារនៃឯកជនភាពព័ត៌មានគួរអាចត្រូវ

បានធ្វើចរាចរយ៉ាងសេរីដូចជាស្ថិតនៅផ្នែកខាងក្នុងនៃដែនដីនីមួយៗ។ ប្រសិនបើគ្មានការសហការគ្នាទៅវិញទៅមកលើការការពារ និងការកំណត់នៅចរាចរនៃទិន្នន័យទាំងនោះទេ ប្រហែលជាមិនអាចគេចផុតពីការហូរចូលហួសប្រមាណនៃទិន្នន័យ និងដូចជានៅឆ្ងាយសម្រាប់ធ្វើការការពារនៅអ្វីដែលឯកជនទាមទារ។

១០.ដំណើរការប្រតិបត្តិនៃការស្នើសុំ

នៅក្នុងជំហានដំបូង គោលការណ៍បច្ចុប្បន្នគួរធ្វើនៅសេចក្តីស្នើសុំទៅកាន់ផ្នែកសាធារណៈ និងផ្នែកឯកជនឲ្យរក្សាទុកទិន្នន័យដោយកុំព្យូទ័រ ដែលវាមានភាពងាយស្រួលក្នុងការកែប្រែដែលធ្វើឡើងដោយដៃចំពោះបញ្ជីទិន្នន័យនោះ។ ច្បាប់សំខាន់នានាក៏ដូចជាជម្រើសផងដែរ សម្រាប់ការពង្រីកសេចក្តីទៅកាន់រាល់ ឬផ្នែកណាមួយនៃគោលការណ៍ចំពោះបញ្ជីទិន្នន័យរបស់បុគ្គលដែលមានសិទ្ធិធ្វើកិច្ចការលើវា ជាពិសេសនៅពេលដែលបញ្ជីទិន្នន័យនោះផ្ទុកនៅព័ត៌មាននៃបុគ្គលម្នាក់ៗ។[46]

សេចក្តីណែនាំជាផ្លូវការលើការការពារទិន្នន័យរបស់ EU

គណៈរដ្ឋមន្ត្រីរបស់ EU បានទទួលយក Euroupean Directive ចំពោះ Protection of Individuals ជាមួយRegard to Processing of Personal Data និងទៅលើ Free Movement នៃទិន្នន័យទាំង (EU Directivi) នៅថ្ងៃទី ២៤ ខែតុលា ឆ្នាំ១៩៩៥ ផ្តល់នៅគម្រោងស្របច្បាប់ដើម្បីរក្សាការធានា និងសេរីភាពនៃការផ្លាស់ប្តូរទិន្នន័យផ្ទាល់ខ្លួនឆ្លងកាត់ព្រំដែនជាតិនានា នៃប្រទេសជាសមាជិករបស់ EU បន្ថែមលើសនេះទៀត ដើម្បីជាការបង្កើតព្រំដែននៃសន្តិសុខជុំវិញព័ត៌មានផ្ទាល់ខ្លួននៅកន្លែងណាក៏ដោយដែលវាត្រូវបានរក្សា បញ្ជូន ឬដំណើរការ

EU Data Protection Directive ត្រូវបានបង្កើតនៅក្នុងកិច្ចខិតខំប្រឹងមួយដើម្បីបង្រួបបង្រួម និងធ្វើឲ្យមានសេចក្តីសុខជាមួយច្បាប់រាជការ ដែលជាប់ពាក់ព័ន្ធទៅនឹងការការពារឯកជនភាព។ មាត្រា១ EU Directive ប្រកាសថា “រដ្ឋដែលជាសមាជិកនឹងការពារសិទ្ធិជាមូលដ្ឋាន និងសេរីភាពនៃមនុស្សជាតិ និងជាពិសេសសិទ្ធិឯកជនរបស់ពួកគេជាមួយការគោរពចំពោះដំណើរការនៃទិន្នន័យផ្ទាល់ខ្លួន។”

46 The principles are quoted from the Office of the High Commissioner for Human Rights, “Guidelines for the Regulation of Computerized Personal Data Files,” http://www.unhchr.ch/html/menu3/b/71.htm.

EU Direct ហាមឃាត់ការបញ្ជូនព័ត៌មានផ្ទាល់ខ្លួនទៅកាន់ប្រទេសណាដែលមានកម្រិតនៃការការពារមិនគ្រប់គ្រាន់ នេះជាហេតុបណ្តាលឲ្យមានការប្រឆាំងគ្នារវាងរដ្ឋាភិបាល EU និង US។[47]

ជាតិជាសមាជិក EU និមួយបានធ្វើសារឡើងវិញនៅច្បាប់ដែលមានស្រាប់ផ្ទាល់ខ្លួន ឬក៏បង្កើតនៅច្បាប់ការពារឯកជនថ្មីដើម្បីប្រតិបត្តិទៅតាម EU Directive ។

ឧទាហរណ៍ផ្សេងទៀតនៃច្បាប់នានារបស់ EU អំពីការការពារឯកជនភាពគឺមាត្រា៨នៃអនុសញ្ញាអឺរ៉ុបស្តីពីសិទ្ធិមនុស្ស Directive 95/46/EC (Data Protection Directive) Directive 2002/58/EC (the e-Privacy Directive) និង Directive 2006/24/EC មាត្រា៥ (the Data Retention Directive)។[48]

ការការពារឯកជនភាពនៅក្នុងសាធារណរដ្ឋកូរ៉ែ

សាធារណរដ្ឋកូរ៉ែមានចំនួនច្រើនបំផុតនៃអ្នកប្រើប្រាស់ប្រព័ន្ធរលកសញ្ញានៅក្នុងពិភពលោក។នៅក្នុងពាក់កណ្តាលឆមាសទី១ក្នុងឆ្នាំ២០០៥ គឺមាន២៥ភាគរយនៃចំនួនប្រជាជន និង៧៥ភាគរយនៃផ្ទះដែលត្រូវបានចុះឈ្មោះប្រើប្រាស់ប្រព័ន្ធបណ្តាញរលកអាកាស។[49] សព្វថ្ងៃបណ្តាញរលកអាកាស និងបណ្តាញគមនាគមន៍ Wireless របស់សាធារណរដ្ឋកូរ៉ែគឺត្រូវបានទទួលស្គាល់ជាបណ្តាញមួយក្នុងចំណោមបណ្តាញដ៏ល្អបំផុតនៅក្នុងពិភពលោក។ ដូច្នេះរលកសញ្ញានៃការលេចចេញនៅព័ត៌មានផ្ទាល់ខ្លួននៅក្នុងប្រទេសបានកើនឡើងជាគំហុកនោះគឺស្នើឲ្យមានដំណោះស្រាយទាំងពីច្បាប់ និងខាងបច្ចេកវិទ្យា។

ទោះបីជាយ៉ាងណាក៏ដោយ រដ្ឋាភិបាលកូរ៉ែបានឆ្លើយតបយ៉ាងគ្រប់គ្រាន់ចំពោះបញ្ហាទាំងនេះ។ ច្បាប់ការពារឯកជនភាពទាមទារការរង់ចាំនៅក្នុងសភាជាតិ និងគឺគ្មានច្បាប់ឯករាជ្យណាស្តីពីការការពារព័ត៌មានផ្ទាល់ខ្លួន។

47 Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT'L & COMP. L.J. 661, 666 (1999).
48 Justice and Home Affairs, "Data Protection," European Commission, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
49 Internet World Stats, "Korea," Miniwatts Marketing Group, http://www.internetworldstats.com/asia/kr.htm.

ម្យ៉ាងវិញទៀត រដ្ឋាភិបាលកូរ៉េបានបង្កើង “Mid- and Long-term Information Security Roadmap for Realizing u-SafeKorea” និងគម្រោងចម្បងបួនធំៗរបស់វាចាប់តាំងពីឆ្នាំ ២០០៥ ដែលរួមមាន (១)ការធានារ៉ាប់រងលើសន្តិសុខនៃហេដ្ឋារចនាសម្ព័ន្ធទំនើប (២) ការបង្កើតភាពគួរឲ្យជឿទុកចិត្តនៅក្នុងសេវាកម្ម IT ថ្មីនានា (៣) ពង្រឹងមុខងារនានានៃការការពារព័ត៌មានសម្រាប់ការលូតលាស់ថ្មីនៃវិស្វកម្ម និង (៤) ការកសាងសន្តិសុខព័ត៌មានផ្អែកនៅក្នុងបរិដ្ឋានរលកសញ្ញាថ្មី។ គម្រោងចម្បងទី៤ រួមមានអនុគម្រោងដែលត្រូវបានហៅថា “ពង្រឹងប្រព័ន្ធការការពារឯកជនភាព”។

ភាពដូចជា “ច្បាប់ការពារព័ត៌មានផ្ទាល់ខ្លួននៅក្នុងសាធារណៈ” និង “ច្បាប់ស្តីពីការការពារព័ត៌មាន និងបណ្តាញទូរគមនគមន៍”

ច្បាប់ការការពារព័ត៌មានផ្ទាល់ខ្លួននៅក្នុងសាធារណៈ: ច្បាប់នេះរួមមានការផ្តល់នៅការកាន់កាប់ និងការគ្រប់គ្រងលើព័ត៌មានផ្ទាល់ខ្លួនដែលត្រូវបានដំណើរការនៅក្នុងប្រព័ន្ធកុំព្យូទ័រនាននៃវិទ្យាស្ថានសាធារណៈផ្សេងៗដែលសម្រាប់ការការពារឯកជនភាព ក៏ដូចជាការផ្សេងដែលទាក់ទងទៅនឹងការបង្កើតនៅជំនួញសាធារណៈ និងការការពារនៅសិទ្ធិ និងផលប្រយោជន៍របស់ប្រជាជន។

សកម្មភាពស្តីពីការជំរុញវិស័យព័ត៌មាន ការការពារព័ត៌មាននិងការបង្រួបបង្រួមបណ្តាញគមនាគមន៍:គោលបំណងនៃសកម្មភាពគឺធ្វើឲ្យប្រសើរឡើងប្រព័ន្ធការពារឯកជននៃវិស័យឯកជន ដោយអាស្រ័យលើការរីកចំរើនធំធាត់នៃបណ្តាញគមនាគមន៍ព័ត៌មាន និងការធ្វើឲ្យទូទៅនៃការប្រមូល និងចែកចាយនៃព័ត៌មានផ្ទាល់ខ្លួន។ សកម្មភាពខាងក្រោមគឺជាដំណើរការនៃការការពារឯកជនភាព ផ្អែកលើវឌ្ឍនកាលនៃអាយុរបស់ព័ត៌មានផ្ទាល់ខ្លួន ដូចជាការប្រមូលផ្តុំ ការប្រើប្រាស់ ការគ្រប់គ្រង និងការលុបចោល។ សកម្មភាពនេះផ្តល់នៅអ្វីដែលទាក់ទងទៅនឹងសិទ្ធិរបស់អ្នកប្រើប្រាស់នៃព័ត៌មានផ្ទាល់ខ្លួន និងការបង្កើត និងប្រតិបត្តនៃគណៈកម្មាធិការផ្សះផ្សាឯកជនភាព។

សកម្មភាពការការពារនៃការរក្សាការសម្ងាត់គមនាគមន៍:សកម្មភាពកំណត់លំដាប់ទិសដៅនៃឯកជនភាព និងសេរីភាពនៃគមនាគមន៍ដើម្បីការពារឯកជនភាពនៃគមនាគមន៍ និងធានាសេរីភាពនៃគមនាគមន៍។

ច្បាប់ហាមឃាត់ការលុកលុយនៃការសន្ទនាជាសម្ងាត់ដូចជាតាមរយៈការថតសម្លេង ឬក៏លួចស្តាប់ និងការពារឯកជនភាពនៅក្នុងការទំនាក់ទំនងគ្នាផ្សេងៗទៀត។

សកម្មភាពការពារព័ត៌មានតាមតំបន់: សកម្មស្វែងរកដើម្បីភាពស្របច្បាប់ក្នុងការប្រមូល និងប្រើប្រាស់នៅព័ត៌មានផ្តែកទៅតាមតំបន់។ ដើម្បីប្រឆាំងនឹងការលេខធ្លាយ ការប្រើខុស និងការចោទប្រកាន់នៃព័ត៌មានជំរុញឲ្យមានការប្រើប្រាស់ព័ត៌មាននៅក្នុងបរិស្ថានដែលមានសុវត្តិភាពមួយ។ ច្បាប់បានរៀបចំសមត្ថភាពនៃបច្ចេកវិទ្យាគមនាគមន៍សព្វថ្ងៃដើម្បីធ្វើការកំណត់តំបន់ដាច់ដោយឡែកៗ (ឧទាហរណ៍ដូចជាតាមរយៈ ទូរស័ព្ទដៃ) និងភាពពិតដែលលេចចេញនៃព័ត៌មានដែលអាចបង្កឲ្យមានការរំលោភបំពានលើឯកជនភាពធ្ងន់ធ្ងរ។ ដូច្នេះច្បាប់បានដើរតួនាទីមួយចំពោះការមិនផ្សព្វផ្សាយព័ត៌មានលើកលែងមានការស្នើណាមួយចេញពីច្បាប់។

ការការពារឯកជនភាពនៅក្នុងសហរដ្ឋអាមេរិក

US បានផ្តល់សកម្មភាពនានាលើកិច្ចការបារឯកជនទៅឲ្យទីផ្សារចាប់តាំងពីលក្ខ័ណ្ឌលើការគ្រប់គ្រងដូចជាច្រើនពេកដែលបានបណ្តាលឲ្យមានការរាំងស្ទះដល់សកម្មភាព e-commerce ជាលទ្ធផល ត្រារបស់ឯកជនភាពដូចជា Trust-e ឬ Better Business Bureau Online បានផុសឡើង និងច្បាប់នានាស្តីអំពីការការពារនៃឯកជនភាពគឺមិនត្រូវបានធ្វើសមាហរណកម្មជាមួយគ្នា។ សកម្មភាពឯកជននៃ ឆ្នាំ ១៩៧៤ ផ្តល់សម្រាប់ការការពារនៃព័ត៌មានឯកជននៅក្នុងវិស័យសាធារណៈក្នុងកំឡុងពេលដែលច្បាប់ផ្សេងៗដទៃទៀតគ្រប់គ្រងលើឯកជនភាពនៅក្នុងវិស័យឯកជន។ គឺគ្មានការរៀបចំដោះស្រាយជាមួយរាល់បញ្ហានៃការការពារឯកជនភាពនៅក្នុងវិស័យឯកជននោះទេ។នៅក្នុងវិស័យសាធារណៈ ការិយាល័យនៃការគ្រប់គ្រង និងថវិកា (OMB) ដើរតួនាទីនៅក្នុងការបង្កើតគោលការណ៍ច្បាប់ឯកជនរបស់រដ្ឋាភិបាលសហព័ន្ធយោងទៅតាមសកម្មភាពឯកជន។ នៅក្នុងវិស័យដែលការពារឯកជនភាព Online របស់កុមារព័ត៌មានឥណទានរបស់អតិថិជន និងការអនុវត្តន៍នៅការដឹកជញ្ជូនស្មើភាពគ្នា។

ច្បាប់នានារបស់ US ដែលមានការជាប់ពាក់ព័ន្ធទៅលើការការពារឯកជនភាពរួមមាន:

- The Privacy Act, 1974
- Consumer Credit Protection Act, 1984

- Electric Communications Privacy Act, 1986
- Gramm-Leach-Bliley Act, 1999
- Health Insurance Portability and Accountability Act, 1996
- Sarbanes-Oxley Act, 2002
- Children's Online Privacy Protection Act, 1998

វិធានការការពារឯកជនភាពនានានៅក្នុងប្រទេសជប៉ុន

នៅក្នុងឆ្នាំ ១៩៨២ ជប៉ុនបានបង្កើតវិធានការការពារឯកជនភាពផ្អែកលើគោលការណ៍គ្រឹះទាំង ៨នៃ OECD។ នៅក្នុងឆ្នាំ 1998 ច្បាប់សម្រាប់ការការពារឯកជនភាពនៅក្នុងវិស័យសាធារណៈត្រូវបានប្រកាសឲ្យប្រើប្រាស់ និងបានចូលជាធរមាន។ នៅក្នុងវិស័យឯកជន សេចក្តីណែនាំសម្រាប់ការការពារនៃឯកជនភាពត្រូវបានចែកឲ្យប្រើដោយក្រសួងឧស្សាហកម្ម និងដឹកជញ្ជូនអន្តរជាតិនៅក្នុងឆ្នាំ ១៩៩៧។ ដើម្បីធ្វើឲ្យប្រសើរឡើងនៅភាពស្របគ្នានៃច្បាប់នេះ ជាតិផ្សេងៗជាមួយសេចក្តីណែនាំអន្តរជាតិនានា បញ្ជាការដ្ឋាន ការជំរុញសង្គមទូរគមនាគមន៍ និងព័ត៌មានពិសេសនឹងកំពុងជំរុញសម្រាប់ការតែងច្បាប់នៃច្បាប់ការពារព័ត៌មានផ្ទាល់ខ្លួន។

បន្ថែមលើនេះទៀត អាជ្ញាធរការពារទិន្នន័យត្រូវបានបង្កើតឡើងជាភ្នាក់ងារឯករាជ្យមួយដែល នឹងធានាឲ្យមានការគោរពប្រតិបត្តិដោយត្រឹមត្រូវ និងជួយដល់បុគ្គលម្នាក់ៗនៅក្នុងករណីមានការឈ្លានពានលើឯកជនភាពរបស់ពួកគេ។ អាជ្ញាធរការពារទិន្នន័យត្រូវបានគេប្រគល់សិទ្ធិដើម្បីធ្វើឲ្យប្រសើរឡើងលើដំណើរការព័ត៌មានប្រកបដោយភាពបរិសុទ្ធ, ការធានារ៉ាប់រងនៅផលប្រយោជន៍, និងសិទ្ធិនានារបស់កម្មវត្ថុទិន្នន័យ, និងធានាថាទាំងភ្នាក់ងារប្រតិបត្តិទិន្នន័យ និងអ្នកប្រើប្រាស់ព័ត៌មានធ្វើទៅតាមតួនាទីរបស់ពួកគេ។ អាជ្ញាធងដែរត្រូវបានរំពឹងថានឹងដើរតួនាទីដើម្បីការពារផលប្រយោជន៍ជាតិ ជាពិសេសនៅក្នុងករណីផ្សេងៗដែលជាប់ពាក់ព័ន្ធទៅនឹងការបញ្ជូនព័ត៌មានកាត់តាមព្រំដែនជាតិនានា។

ច្បាប់របស់ ប្រទេសជប៉ុនដែលជាប់ទាក់ទងទៅនឹងការការពារនៃឯក ជនភាពរួមមានដូចខាងក្រោម:

- Act for the Protection of Computer Processed Personal Data Held by Administrative Organs 1988
- Regulations of Local Governments (enacted in 1999 for 1,529 local governments)
- Act for the Protection of Personal Information, 2003
- Act on the Protection of Personal Information Held by Administrative Organs, 2003
- Act for the Protection of Personal Information Retained by Independent Administrative Institutions, 2003
- Board of Audit Law, 2003
- Guidelines for Privacy Protection with regard to RFID Tags, 2004

សំនួរត្រិះរិះ

១. នៅក្នុងប្រទេសរបស់អ្នក តើគោលការណ៍ច្បាប់ និងច្បាប់នានាគឺមានការការពារឯកជនភាពនៃព័ត៌មានដែរឬទេ?

២. តើមានបញ្ហាឬការគិតណាខ្លះដែលប្រឆាំងទៅលើការអនុម័ត និងការអនុវត្តន៍នៃគោលការណ៍ និងច្បាប់ទាំងនោះឬទេ។

៣. តើគោលការណ៍ណាខ្លះ (គោលការណ៍ច្បាប់ដែលបានរៀបរាប់មកនៅក្នុងសេចក្តីណែនាំនានារបស់ OECD និង UN) ដែលអ្នកគិតថាគាំទ្រច្បាប់ និងគោលការណ៍ច្បាប់ទាំងនោះចំពោះការការពារឯកជនភាពនៅក្នុងប្រទេសរបស់អ្នក?

៥.៣ ការប៉ាន់ប្រមាណលើផលប៉ះពាល់ឯកជនភាព

អ្វីគឺជា PIA?

PIA គឺជាដំណើរការបែបប្រព័ន្ធលក្ខណៈនៃការស៊ើបអង្កេត ការវិភាគ និងការវាយតម្លៃនៅផលប៉ះពាល់ទៅលើឯកជនភាពរបស់អ្នកប្រើប្រាស់ ឬរបស់ជាតិជំពោះសេចក្តីណែនាំនៃប្រព័ន្ធព័ត៌មានថ្មីៗនានាឬការកែប្រែលើប្រព័ន្ធព័ត៌មានដែលមានស្រាប់ផ្សេងៗ។ PIA គឺសំដៅលើ "គោលការណ៍នៃការការពារដំបូងឧទាហរណ៍ ការការពារប្រសើរជាងព្យាបាល"។ វាមិនប្រាកដជាប្រព័ន្ធវាយតម្លៃមួយនោះទេ

ប៉ុន្តែវាពិនិត្យពិច័យលើផលប៉ះពាល់ធ្ងន់ធ្ងរទៅលើឯកជនភាពចំពោះ សេចក្តីណែនាំ ឬចំពោះការផ្លាស់ប្តូរនៅប្រព័ន្ធថ្មី។ ដូច្នេះវាគឺផ្សេងពីសារនកម្មការការពារឯកជនភាពដែលធានានៅការប្រតិបត្តិតាមនៃគោលការណ៍ច្បាប់ផ្ទៃក្នុង និងសេចក្តីស្នើសុំខាងក្រៅផ្សេងៗទៀតសម្រាប់ឯកជនភាព។

ពីព្រោះតែ PIA គឺត្រូវបានអនុវត្តន៍ទៅលើការវិភាគចំពោះកត្តាឈ្លានពានលើឯកជនភាពនៅពេលដែលប្រព័ន្ធថ្មីគឺត្រូវបានកសាងឡើង វាគួរតែត្រូវបានធ្វើនៅឯងមុនពេលនៃការអភិវឌ្ឍន៍ហើយនៅពេលមានការកែប្រែចំពោះការអភិវឌ្ឍន៍នានាគឺនៅតែអាចដំណើរការទៅបាន។ ទោះបីជាយ៉ាងណាក៏ដោយនៅពេលមានហានិភ័យដោយការឈ្លានពានដ៏ធ្ងន់ធ្ងរនោះកើតឡើងក្នុងពេលកំពុងប្រមូល កំពុងប្រើប្រាស់ និងកំពុងតែគ្រប់គ្រងលើព័ត៌មានផ្ទាល់ខ្លួនខណៈពេលមានការអនុវត្តន៍នៅសេវាកម្មដែលមានស្រាប់នោះ និងត្រូវបានធ្វើការសម្រេចចិត្តដើម្បីបង្កើតនៅ PIA និងបន្ទាប់មកកែប្រែលើប្រព័ន្ធភ្លាមៗ។

ដំណើរការរបស់ PIA [50]

ដំណើរការទូទៅរបស់ PIA រួមមាន៣ដំហាន: (តារាងលេខ១០)

តារាងលេខ១០.ដំណើរការរបស់ PIA

ការវិភាគជាលក្ខណៈមូលដ្ឋាន	ការវិភាកលើការចរាចររបស់ទិន្នន័យ	តាមដានលើការវិភាគ
រៀបចំជាភាសាគម្រោងមួយពិពណ៌នាពីរយៈពេល និងហេតុផល របស់កិច្ចការជំនួញនៅពេលដំបូងនៃការស្នើសុំ។ កំណត់នៅមធ្យោបាយដំបូងលើបញ្ហា និងហានិភ័យនានារបស់ឯកជនភាបនៅមិនទាន់លេចឡើងព្រមទាំង ភាគហ៊ុនសំខាន់ៗ	វិភាគចរាចរទិន្នន័យតាមរយៈដ្យាក្រាមដំណើរការរបស់ពាណិជ្ជកម្ម និងកំណត់នៅធាតុទិន្នន័យផ្ទាល់ខ្លួនដ៏ជាក់លាក់ ឬចង្កោមនៃទិន្នន័យ ធ្វើការប៉ាន់ប្រមាណលើភាពត្រូតគ្នារបស់សេចក្តីស្នើសុំជាមួយសេរីភាពនៃព័ត៌មាន (FOI) និងការតែងនៅច្បាប់ឯកជនភាពព្រមទាំងរូបរាងកម្មវិធីដែលជាប់ពាក់ព័ន្ធនានា។ធ្វើការប៉ាន់ប្រមាណទៅលើសភាពដូច	សង្ខេប និងវិភាគលើផ្នែករឹងពិតៗនិងរៀបចំប្រព័ន្ធនៃគំនិតដំបូងដែលបានស្នើឡើងដើម្បីធានានៅភាពយល់ស្របជាមួយសេចក្តីត្រូវការ នានាក្នុងការរៀបចំឯកជនភាព។ ផ្តល់នៅការសង្ខេបចុងក្រោយលើគំនិតដំបូង ដែលត្រូវបានស្នើ។

50 This section is drawn from Information and *Privacy Office, Privacy Impact Assessment: A User's Guide* (Ontario: Management Board Secretariat, 2001), http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

ផ្តល់នៅការពិពណ៌នាលម្អិតនៃទ្រង់ទ្រាយសំខាន់ៗរបស់សេចក្តីស្នើសុំ រួមមានទាំងការវិភាគរបស់គោលការណ៍ច្បាប់នៃបញ្ហាធំៗ ឯកសារពីការហូរចូលដ៏ច្រើនលើសលប់នៃព័ត៌មានផ្ទាល់ខ្លួន ប្រមូលផ្តុំការវិភាគនៅបញ្ហានានាដើម្បីសង្ខេបរបៀបម៉ែចដែលការកាត់ក្តីផ្សេងទៀតបានបកស្រាយ ចំពោះគំនិតស្រដៀងគ្នានេះ។ ការខ្វល់ខ្វាយនានារបស់ភាគហ៊ុន ប៉ាន់ប្រមាណមើលប្រតិកម្មតបរបស់សាធារណៈ។	ទូទៅជាមួយគោលការណ៍ឯកជនភាពទូទៅ។ វិភាគលើហានិភ័យដោយផ្តែកលើការវិភាគលើឯកជនភាពនៃពេលដំបូង និងកំណត់នៅដំណោះស្រាយដែលអាចទៅរួច។ សង្ខេបនៅជំរើសនានាលើការរៀបចំ និងកំណត់នៅភាពជាប់ទាក់ទងបញ្ហានានារបស់ឯកជនភាពសំខាន់ៗដែលមិនបានគិតចំពោះ។ រៀបចំនៅការឆ្លើយតបមួយសម្រាប់បញ្ហាឯកជនភាពមួយចំនួនដែលមិនអាចដោះស្រាយបាន។	អនុវត្តន៍ឯកជនភាពមួយ និងវិភាគលើហានិភ័យនៃការផ្លាស់ប្តូរថ្មីខ្លះចំពោះដើមគំនិតដំបូងដែលបានស្នើឡើង ដែលជាប់ពាក់ព័ន្ធទៅនឹងការរៀបចំផ្តែករឹង និងទន់ដើម្បីធានាភាពត្រូវគ្នាជាមួយ FOI និងការតែងច្បាប់ឯកជនភាព ភាពជាប់ទាក់ទងគ្នានឹងកម្មវិធីនិងគោលការណ៍ឯកជនទូទៅ។ រៀបចំនៅគម្រោងគមនាគមន៍នានា។

Source: Information and Privacy Office, *Privacy Impact Assessment: A User's Guide* (Ontario: Management Board Secretariat, 2001), 5, http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

ការប៉ាន់ប្រមាណលើរយៈពេលនៃដំណើរការ PIA

PIA គឺត្រូវបានធ្វើឡើងនៅពេល

១. កសាងនៅប្រព័ន្ធមានថ្មីដែលនឹងក្តោបនឹងគ្រប់គ្រងលើបរិមាណដ៏ធមួយនៃព័ត៌មានផ្ទាល់ខ្លួន។
២. ប្រើប្រាស់នៅបច្ចេកវិទ្យាថ្មីនៅកន្លែងដែលឯកជនភាពអាចត្រូវបានគេវាយប្រហារ។
៣. ធ្វើការកែប្រែលើប្រព័ន្ធដែលមានស្រាប់ដែលកាន់កាប់ និងគ្រប់គ្រងលើព័ត៌មានផ្ទាល់ខ្លួន និង

៤. ការប្រមូលផ្តុំ ការប្រើប្រាស់ ការរក្សាទុក និង ការបំផ្លាញចោលនៅព័ត៌មានផ្ទាល់ខ្លួនកំឡុងពេលដែលហានិភ័យមួយនៃការលុកលុយលើកងកជនភាពកើតឡើង។

ប៉ុន្តែវាមិនចាំបាច់ដើម្បីអនុវត្តន៍នៅ PIA ចំពោះរាល់ប្រព័ន្ធព័ត៌មានទេ។ PIA គឺមិនត្រូវបានធ្វើឡើងទេនៅពេលដែលគ្រាន់តែមានការផ្លាស់ប្តូរបន្តិចបន្តួចនៃកម្មវិធី និងប្រព័ន្ធដែលមានស្រាប់នោះទេ។

ឧទាហរណ៍នានៃ PIAs

តារាងលេខ១១រាយនៅប្រព័ន្ធ PIA ផ្សេងៗនៅក្នុងប្រទេសចំនួនបី។

តារាងលេខ១១.ឧទាហរណ៍នៃ PIAs ជាតិ

	សហរដ្ឋអាមេរិក	**កាណាដា**	**អូស្ត្រាលី/ញ៉ូហ្សេឡែន**
មូលដ្ឋានស្របច្បាប់	ផ្នែក២០៨នៃសកម្មភាព e-government ក្នុងឆ្នាំ ២០០២ OMB ផ្តល់នៅសេចក្តីត្រូវការរបស់ PIA នៅក្នុង OMB –M-03-22	បានណែនាំពីគោលការណ៍ច្បាប់និងសេចក្តីណែនាំ PIA របស់ខ្លួននៅក្នុងខែឧសភា ឆ្នាំ ២០០២ ប្រតិបត្តិដោយខានមិនបាននៃ PIA ទៅលើមូលដ្ឋានគ្រឹះនៃច្បាប់ធម្មតាលើឯកជនភាព។	អនុវត្តន៍យ៉ាងស្ម័គ្រចិត្តនៃ PIA (គ្មានច្បាប់ពិត) សៀវភៅក្បួនច្បាប់របស់ PIA សម្រាប់ការគាំទ្រលើ PIA (២០០៤ ញ៉ូហ្សេឡែន) សេចក្តីណែនាំសម្រាប់ PIA (២០០៤ អូស្ត្រាលី)
កម្មវត្ថុ	រាល់ភ្នាក់ងារ និងនាយកដ្ឋានសាខាប្រតិបត្តិព្រមទាំងអ្នកធ្វើកិច្ចសន្យាដែលប្រើប្រាស់ IT ឬដែលប្រើនៅគេហទំព័រនានាសម្រាប់គោលបំណងធ្វើការទំ	រាល់កម្មវិធី និងសេវាកម្មដែលភ្នាក់ងាររដ្ឋាភិបាលផ្តល់ឲ្យ	គ្មានការកិច្ច ឬក៏ដែនកំណត់ចំពោះការប្រើប្រាស់

	នាក់ទំនងជាមួយសាធារណៈ ភ្នាក់ងារកាកបាទក្រហមរួមទាំងភ្នាក់ងារដែលស្ថិតនៅឆ្ងាយពី e-government		
អ្នកអនុវត្តន៍	ភ្នាក់ងារនានាដែលបានធ្វើនៅគម្រោង e-government ក្នុងការដោះស្រាយជាមួយព័ត៌មានផ្ទាល់ខ្លួន។	ភ្នាក់ងាររដ្ឋាភិបាលទទួលបន្ទុកលើការអភិវឌ្ឍន៍ និងការអនុវត្តន៍នៃកម្មវិធី និងសេវាកម្មនានា។	ភ្នាក់ងារដែលជាប់ពាក់ព័ន្ធ ឬដោយការស្នើសុំពីភ្នាក់ងារប្រឹក្សាខាងក្រៅ។
Publication ការផ្សព្វផ្សាយ	ធ្វើឲ្យ PIA អាចរកបាននៅទីកន្លែងសាធារណៈតាមរយៈ គេហទំព័រនៃភ្នាក់ងារ ការផ្សព្វផ្សាយនៅក្នុងពេលចុះឈ្មោះនៃសហព័ន្ធ ឬមធ្យោបាយផ្សេងទៀតដែលត្រូវបានគេកែប្រែឬលែងតែហេតុផលសន្តិសុខដើម្បីការការពារព័ត៌មានដែលត្រូវបានកម្រិត ឬព័ត៌មានឯកជនដែលមាននៅក្នុងការប៉ាន់ប្រមាណណាមួយ។ ភ្នាក់ងារទាំងឡាយនឹងផ្តល់ Director of OMB ជាមួយច្បាប់ចម្លងនៃ PIA សម្រាប់ប្រព័ន្ធនិមួយៗដែលទៅតាមចំនួនទឹកប្រាក់ដែលត្រូវបានស្នើសុំ	ធ្វើនៅសេចក្តីសង្ខេបពី PIA ដែលអាចរកបាននៅតាមសាធារណៈ។ ផ្តល់កនៅច្បាប់ថតចម្លងពីចុងក្រោយនៃ PIA និងរាយការណ៍ទៅកាន់ការិយាល័យនៃគណៈកម្មធិការឯកជននៅក្នុងភាពចាំបាច់ដើម្បីទទួលបាននៅដំបូន្មាន ឬសេចក្តីណែនាំសមរម្យមួយរួមទាំងការធ្វើតាមនៅយុទ្ធសាស្ត្រការពារដ៏សមរម្យនោះ។	លទ្ធផលនៃ PIA គឺជារឿយៗមិនអាចរកបានជាសាធារណៈ (គ្មានការរាយការណ៍ ឬនិងផ្សព្វផ្សាយ)

សាកល្បងខ្លួនឯង

១. តើព័ត៌មានផ្ទាល់ខ្លួន ខុសពីព័ត៌មានផ្សេងទៀតដូចម្តេច?

២. ហេតុអ្វីបានជាព័ត៌មានផ្ទាល់ខ្លួនគួរត្រូវបានគេការពារ?

៣. អ្វីគឺជាចំនុចសំខាន់នៃគោលការណ៍នានារបស់ OECD និង UN ស្តីពីគោលការណ៍ច្បាប់ការការពារ?

៤. ហេតុអ្វីបានជាការប៉ាន់ប្រមាណលើផលប៉ះពាល់ឯកជនភាពត្រូវបានធ្វើ?

៦.០ ការបង្កើត និងការប្រតិបត្តិ CSIRT

ចំនុចនេះមា៉ននគោលបំណង

- **ពន្យល់របៀបបង្កើត និងប្រតិបត្តិនៃក្រុមទទួលខុសត្រូវលើឧប្បទ្ទវហេតុសន្តិសុខជាតិលើកុំព្យូទ័រ (CSIRT) និង**
- **ផ្តល់នៅគំរូនានានៃ CSIRT ពីប្រទេសជាច្រើន**

រលកសញ្ញាឧក្រិដ្ឋកម្ម និងការគំរាមកំហែងនានាចំពោះសន្តិសុខព័ត៌មានបានក្លាយជាភាពធ្ងន់ធ្ងរដោយសារតែ ផលប៉ះពាល់លើសេដ្ឋកិច្ចមានភាពធំធេង។ ជាឧទាហរណ៍ សមាគមន៍សន្តិសុខបណ្តាញនៃប្រទេសជប៉ុន បានធ្វើការវាយតម្លៃលើការខាតបង់របស់សេដ្ឋកិច្ចពីការហូរចេញនៅព័ត៌មានឯកជនប្រហែល ៤៤៦លានដុល្លា ឬ ៣៤៧ដុល្លាសម្រាប់មនុស្សម្នាក់នៅក្នុងឆ្នាំ ២០០៦។ វិទ្យាស្ថានស្រាវជ្រាវ Ferris បានវាយតម្លៃលើការខូចខាតនានាបណ្តាលពី Spam នៅក្នុង US មានប្រហែល ៨.៩ រយកោដិដុល្លារក្នុងឆ្នាំ ២០០២ ២០រយកោដិដុល្លាក្នុងឆ្នាំ ២០០៤ និង ៥០រយកោដិដុល្លា ក្នុងឆ្នាំ ២០០៥។

ការបង្កើត CISRT គឺជាមធ្យោបាយដ៏មានប្រសិទ្ធិភាពមួយនៃការរារាំង និងការបំផ្លាញស្ថិតក្នុងកម្រិតអប្បបរមាពីការវាយប្រហារចំពោះប្រព័ន្ធព័ត៌មាននានា និងការធ្វើឲ្យបែកបាក់នៅសន្តិសុខព័ត៌មាន។

៦.១ ការអភិវឌ្ឍន៍ និងការអនុវត្តន៍នៃ CSIRT

CSIRT គឺជាអង្គការមួយដែលត្រូវបានដឹងថាដូចដូចនោះឬក៏ពិសេស ដែលទទួលខុសត្រូវសម្រាប់ការទទួលការធ្វើឡើងវិញ និងការឆ្លើយតបចំពោះការធ្វើសកម្មភាព និងរាយការន៍ពីឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រ។ គោលបំណងជាមូលដ្ឋាននៃ CSIRT គឺផ្តល់នៅសេវាកម្មនានាគ្រប់គ្រងលើឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រឲ្យស្ថិតក្នុងកម្រិតទាបនៃការបំផ្លាញ និងអនុញ្ញាតឲ្យមានការស្តារឡើងវិញពីឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រ។[51]

នៅក្នុងឆ្នាំ ១៩៨៨ ការកើតឡើងជាដំបូងនៅ Worm បានលេចឡើង និងបានចែកចាយជាបន្តបន្ទាប់នៅជុំវិញ ពិភពលោក។ បន្ទាប់ពីនេះ ភ្នាក់ងារគម្រោងស្រាវជ្រាវដ៏សំខាន់លើការការពារបានស្ថាបនា វិទ្យាស្ថាន

51 CERT, "CSIRT FAQ," Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.

វិស្វកម្ម Software និងបន្ទាប់មកទៀតបានបង្កើត CERT/CC នៅឯមហាវិទ្យាល័យ Carncgie Mellon ក្រោមកិច្ចសន្យារដ្ឋាភិបាលសហរដ្ឋអាមេរិក។ ចាប់តាំងពីនោះមក ប្រទេសនិមួយៗនៅអឺរ៉ុបបានបង្កើតនៅស្ថាប័នស្រដៀងគ្នា។ ចាប់តាំងពីពេលនោះមកមិនមែនមានតែ CSIRT តែមួយប៉ុណ្ណោះ ទេដែលអាចដោះស្រាយនៅឧប្បទ្ទវហេតុងាយរងគ្រោះជាទូទៅនោះ ហើយថវិការនៃការទទួលខុសត្រូវលើឧប្បទ្ទវហេតុ និងក្រុមសន្តិសុខ (FIRST) ត្រូវបានបង្កើតឡើងក្នុងឆ្នាំ ១៩៨០។ តាមរយៈ FIRST ភ្ជាក់ងារសន្តិសុខព័ត៌មានជាច្រើន និង CSIRT អាចផ្លាស់ប្តូរគំនិត និងចែករំលែកព័ត៌មានគ្នាទៅវិញទៅមក។

ការជ្រើសរើសនៅគំរូ CSIRT **ដែលត្រឹមត្រូវ**[52]

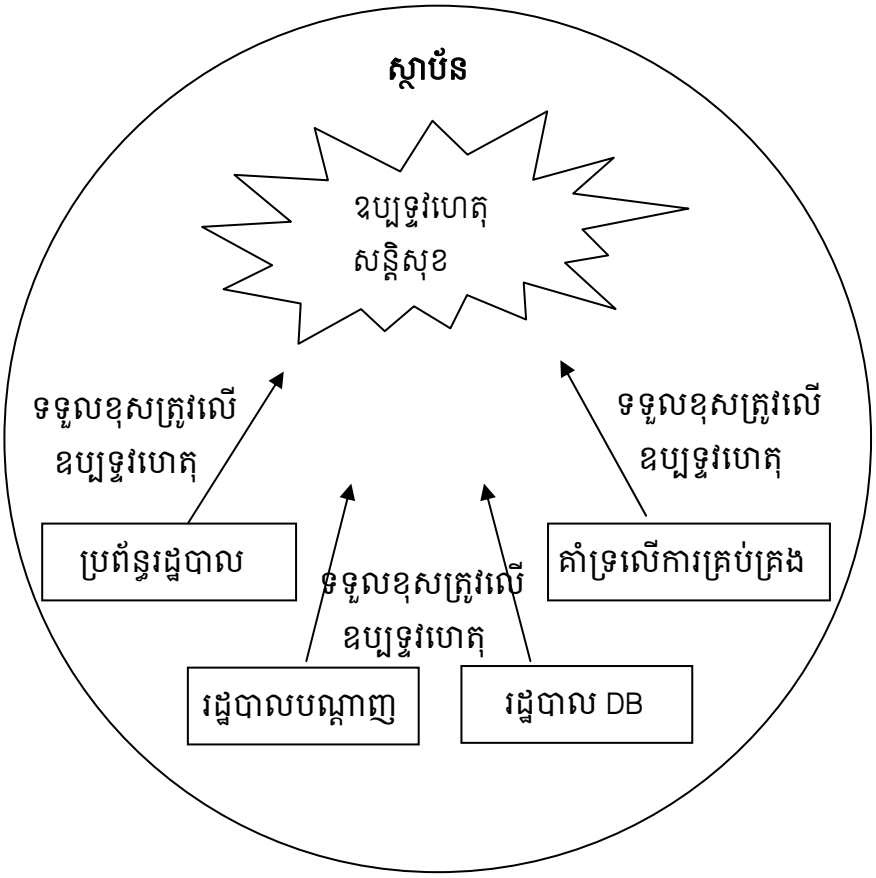
គឺមានប្រាំគំរូដែលត្រូវបានស្គាល់ជាទូទៅសម្រាប់ CSIRTs។ គំរូមួយដែលមានភាពសាកសមបំផុតចំពោះស្ថាប័នមួយ ឧទាហរណ៍គិតចំពោះលក្ខខណ្ឌផ្សេងដូចជាបរិស្ថាន លក្ខណៈហិរញ្ញវត្ថុ និងធនធានមនុស្សគួរត្រូវបានគេទទួលយក។

១. **គំរូក្រុមសន្តិសុខ** (**ប្រើប្រាស់សម្រាប់បុគ្គលិក** IT **ដែលមានស្រាប់**)

គំរូក្រុមសន្តិសុខវាគឺមិនមែនជាប្រភេទគំរូ CSIRT ពិតណាស់វាគឺផ្តុំយពីគំរូ CSIRT។ នៅក្នុងគំរូនេះគឺមិនមានការរៀបចំនៅផ្នែកកណ្តាលដែលការទទួលខុសត្រូវទៅលើការគ្រប់គ្រងឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រជំនួស មកវិញកិច្ចការកាន់កាប់ឧប្បទ្ទវហេតុត្រូវបានធ្វើដោយប្រព័ន្ធ និងរដ្ឋបាលបណ្តាញ ឬដោយអ្នកជំនាញប្រព័ន្ធសន្តិសុខដទៃទៀត។

52 This section is drawn from Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

រូបទី១៤.គំរូក្រុមសន្តិសុខ



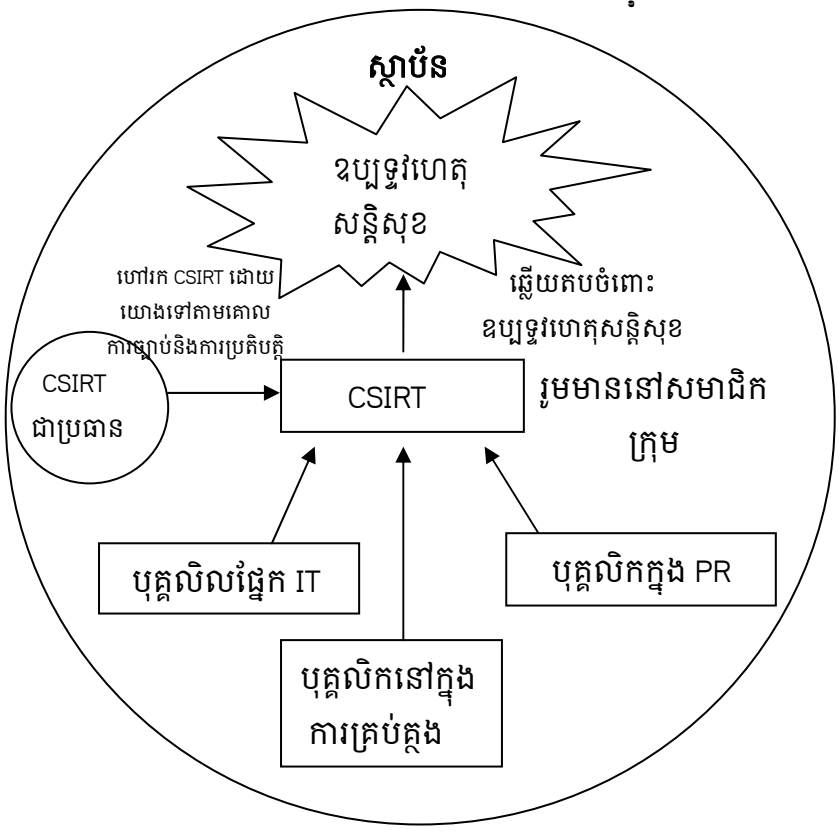
២. Internal Distrubuted CSIRT Model (**គំរូ** CSIRT **ចែកចាយខាងក្នុង**)

គំរូនេះគឺសំដៅផងដែរទៅរក "ការចែកចាយ CSIRT" ក្រុមនៅក្នុងគំរូនេះគឺត្រូវបានរៀបចំឡើងដោយមានផ្នែករដ្ឋបាល CSIRT ដែលទទួលខុសត្រូវសម្រាប់ការរាយការណ៍ និងរាល់ការគ្រប់គ្រងទាំងអស់ និងបុគ្គលិកពីផ្នែកតូចៗផ្សេងទៀតនៃសហគ្រាសនិងភ្នាក់ងារ។ CSIRT នៅក្នុងគំរូនេះគឺជាស្ថាប័នមួយដែលត្រូវបានទទួលស្គាល់ជាផ្លូវការជាមួយភាពទទួលខុសត្រូវសម្រាប់ការកាន់កាប់ រាល់សកម្មភាពឧប្បទ្ទវហេតុនានា។ ដូច្នេះក្រុមនៃគំរូនេះគឺគេកសាងឡើងដូចជាក្រុមហ៊ុន ឬ ភ្នាក់ងារមួយដែលធ្វើការនៅផ្នែកខាងក្នុង។

គំរូ CSIRT ចែកចាយខាងក្នុង (Internal Distrubuted CSIRT Model) គឺផ្សេងពីគំរូសន្តិសុខ (Security Team Model) ដូចខាងក្រោម៖

- មាននៅទម្រង់គ្រប់គ្រងលើឧប្បទ្ទវហេតុដែលមានទាំងគោលការណ៍ច្បាប់ វិធានការ និងដំណើរការផ្សេងៗ
- យុទ្ធវិធីត្រូវបានបង្កើតឡើងឲ្យមានទំនាក់ទំនងជាមួយការគិតគូពីការគំរាមកំហែងនានាលើសន្តិសុខសហគ្រាសដើម្បីឆ្លើយតបទៅនឹងការគំរាមកំហែងនោះ
- CSIRT ត្រូវបានរៀបចំឡើងដោយមានជាផ្នែកគ្រប់គ្រង និងសមាជិកក្រុមដែលមានការងារកំណត់ជាក់ច្បាស់រៀងៗខ្លួន។

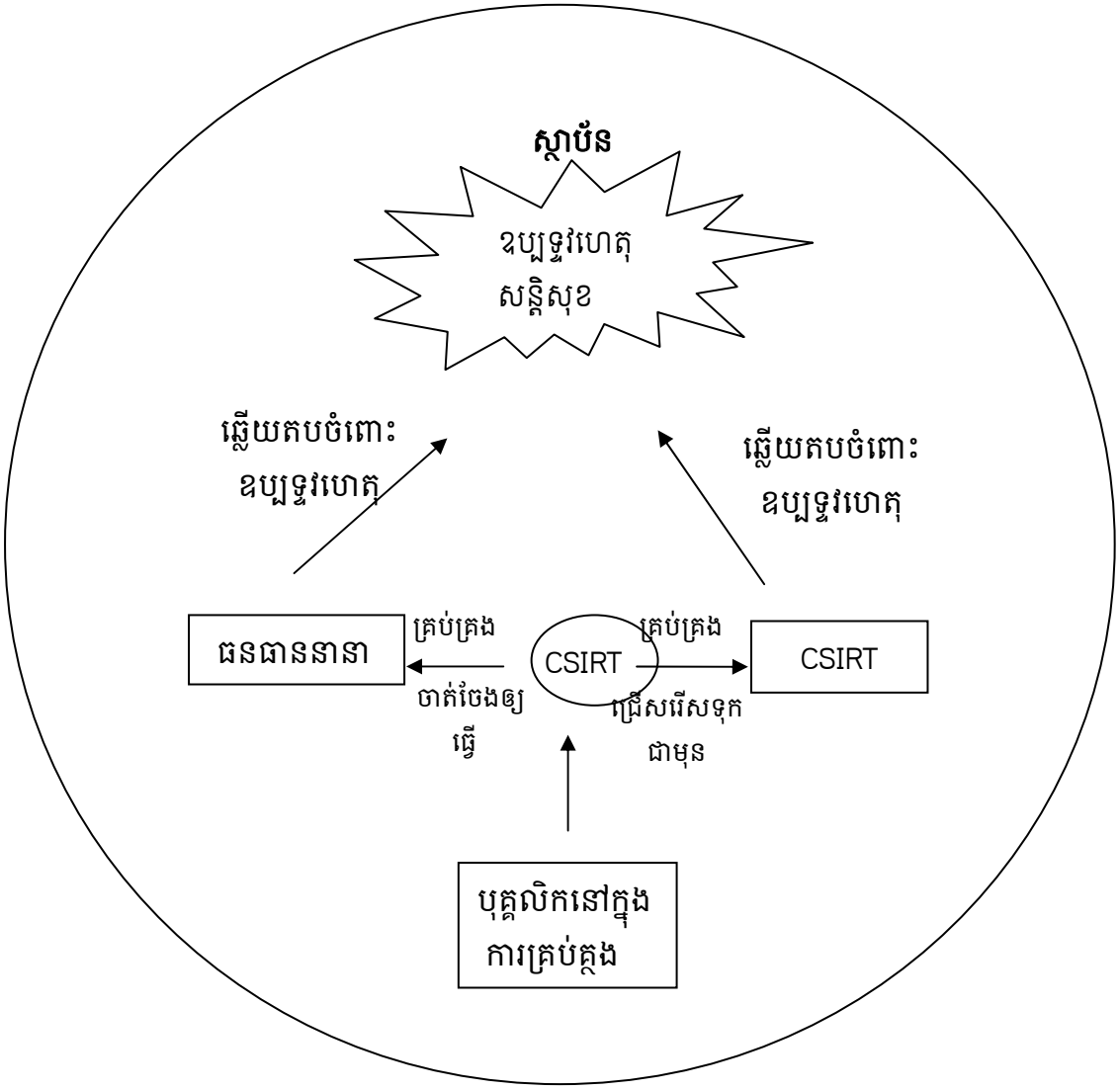
រូបទី១៥.គំរូ CSIRT **ចែកចាយខាងក្នុង**



៣. Internal Centralized CSIRT Model (**គំរូ** CSIRT **ជាផ្នែកកណ្តាលនៅខាងក្នុង**)

នៅក្នុង Internal Centralized CSIRT Model ក្រុមការងារមួយត្រូវបានដាក់រួមគ្នានៅចំផ្នែកកណ្តាល ដើម្បីត្រួតពិនិត្យ និងគាំទ្រស្ថាប័នមួយ។ CSIRT មានភាពទទួលខុសត្រូវទៅលើសកម្មភាពនៃការរាយការណ៍ការវិភាគ និងឆ្លើយតបរាល់ឧប្បទ្ទវហេតុដែលកើតឡើង។ ដូច្នេះវាមិនធ្វើការចំពោះឧប្បទ្ទវហេតុណាដែលស្ថិតនៅខាងក្រៅ។ CSIRT ជាប្រធានធ្វើសេចក្តីរាយការណ៍ផងដែរទៅកាន់ថ្នាក់គ្រប់គ្រងជាន់ខ្ពស់ដូចជាមន្ត្រីប្រធាន ព័ត៌មាន មន្ត្រីប្រធានសន្តិសុខ ឬក៏មន្ត្រីប្រធានហានិភ័យ។

រូបលេខ១៦.គំរូ CSIRT ជាផ្នែកកណ្តាលនៅខាងក្នុង

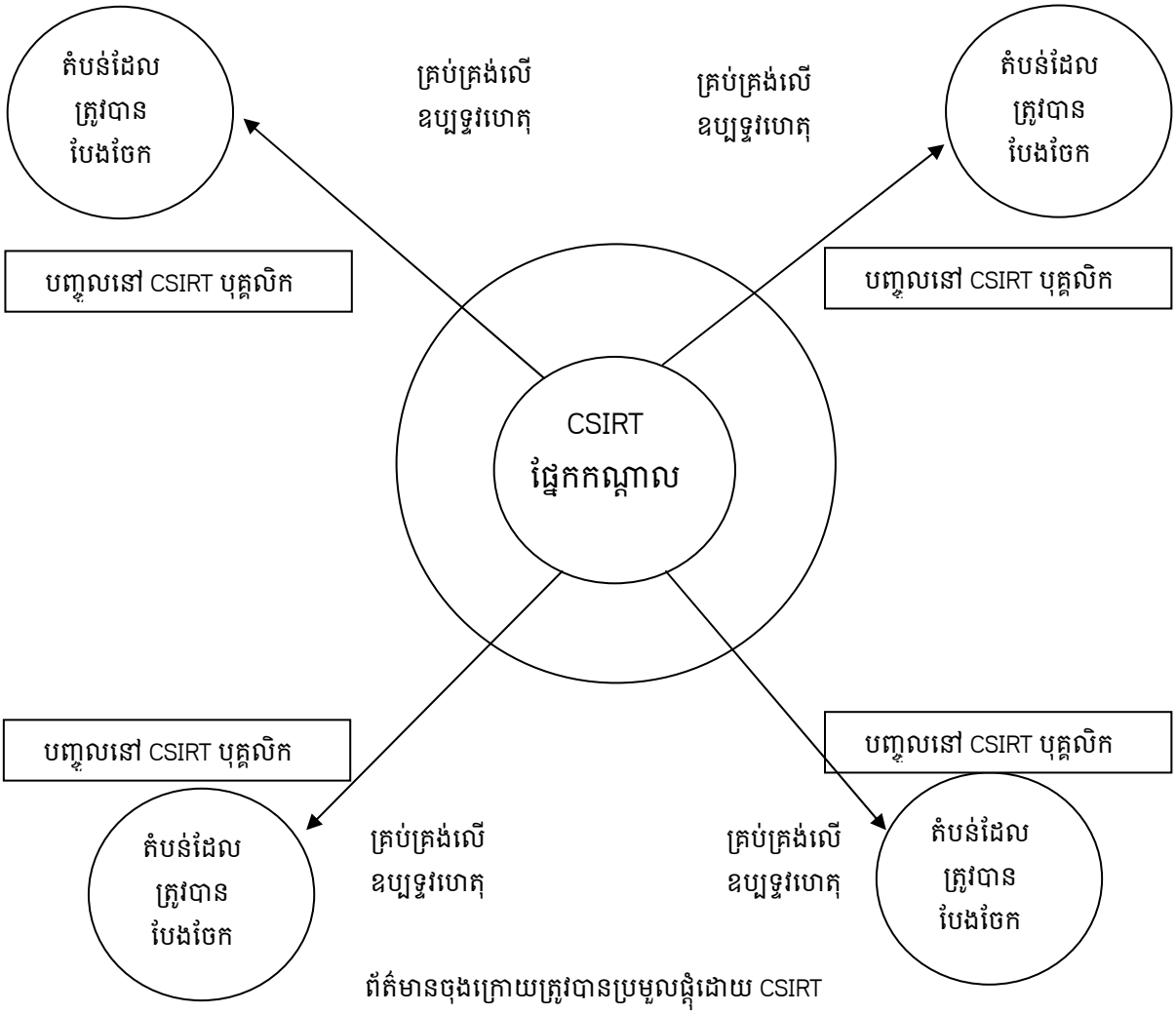


៤. Combined Distrubuted and Centralized CSIRT Model (**ការបញ្ចូលគ្នានៃគំរូ** CSIRT **ចែកចាយ និង ផ្នែកកណ្តាល**)

នេះគឺត្រូវគេស្គាល់ថាជា <<ការបញ្ចូលគ្នានៃគំរូ CSIRT (Comnined CSIRT)>>។ ផ្នែកខាងក្រៅ CSIRT ផ្នែកកណ្តាលមិនអាចគ្រប់គ្រងបានទេ។ ដូច្នេះសមាជិកក្រុមខ្លះដើរតួជា CSIRT ចែកចាយទៅ តំបន់ សាខា ផ្នែកតូចរបស់ស្ថាប័នដើម្បីផ្តល់មកដោយ CSIRT ផ្នែកកណ្តាល។

ក្រុមផ្នែកកណ្តាលផ្តល់នៅទិន្នន័យវិភាគក្នុងកម្រិតខ្ពស់ យុទ្ធវិធីស្តារឡើងវិញ និងយុទ្ធសាស្ត្រនានានៃការ ទប់ ស្កាត់។ វាផ្តត់ផ្តង់ផងដែរសម្រាប់សមាជិកក្រុមដែលត្រូវបានបែងចែកចេញទៅជាមួយការគាំទ្រផ្នែក ឆ្លើយតបលើឧប្បទ្វវហេតុ ភាពងាយរងគ្រោះ និង ឧបាយកលនានា។ សមាជិកក្រុមដែលត្រូវបាន បែងចែកទាំងនោះនៅ ឯតំបន់នីមួយៗអនវត្តន៍នៅយុទ្ធសាស្ត្រនានា និងផ្តល់នៅការធ្វើកោសល្យ វិច័យនៅក្នុងតំបន់។

រូបទី១៧. CSIRT ត្រូវបានបញ្ជូលគ្នា



ព័ត៌មានចុងក្រោយត្រូវបានប្រមូលផ្តុំដោយ CSIRT ផ្នែកកណ្តាលគឺត្រូវបានបញ្ជូនចុះទៅតំបន់ដែលបានកំណត់វិញតាមរយៈ CSIRT ដែលត្រូវបានផ្ទេរទៅកាន់ទីនោះ។

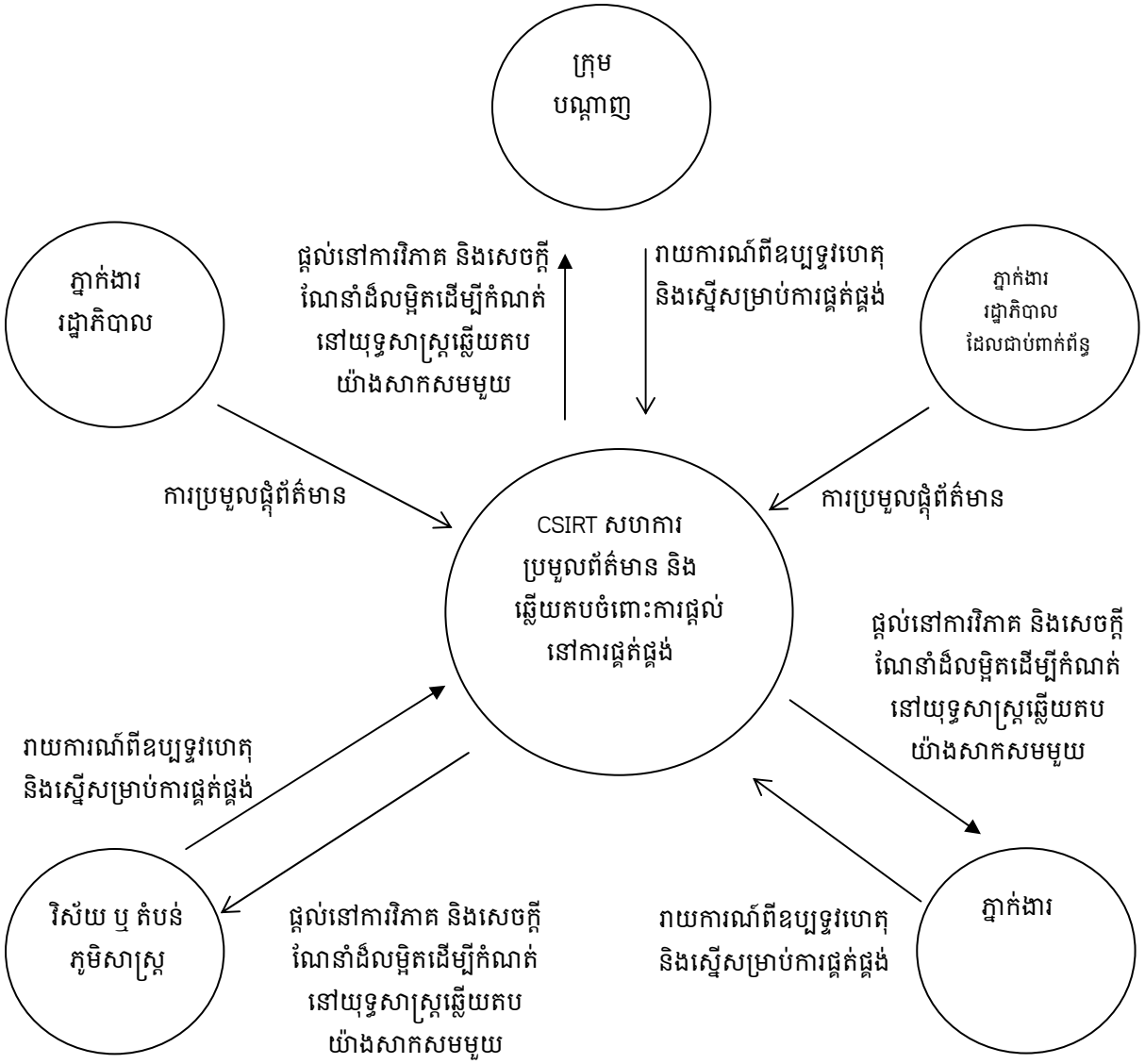
៥. Coordinating CSIRT Model (**គំរូ** CSIRT **សហការណ៍**)

គំរូ CSIRT សហការណ៍ពង្រឹងនៅមុខងារនៃក្រុមដែលត្រូវបានបែងចែកនៅក្នុង CSIRT ដែលត្រូវបានបញ្ចូលគ្នា(Combined CSIRT Model)។ នៅក្នុងគំរូ CSIRT សហការណ៍ក្រុមជាសមាជិកនៅក្នុងគំរូ CSIRT បញ្ចូលគ្នាគឺត្រូវបានចងក្រងជាក្រុមៗចូលទៅកាន់ CSIRT ឯករាជ្យទាំងអស់ត្រូវបានគ្រប់គ្រងដោយ CSIRT ផ្នែកកណ្តាលមួយ។

CSIRT សហការណ៍គឺសាកសមសម្រាប់ប្រព័ន្ធ CSIRT ជាតិមួយ។ គំរូនេះអាចប្រើប្រាស់ទៅលើសកម្មភាពខាងក្នុងអង្គការមួយ និងធ្វើការគាំទ្រ ព្រមទាំងធ្វើការសហការយ៉ាងជិតស្និទ្ធជាមួយភ្នាក់ងារខាងក្រៅ។

សកម្មភាពក្នុងការសហការណ៍ និងជួយសម្រួលនានាគ្របដណ្តប់ទាំងលើកការចែករំលែកព័ត៌មានផ្តល់នៅយុទ្ធសាស្ត្រទប់ស្កាត់ ឆ្លើយតបចំពោះឧប្បទ្ទវហេតុ យុទ្ធវិធីស្តារឡើងវិញ វិភាគ ស្រាវជ្រាវនៃនិន្នាការនានា និងគំរូនានានៃសកម្មភាពឧប្បទ្ទវហេតុ ទិន្នន័យនៃភាពងាយរងគ្រោះ ការិយាល័យសម្រាប់សន្តិសុខ និងសេវាកម្មណែនាំព្រមទាំងភាពប្រុងប្រយ័ត្ននានា។

រូបលេខ១៨. CSIRT **សហការណ៍**



បង្កើតនៅ CSIRT មួយៈ ជំហានសម្រាប់ការបង្កើតនៅ CSIRT ជាតិ [53]

គឺមានប្រាំដំណាក់កាល។ គោលបំណង ទស្សនៈ ឬតួនាទីនានានៃ CSIRT គួរតែរក្សាជាសេចក្តីណែនាំនៅក្នុងដំណើរបន្តតាមរយៈដំណាក់កាលទាំងនោះ។

53 This section is drawn from Georgia Killcrece, *Steps for Creating National CSIRTs* (Pittsburgh: Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

ដំណាក់កាលទី១ - អប់រំម្ចាស់ភាគហ៊ុននានាអំពីការអភិវឌ្ឍន៍នៃក្រុមជាតិមួយ

ដំណាក់កាលទី១គឺការយល់ដឹងពីដំណាក់កាលដែលម្ចាស់ភាគហ៊ុនរីកចម្រើនលើការយលសេងនៅក្នុងអ្វីដែលជាប់ពាក់ព័ន្ធនៅក្នុងការបង្កើតឡើងនៅ CSIRT ។តាមរយៈយុទ្ធវិធីអប់រំផ្សេងៗពួកគេសិក្សាអំពី:

a. អ្នកមានចំណាប់អារម្មណ៍ និងអ្នកដឹងនាំជំនួញស្ថិតនៅពីក្រោយសេចក្តីត្រូវការនៃ CSIRT ជាតិមួយ
b. តម្រូវការនានាដែលមិនអាចខ្វះបានសម្រាប់ការអភិវឌ្ឍន៍លើសមត្ថភាពឆ្លើយតបនឹងឧប្បទ្វវហេតុនៃ CSIRT ជាតិ។
c. ធ្វើឲ្យប្រជាជនចូលរួមក្នុងកិច្ចពិភាក្សាសម្រាប់ការកសាងក្រុមជាតិមួយ
d. ប្រពៃណីសំខាន់ និងហេដ្ឋរចនាសម្ព័ន្ធសំខាន់ៗដែលមាននៅក្នុងប្រទេស។
e. ប្រភេទនៃប៉ុស្តិ៍គមនាគមន៍ដែលត្រូវការធ្វើជាកន្លែងកំណត់លើទំនាក់ទំនងជាមួយមណ្ឌល CSIRT។
f. គោលការន៍ជាក់លាក់នានា ភាពត្រឹមត្រូវទៅតាមច្បាប់នានា និងគោលការណ៍ច្បាប់ផ្សេងៗទៀតដែលនឹង មានឥទ្ធិពលលើការអភិវឌ្ឍន៍នៃ CSIRT ជាតិ។
g. ផ្តល់នៅយុទ្ធសាស្ត្រផ្សេងៗដែលត្រូវបានប្រើលើការអភិវឌ្ឍន៍ ការបង្កើតគម្រោង ការអនុវត្តន៍ និងការប្រតិបត្តិចំពោះសមត្ថភាពឆ្លើយតប។
h. បច្ចេកវិទ្យា និងហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញព័ត៌មានដែលត្រូវការចំពោះការផ្តត់ផ្តង់លើសេចក្តីប្រតិបត្តិនៃក្រុមជាតិ។
i. គម្រោងឆ្លើយតបជាគ្រឹះនានា និងភាពឯករាជ្យផ្សេងៗដូចដែលពួកគេប្រើឆ្លងកាត់វិស័យផ្សេងៗ។
j. បង្កើតនៅសក្តានុពលនៃសេវាកម្មស្នូលនានាដែល CSIRT ជាតិដែលប្រហែលផ្តល់ទៅឲ្យមណ្ឌលរបស់វា។
k. ការអនុវត្តន៍ និងសេចក្តីណែនាំដ៏ល្អបំផុតដទៃៗទៀត។

ជំហានទី២ - គ្រោងការលើ CSIRT ការកសាងឡើងទៅលើចំណេះដឹង និងព័ត៌មានដែលបានមកពីជំហានទី១

ជំហានទី២ជាប់ពាក់ព័ន្ធលើគម្រោងបង្កើត CSIRT ដោយផ្អែកលើចំណេះដឹង និងព័ត៌មានដែលបានទទួលពីជំហានទី១។ បញ្ហាដែលបានពិភាក្សានៅក្នុងជំហានទី១ គឺត្រូវបានធ្វើសារឡើងវិញ និងធ្វើការពិភាក្សា

បន្ថែម និង បន្ទាប់មកការលម្អិតនានាត្រូវបានកំណត់ និងប្រើចំពោះដំណើរការនៃគម្រោង។ គម្រោងត្រូវបានធ្វើឡើងដោយគិតទៅលើសកម្មភាពដូចខាងក្រោម:

a. កំណត់លើតម្រូវការនានានិងសេចក្តីត្រូវការសម្រាប់ CSIRT ជាតិ
   - ច្បាប់ និងភាពគោរពច្បាប់នានាដែលមានឥទ្ធិពលលើការអនុវត្តន៍ផ្សេងៗនៃក្រុមជាតិ
   - ធនធានសំខាន់ៗដែលត្រូវការធ្វើការកំណត់ និងត្រូវការការពារ
   - ឧប្បទ្ទវហេតុថ្មីៗ និងនិន្នាការថ្មីៗដែលបាននឹងកំពុងត្រូវបានរាយការណ៍ ឬក៏គួរតែរាយការណ៍។
   - សមត្ថភាពផ្សេងៗលើការឆ្លើយតបចំពោះឧប្បទ្ទវហេតុដែលមានស្រាប់ និងការធ្វើកោសល្យវិច័យលើសន្តិសុខកុំព្យូទ័រ
b. ឲ្យនិយមន័យលើទស្សនៈនៃ CSIRT ជាតិ
c. ឲ្យនិយមន័យលើគណៈប្រតិភូនៃក្រុមជាតិ
d. កំណត់នៅមណ្ឌលមួយ (ឬក៏ច្រើន) ដែលនឹងត្រូវប្រើ
e. ឲ្យអត្តសញ្ញាណនៅការទំនាក់ទំនងចំពោះមុខរវាងមណ្ឌល និងក្រុមជាតិមួយ
f. ឲ្យអត្តសញ្ញាណនៅប្រភេទនៃការយល់ព្រមរបស់ថ្នាក់គ្រប់គ្រងជាតិ ភាពជាអ្នកដឹងនាំ ភាពជាអ្នកឧបត្ថម្ភ
g. ឲ្យអត្តសញ្ញាណនៅប្រភេទនៃជំនាញ និងចំណេះដឹងរបស់បុគ្គលិកដែលត្រូវការដំណើរការលើក្រុម
h. កំណត់ទៅតាមប្រភេទនៃតួនាទី និងការទទួលខុសត្រូវសម្រប់ CSIRT ជាតិ
i. ធ្វើឲ្យមានភាពជាក់លាក់លើដំណើរការគ្រប់គ្រងឧប្បទ្ទវហេតុនៃ CSIRT ក៏ដូចជាការកំណត់នៅភាពទំនាក់ទំនងគ្នាចំពោះដំណើរការប្រហាក់ប្រហែលគ្នានេះនៅក្នុងស្ថាប័នសំខាន់ៗផ្នែកខាងក្រៅខ្លះ។
j. ធ្វើការអភិវឌ្ឍន៍នៅបណ្តុំជាលក្ខណៈគំរូនៃភាពសំខាន់ និងរឹងប៉ឹងរបស់បច្ចេកវិទ្យាសម្រាប់ការចែកជាផ្នែកៗ និងកំណត់នៅព្រឹត្តិការណ៍ និងសកម្មភាពឧប្បទ្ទវហេតុនានា។
k. កំណត់នៅរបៀបណាដែល CSIRT ជាតិនឹងធ្វើការទំនាក់ទំនងជាមួយមណ្ឌល និង CSIRT សាកលដទៃទៀត ឬក៏ដៃគូខាងក្រៅនានា។
l. កំណត់នៅដំណើរការផ្សេងៗដេលបានស្នើឲ្យមានការធ្វើសមាហារណកម្មជាមួយការស្តារឡើងវិញនៅគ្រោះមហន្តរាយដែលមានស្រាប់ គម្រោងឆ្លើយតបឧប្បទ្ទវហេតុនានា គម្រោងនិរន្តភាពនៃជំនួញនានា វិបត្តិការគ្រប់គ្រង និងគម្រោងលើការគ្រប់គ្រងបន្ទាន់ដទៃៗទៀត
m. ធ្វើការអភិវឌ្ឍន៍នៅរយៈពេលដែលគម្រោងត្រូវអនុវត្តន៍

n. ការបង្កើតគម្រោង CSIRT ផ្អែកលើលទ្ធផលនានាចេញពីសកម្មភាពលើការធ្វើគម្រោងទស្សនៈ និងគ្រោងការដែលមានភាពស្របគ្នា

ដំណាក់កាលទី៣ - ក្រុមរបស់គម្រោងប្រើព័ត៌មាន និងផែនការណ៍ពីដំណាក់កាលទី១ និងទី២ ដើម្បីអនុវត្តន៍នៅ CSIRT ដំណើរការលើការអនុវត្តន៍គឺមានដូចខាងក្រោម:

a. ទទួលយកមូនិធិពីប្រភពនានាដែលបានកំណត់ក្នុងពេលដំណាក់កាលនៃការធ្វើផែនការណ៍។
b. ធ្វើការប្រកាសជាទូទៅថា CSIRT ជាតិគឺកំពុងបាននឹងបង្កើត និងដែលនឹងបូកបន្ថែមនៅព័ត៌មានដែលអាចបានមកពី (ដំណើរការបន្តលើការអភិវឌ្ឍន៍ ការរាយការណ៍ពីតម្រូវការនានា។ល។)
c. ធ្វើឧជាក់លាក់លើសហការណ៍ និងទំនាក់ទំនងជាមួយម្ចាស់ភាគហ៊ុន កិច្ចសន្យាសាកសមដទៃទៀត
d. អនុវត្តន៍នៅប្រព័ន្ធព័ត៌មានសន្តិសុខ និងហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញដើម្បីប្រតិបត្តិ CSIRT ជាតិ
e. ការអភិវឌ្ឍន៍នៅការប្រតិបត្តិ និងដំណើរការសម្រាប់បុគ្គលិក CSIRT រួមមានទាំងគំរូដែលត្រូវបានយល់ស្របនៅក្នុងដំណាក់កាលនៃការធ្វើផែនការណ៍ និងការរាយការណ៍ពីសេចក្តីណែនាំ។
f. អភិវឌ្ឍន៍គោលការណ៍ និងវិធានការផ្ទៃក្នុងនានាសម្រាប់ដំណើរ និងការអនុវត្តន៍នៃឧបករណ៍ CSIRT និង ឧបករណ៍ផ្ទាល់ខ្លួនដ៏ដូចជាទទួលយល់ព្រមលើការប្រើប្រាស់នៅគោលការណ៍នានា។
g. ធ្វើការប្រតិបត្តិលើដំណើរការនានាសម្រាប់សកម្មភាពជាអន្តរជាតិរបស់ CSIRT ជាមួយមណ្ឌលរបស់វា។
h. កំណត់ និងជួល (ឬរៀបចំចាត់ចែងជាថ្មី) បុគ្គលិកឲ្យមានការហ្វឹកហ្វឺន និងអប់រំដ៏សមរម្យសម្រាប់បុគ្គលិក CSIRT ក៏ដូចជាការកំណត់ទៅលើកិច្ចខំប្រឹងប្រែងប្រកបដោយសក្តានុពលលើការហ្វឹកហ្វឺន និងអប់រំឲ្យទៅដល់មណ្ឌល។

ដំណាក់កាលទី៤ - ការប្រតិបត្តិ CSIRT

នៅដំណាក់កាលប្រតិបត្តិនេះ សេវាកម្មសំខាន់ៗនានាដែល CSIRT ត្រូវផ្តល់ឲ្យនោះត្រូវបានធ្វើការកំណត់ ហើយប្រសិទ្ធិភាពនៃការប្រតិបត្តិដើម្បីប្រើប្រាស់នៅសមត្ថភាពគ្រប់គ្រងលើឧប្បទ្ទវហេតុគឺត្រូវបានវាយតម្លៃលើ ។ ផ្អែកលើលទ្ធផល ការលម្អិតនៃការប្រតិបត្តិនានាគឺត្រូវបានគេបង្កើតឡើង និងត្រូវបានធ្វើឲ្យប្រសើរឡើង។ សកម្មភាពនានានៅដំណាក់កាលនេះគឺ:

a. បង្កើតយ៉ាងសកម្មនៅសេវាកម្មផ្សេងៗដែលត្រូវបានផ្តល់ដោយ CSIRT ជាតិ។
b. ធ្វើការអភិវឌ្ឍន៍ និងការអនុវត្តន៍យន្តការមួយសម្រាប់ការវាយតម្លៃលើប្រសិទ្ធិភាពនៃការប្រតិបត្តិនានរបស់ CSIRT ជាតិ។
c. ធ្វើឲ្យប្រសើរឡើងនៅ CSIRT ជាតិដោយយោងទៅតាមលទ្ធផលនៃការវាយតម្លៃ។
d. ពង្រីកសមត្ថភាពគណៈកម្មាធិកា សេវាកម្មនានា និងបុគ្គលិកដែលសាកសមអាចនឹងគាំទ្រលើសេវាកម្មផ្សេងទៀតចំពោះមណ្ឌល។
e. ការបន្តការអភិវឌ្ឍន៍លើវិធានការ និងគោលការណ៍របស់ CSIRT។

ដំណាក់កាលទី៥ - សហការ

CSIRT ជាតិអាចអភិវឌ្ឍន៍នៅទំនាក់ទំនងដ៏គួរឲ្យទុកចិត្តមួយជាមួយម្ចាស់ភាគហ៊ុនសំខាន់ៗតាមរយៈការប្រតិបត្តិប្រកបដោយប្រសិទ្ធិភាព (ដំណាក់កាលទី៤)។ ប៉ុន្តែ CSIRT ជាតិត្រូវការផងដែរនៅការផ្លាស់ប្តូរព័ត៌មានសំខាន់ៗ និងបទពិសោធន៍នានានៃការកាន់កាប់ឧប្បទ្វវហេតុតាមរយៈការផ្លាស់ប្តូរក្នុងរយៈកាលយូរជាមួយការសហការវិទ្យាស្ថាន CSIRT នានានៅក្នុងស្រុក និង CSIRT អន្តរជាតិ។ សកម្មភាពនៅក្នុងដំណាក់កាលនេះរួមមាន:

a. ចូលរួមនៅក្នុងសកម្មភាពផ្សេងៗលើការចែករំលែកព័ត៌មាន និងទិន្នន័យព្រមទាំងគាំទ្រលើការអភិវឌ្ឍន៍នៃ គំរូនានាសម្រាប់ការចែករំលែកព័ត៌មាន និងទិន្នន័យរវាយដៃគូ CSIRT ដទៃទៀតមណ្ឌល និងជំនាញសន្តិសុខកុំព្យូទ័រដទៃទៀត។
b. ចូលរួមនៅក្នុងមុខងារផ្សេងៗលើការ “ឃ្លាំមើល និង ការព្រមាន” ជាសកលដើម្បីគាំទ្រលើសហគមនៃ CSIRT
c. ធ្វើឲ្យប្រសើឡើងនៅគុណភាពនៃសកម្មភាពរបស់ CSIRT ដោយកាផ្តលើនៅការហ្វឹកហ្វឺនសិក្ខាសាលា និងការធ្វើសន្និសិទ្ធ ដែលពិភាក្សាលើនិន្នាការនៃការវាយប្រហារ និងយុទ្ធសាស្ត្រនៃការឆ្លើយតប។
d. សហការជាមួយអ្នកដទៃទៀតនៅក្នុងសហគមន៍ដើម្បីអភិវឌ្ឍន៍នៅឯកសារស្តីពីការអនុវត្តន៍ និងសេចក្តីណែនាំនានាដ៏ល្អបំផុត។

e. ការធ្វើឡើងវិញ និងការបន្ថែមបន្តយនៅដំណើរការផ្សេងៗសម្រាប់ការគ្រប់គ្រងលើឧប្បទ្ទវហេតុ ដែលជាផ្នែកមួយនៃការបន្តនៅដំណើរប្រតិបត្តិ។

សេវាកម្មនានារបស់ CSIRT[54]

សេវាកម្មនានាដែល CSIRT ផ្តល់ប្រហែលត្រូវបានចែកចេញជាផ្នែកៗចូលជាសេវាកម្មតបត សេវាកម្មលើសកម្មភាពមុន និងសេវាកម្មគ្រប់គ្រងគុណភាពនៃសេវា។

សេវាកម្មតបតគឺជាសេវាកម្មស្នូលនៃ CSIRT ។ពួកគេរួមមាន:

១. ប្រកាសប្រាប់ និងការព្រមាន: សេវាកម្មនេះរួមមានទាំងការផ្តល់ព័ត៌មាន និងយុទ្ធវិធីឆ្លើយតបលើការដោះស្រាយបញ្ហាដូចជាភាពងាយរងគ្រោះលើសន្តិសុខ ប្រកាសប្រាប់ពីការចូលឈ្លានពាន មេរោគកុំព្យូទ័រ ឬឧបាយកលបោកបញ្ឆោត។

២. ការគ្រប់គ្រងឧប្បទ្ទវហេតុ នេះជាប់ពាក់ព័ន្ធជាមួយលើការទទួលការតាមដាន និងការឆ្លើយតបទៅលើសំណើរ និងការរាយការណ៍ ព្រមទាំងការវិភាក និងអាទិកម្មលើឧប្បទ្ទវហេតុ និងព្រឹត្តការណ៍ផ្សេងៗសកម្មភាពលើការឆ្លើយតបដ៏ជាក់ច្បាស់នានារួមមានដូចខាងក្រោម:

- វិភាគលើឧប្បទ្ទវហេតុ - ធ្វើការវិភាគមួយនៃរាល់ព័ត៌មានដែលអាចរកបាន និងការគាំទ្រចំពោះភស្តុតាង ឬក៏ការទាក់ទងមុនៗចំពោះឧប្បទ្ទវហេតុ ឬហេតុការណ៍មួយ។ គោលបំណងនៃការរាយតម្លៃគឺកំណត់នៅរយៈពេលនៃឧប្បទ្ទវហេតុ ការរីកធំធាត់នៃការបំផ្លាញដែលបានបណ្តាលមកពីឧប្បទ្ទវហេតុ ភាពដើមនៃឧប្បទ្ទវហេតុ និងយុទ្ធសាស្ត្រនានាលើការឆ្លើយតបដែលអាករកបាន ឬក៏ការរនៅជុំវិញឧប្បទ្ទវហេតុនោះ។

54 This section is drawn from Carnegie Mellon University, *CSIRT Services* (2002), http://www.cert.org/archive/pdf/CSIRT-services-list.pdf.

- ការប្រមូលនៅភស្តុតាងតាមនីតិក្រម - ប្រមូល ថែរក្សា ការរក្សាជាឯកសារ និងការវិភាគនៃភស្តុតាងពីការសហការនៃប្រព័ន្ធកុំព្យូទ័រ ដើម្បីកំណត់ការផ្លាស់ប្តូរចំពោះប្រព័ន្ធ និងជួយនៅកន្លងការស្ថាបនាឡើងវិញនៃហេតុការណ៍នានាដែលដឹកនាំទៅរកកិច្ចព្រមព្រៀងមួយ។

- ការស្វែងរកដាន ឬការតាមដាន - ជាប់ពាក់ព័ន្ធនឹងការស្វែងរកដាន ឬការតាមដាននៅរបៀបណាដែលអ្នកឈ្លានពានបានចូលទៅធ្វើឲ្យមានផលប៉ះពាល់លើប្រព័ន្ធនានា និងបណ្តាញ។ សកម្មភាពទាំងនេះរួមមានការតាមដាននៅប្រភពដើមនៃអ្នកឈ្លានពាន ឬក៏ការកំណត់នៅទីកន្លែងដែលអ្នកឈ្លានពានដំណើរការ។

៣.ការឆ្លើយតបទៅនឹងឧប្បទ្ទវហេតុនៅតាមតំបន់ - CSIRT ផ្តល់ដោយត្រង់ទៅលើតំបន់ជាជំនួយដើម្បីជួយ មណ្ឌលនានស្តារឡើងវិញពីឧប្បទ្ទវហេតុ។

៤.គាំទ្រការឆ្លើយតបចំពោះឧប្បទ្ទវហេតុ - CSIRT ជួយ នឹងណែនាំជនរងគ្រោះនៃការវាយប្រហារនៅក្នុងការស្តារឡើងវិញពីឧប្បទ្ទវហេតុតាមរយៈទូរស័ព្ទ អ៊ីមែល ទូរសារ ឬឯកសារ។

៥.សហការលើការឆ្លើយតបឧប្បទ្ទវហេតុ - កិច្ចខិតខំប្រឹងប្រែងលើការឆ្លើយតបជាមួយនឹងឧប្បទ្ទវហេតុគឺត្រូវបានសហការគ្នា។ នេះជារឿយៗរួមមានជនរងគ្រោះពីការវាយប្រហារ តំបន់ផ្សេងៗដែលជាប់ពាក់ព័ន្ធនៅក្នុងការវាយប្រហារ និងតំបន់នានាដែលស្នើឲ្យមានជំនួយនៅក្នុងការវិភាគនៃការ វាយប្រហារ។ វាប្រហែលរួមទាំងក្រុមផ្សេងៗផងដែរដែលផ្តល់នៅការគាំទ្រផ្នែក IT ចំពោះជនរងគ្រោះដូចជា ISPs និង CSIRTs ដទៃទៀត។

៦.ការគ្រប់គ្រង់លើភាពងាយរងគ្រោះ - នេះជាប់ពាក់ព័ន្ធទៅលើការទទួលព័ត៌មាន និងសេចក្តីរាយការណ៍នានាអំពីជនរងគ្រោះលើ Hardware ការវិភាកលើផលប៉ះពាល់នៃភាពងាយរងគ្រោះ និងការអភិវឌ្ឍន៍នៅយុទ្ធសាស្ត្រតបសម្រាប់ចាប់ និងការជួសជុលឡើងវិញលើការរងគ្រោះនោះ។

- វិភាគលើភាពងាយរងគ្រោះ - សំដៅទៅលើការវិភាគតាមបច្ចេកវិទ្យា និងការវិភាគលើភាពងាយរងគ្រោះនៃ Hardware ឬក៏ Software។ការវិភាគរួមមានការធ្វើឡើងវិញនៅ Source Code ការប្រើអ្នក

ចាំស្គាក់ដើម្បីកំណត់ថាតើកន្លែងណាដែលការរងគ្រោះនោះកើតឡើង ឬក៏ព្យាយាមចម្លងនៅបញ្ហានោះសម្រាប់ការធ្វើសាកល្បងដោយប្រព័ន្ធ។

- ឆ្លើយតបចំពោះភាពងាយរងគ្រោះ - ជាប់ពាក់ព័ន្ធទៅនឹងការកំណត់នៅការឆ្លើយតបដ៏សមរម្យដើម្បីរារាំងឬក៏ជួសជុលនៅការរងគ្រោះនានា។ សេវាកម្មនេះអាចរួមមានការបង្កើតឡើងនៅការឆ្លើយតបមួយដោយការតម្លើងវិញនៅស្នាមខូចខាត ជួសជុល ឬក៏ការងារជុំវិញបញ្ហានេះ។ វាជាប់ពាក់ព័ន្ធនឹងការកត់សម្គាល់លើបញ្ហាដទៃទៀតនៃយុទ្ធសាស្ត្រលើការរារាំង ការផ្តលើដំបូន្មាន ឬការប្រកាសប្រាប់នានាដទៃទៀតផងដែរ។

- ការសហការលើការឆ្លើយតបនឹងភាពងាយរងគ្រោះ - CSIRT កំនត់នៅផ្នែកផ្សេងៗនៃសហគ្រាសឬក៏មណ្ឌលអំពីភាពងាយរងគ្រោះព្រមទាំងចែកចាយព័ត៌មានអំពីរបៀងជួសជុល ឬក៏រារាំងវា។ CSIRT ផងដែរបានចាត់ជាថ្នាក់ៗលើយុទ្ធសាស្ត្រឆ្លើយតប នឹងភាពងាយរងគ្រោះប្រកបដោយជោគជ័យ។ សកម្មភាពនានារួមមាន ការវិភាគលើភាពងាយរងគ្រោះ ឬរាយការណ៍នៃភាពព្រមទាំងវិភាគលើការ សង្គ្រោះតាមបច្ចេកវិទ្យាដែលត្រូវបានធ្វើដោយផ្នែកផ្សេងៗ។ សេវាកម្មនេះអាចរួមមានទាំងការថែរក្សាស្នាដៃ ឬចំណេះផ្នែកឯកជន ឬក៏ផ្តែកលើយុទ្ធសាស្ត្រផ្សេងៗលើការឆ្លើយតបព្រមគ្នា និងព័ត៌មានពីភាពងាយរងគ្រោះ។

៧. គ្រប់គ្រងលើភាពបោកបញ្ឆោតៈ នេះរួមមានការវិភាគ ឆ្លើយតប សហការ និងគ្រប់គ្រងលើភាពបោកបញ្ឆោតដែលជាប់ពាក់ព័ន្ធនឹងទង្វើរបស់មេរោគកុំព្យូទ័រ កម្មវិធី Trojan Horse , Worm អក្សរប្រកបដោយគ្រោះថ្នាក់ និងឧបករណ៍នានា។

- វិភាគលើការបោកបញ្ឆោត - CSIRT ធ្វើការវិភាគតាមបច្ចេកវិទ្យា និងវិភាគនៃការបោកបញ្ឆោតនានាដែលបានរកឃើញនៅក្នុងប្រព័ន្ធ។
- ឆ្លើយតបលើការបោកបញ្ឆោត - ជាប់ពាក់ព័ន្ធនឹងការកំណត់សកម្មភាពដ៏សមរម្យមួយដើម្បីចាប់និងយកការបោកបញ្ឆោតនោះចេញពីប្រព័ន្ធ។
- សហការលើការឆ្លើយតបទៅនឹងការបោកបញ្ឆោត - ជាប់ពាក់ព័ន្ធនឹងការចែករំលែក និងលទ្ធផលបានពីការវិភាគលើការសង្គ្រោះ និងយុទ្ធសាស្ត្រឆ្លើយតបនានាដែលមានការទាក់ទងទៅនឹងការបោកបញ្ឆោតជាមួយអ្នកស្រាវជ្រាវផ្សេងទៀត CSIRT អ្នកលក់ និងអ្នកជំនាញសន្តិសុខដទៃទៀត។

សេវាកម្មលើការធ្វើសកម្មភាពមុន គឺសម្រាប់ធ្វើឲ្យប្រសើរឡើងនៅហេដ្ឋារចនាសម្ព័ន្ធ និងដំណើរការលើសន្តិសុខនៃមណ្ឌលមុនឧប្បទ្ទវហេតុខ្លះៗ ឬក៏ហេតុការណ៍កើតឡើង ឬក៏ត្រូវបានចាប់បាន។ ពួកគេរួមមានដូចខាងក្រោម:

១. ការប្រកាស: នេះរួមមានការប្រកាសប្រាប់ពីការឈ្លានពាន ការព្រមានអំពីភាពងាយរងគ្រោះ ដំបូន្មាននានាពីសន្តិសុខ និងអ្វីផ្សេងទៀត។ ដូចជាការប្រកាសបញ្ជាក់ប្រាប់មណ្ឌលនានាអំពីការអភិវឌ្ឍន៍ថ្មីៗជាមួយផលប៉ះពាល់ជាមធ្យមទៅកាន់រយៈពេលយូរ ដូចជាការរកឃើញនៅភាពងាយរងគ្រោះថ្មីៗ ឬវិធីនៃការវាយលុករបស់អ្នកឈ្លានពាន។ ការប្រកាសអាចឲ្យមណ្ឌលនានាការពារប្រព័ន្ធរបស់ពួកគេ និងបណ្តាញប្រឆាំងទៅនឹងបញ្ហាដែលទើបនឹងរកឃើញមុនពួកគេត្រូវបានកេងប្រវ័ញ្ចដោយការបោកប្រាស់ទាំងនោះ។

២. ឃ្លាំមើលលើបច្ចេកវិទ្យា - នេះជាប់ពាក់ព័ន្ធទៅនឹងការត្រួតពិនិត្យ និងឃ្លាំមើលនៅការអភិវឌ្ឍន៍នៅបច្ចេកវិទ្យាថ្មីៗ សកម្មភាពនានារបស់អ្នកឈ្លានពាន និងនិន្នាការដែលជាប់ពាក់ព័ន្ធដទៃទៀតដើម្បីជួយកំណត់នៅការគំរាមកំហែងនាពេលអនាគត។ លទ្ធផលនៃសេវាកម្មនេះប្រហែលជាប្រភេទខ្លះនៃសេចក្តីណែនាំ ឬផ្តល់អនុសាសន៍ដែលផ្តោតទៅលើបញ្ហាសន្តិសុខជាច្រើនដែលស្ថិតក្នុងរយៈការមធ្យម ឬក៏វែង។

៣. សវនកម្មសន្តិសុខ ឬការប៉ានប្រមាណ: សេវាកម្មនេះផ្តល់នៅការធ្វើឡើងវិញ និងការវិភាគយ៉ាងលម្អិតនៃហេដ្ឋារចនាសម្ព័ន្ធសន្តិសុខរបស់ស្ថាប័ន ដោយផ្អែកលើតម្រូវការដែលត្រូវបានកំណត់ដោយស្ថាប័ន ឬដោយគំរូ ឧស្សាហកម្មដទៃៗទៀតបានប្រើ។

៤. ការធ្វើឲ្យមានរូបរាងសណ្ឋាន និងការថែរក្សានៃឧបករណ៍សន្តិសុខ ដំណើរការ ហេដ្ឋារចនាសម្ព័ន្ធ និងសេវាកម្មនានា - សេវាកម្មនេះផ្តល់នៅសេចក្តីណែនាំដ៏សមស្របមួយទៅលើរបៀបធ្វើឲ្យមានរូបរាងសណ្ឋាន និងការថែរក្សាលើឧបករណ៍ ដំណើរការ និងហេដ្ឋារចនាសម្ព័ន្ធកុំព្យូទ័រទូទៅប្រកបដោយសុវត្ថិភាព។

៥. អភិវឌ្ឍន៍នៅឧបករណ៍សន្តិសុខនានា - សេវាកម្មនេះរួមមាននៅការអភិវឌ្ឍន៍ថ្មី ឧបករណ៍ជាក់លាក់នៃមណ្ឌល កម្មវិធី Software , Pluc-In និងស្នាមខូចខាត ដែលត្រូវបានអភិវឌ្ឍន៍ និងត្រូវបានបែងចែកសម្រាប់សន្តិសុខ។

៦. សេវាកម្មចាប់នៅការឈ្លានពាននានា - CSIRT ដែលធ្វើនៅសេវាកម្មនេះគឺការធ្វើឡើងវិញនៅការចូលទៅកាន់ប្រព័ន្ធដោយ IDS ដែលមានស្រាប់ វិភាគលើពួកគេ និងចាប់ផ្តើមការឆ្លើយតបមួយសម្រាប់ព្រឹត្តការណ៍នានាដែលជួបនឹងការកំណត់នៅច្រកចូលរបស់ពួកគេ។

៧. ការបែកសាយព័ត៌មានដែលទាកទងនឹងសន្តិសុខ - សេវាកម្មនេះផ្តល់នៅមណ្ឌលនានាជាមួយភាពធំទូលាយ និងភាពងាយស្រួលស្វែងរកនៅការប្រមូលផ្តុំនៃព័ត៌មានដែលអាចប្រើការបានជាប្រយោជន៍ដែលជួយនៅក្នុងការធ្វើឲ្យប្រសើរឡើងលើសន្តិសុខ។

សេវាកម្មគ្រប់គ្រងលើគុណភាពសន្តិសុខ គឺត្រូវបានរៀបចំឡើងដើម្បីផ្តល់នៅចំណេះដឹងដែលបានទទួលពីការឆ្លើយតបចំពោះឧប្បទ្ទវហេតុនានា ភាពងាយរងគ្រោះផ្សេងៗព្រមទាំងការសង្គ្រោះលើការវាយប្រហារ។ ដូចជាសេវាកម្មខាងក្រោម:

១. វិភាគលើហានិភ័យ - នេះជាប់ពាក់ព័ន្ធធ្វើឲ្យប្រសើរឡើងនៅសមត្ថភាពរបស់ CSIRT ដើម្បីប្រមាណមើលនៅការគំរាមកំហែងពិតប្រាកដនានា ផ្តល់នៅបរិមាណក្នុងភាពប្រាកដនិយម និងបរិមាណលើការប៉ាន់ប្រមាណនៃហានិភ័យចំពោះទ្រព្យសម្បត្តិព័ត៌មាន និងការវាយតម្លៃលើការការពារ និងយុទ្ធសាស្ត្រឆ្លើយតបនានា។

២. គម្រោងស្តារឡើងវិញនៅគ្រោះមហន្តរាយ និងនិរន្តន៍ភាពជំនួញ - និរន្តន៍ភាពជំនួញ និងការស្តារឡើងវិញពីគ្រោះមហន្តរាយដែលបានបណ្តាលមកដោយសារការវាយប្រហារលើសន្តិសុខកុំព្យូទ័រ គឺត្រូវបានធានាតាមរយៈ ការបង្កើតផែនការឲ្យបានគ្រប់គ្រាន់។

៣.ការប្រឹក្សាលើសន្តិសុខ - CSIRT អាចផ្តល់នៅដំបូន្មានជាលក្ខណៈអនុវត្តន៍ និងសេចក្តីណែនាំសម្រាប់ដំណើរការនៅជំនួញ។

៤. ការកសាងនៅភាពយល់ដឹង - CSIRT គឺអាចធ្វើឲ្យមានភាពប្រសើរឡើងនៅការយល់ដឹងពីសន្តិសុខដោយការកំណត់នៅអត្តសញ្ញាណ និងការផ្តល់នៅព័ត៌មាន និងសេចក្តីណែនាំអំពីការអនុវត្តន៍ និងគោលការណ៍នានារបស់សន្តិសុខដែលមណ្ឌលនានាស្នើរសុំ។

៥. ការអប់រំ ការហ្វឹកហ្វឺន - សេវាកម្មនេះជាប់ពាក់ព័ន្ធនឹងការផ្តល់នៅការអប់រំ និងការហ្វឹងហ្វឺនទៅលើអត្ថបទទាំងឡាយដូចជាសេចក្តីណែនាំពីការរាយការណ៍ពីឧប្បទ្ទវហេតុ យុទ្ធវិធីនានាក្នុងការឆ្លើយតបយ៉ាងសមរម្យ ឧបករណ៍សម្រាប់ការឆ្លើយតបនឹងឧប្បទ្ទវហេតុ យុទ្ធវិធីនៃការការពារឧប្បទ្ទវហេតុ និងព័ត៌មានចាំបាច់ផ្សេងទៀតដើម្បីការពារ ចាប់ រាយការណ៍ និងឆ្លើយតបចំពោះឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រផ្សេងៗ។ ការហ្វឹកហ្វឺនលើបែបផ្សេងៗរួមមានតាមរយៈសិក្ខាសាលាមុខវិជ្ជា និងការបង្រៀន។

៦. ការវាយតម្លៃលើផលិតផល ឬលិខិតបញ្ជាក់ - CSIRT ប្រហែលជាអនុវត្តន៍ការវាយតម្លៃផលិតផលទៅលើឧបករណ៍ ដំណើរការនានា ឬក៏សេវាកម្មផ្សេងៗទៀតដើម្បីធានាសន្តិសុខនៃផលិតផលទាំងនោះ និងភាពស្របគ្នារបស់ពួកគេដែលត្រូវទទួលយកបានដោយ CSIRT ឬក៏តាមការអនុវត្តន៍នានាដែលត្រូវបានទទួលស្គាល់លើសន្តិសុខ។

តារាងលេខ១២ បង្ហាញពីកម្រិតនៃសេវាកម្ម CSIRT និមួយៗ - ឧទាហរណ៍ថាតើជាស្នូល ជាការបូក បន្ថែម ឬជាសេវាកម្មខុសប្លែកពីគេ - នៅក្នុងគំរូ CSIRT និមួយៗ។

ផ្នែកសេវាកម្ម	សេវាកម្មនានា		ក្រុមសន្តិសុស	ចែកចាយ	ផ្នែកកណ្តាល	បញ្ចូលគ្នា	សហការ
តបត	ការប្រកាសប្រាប់ និងព្រមាន		ការបន្ថែម	ស្នូល	ស្នូល	ស្នូល	ស្នូល
	ការគ្រប់គ្រងលើឧប្បទ្ទវហេតុ	ការវិភាគលើឧប្បទ្ទវហេតុ	ស្នូល	ស្នូល	ស្នូល	ស្នូល	ស្នូល
		ការឆ្លើយតបឧប្បទ្ទវហេតុលើតំបន់	ស្នូល	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម

		គាំទ្រលើការឆ្លើយតបឧប្បទ្ទវហេតុ	ខុសប្លែកពីគេ	ស្មើ	ស្មើ	ស្មើ	ស្មើ
		សហការលើការឆ្លើយតបនឹងឧប្បទ្ទវហេតុ	ស្មើ	ស្មើ	ស្មើ	ស្មើ	ស្មើ
	ការគ្រប់គ្រងលើការបោកបញ្ឆោត	វិភាគលើភាពងាយរងគ្រោះ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
		ឆ្លើយតបចំពោះភាពងាយរងគ្រោះ	ស្មើ	ការបន្ថែម	ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម
		ការសហការឆ្លើយតបចំពោះភាពងាយរងគ្រោះ	ការបន្ថែម	ស្មើ	ស្មើ	ស្មើ	ស្មើ
		វិភាគលើការបោកបញ្ឆោត	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
		ឆ្លើយតបលើការបោកបញ្ឆោត	ស្មើ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
		ការសហការលើការឆ្លើយតបនឹងការបោកបញ្ឆោត	ការបន្ថែម	ការបន្ថែម	ស្មើ	ស្មើ	ស្មើ
ធ្វើសកម្មភាពមុន	ការប្រកាស		ខុសប្លែកពីគេ	ស្មើ	ស្មើ	ស្មើ	ស្មើ
	ការឃ្លាំមើលលើបច្ចេកវិទ្យា		ខុសប្លែកពីគេ	ការបន្ថែម	ស្មើ	ស្មើ	ស្មើ
	សោរនកម្ម ឬការប៉ាន់ប្រមាណលើសន្តិសុខ		ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
	ការធ្វើនៅរូបរាងសណ្ឋាន និងការថែរក្សាលើឧបករណ៍ ដំណើរការ ហេដ្ឋារចនាសម្ព័ន្ធ និងសេវាកម្មសន្តិសុខ		ស្មើ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
	ការអភិវឌ្ឍន៍នៃឧបករណ៍សន្តិសុខ		ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
	សេវាកម្មនានាចាប់នៅអ្នកឈ្លានពាន		ស្មើ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ខុសប្លែកពីគេ
	ការសាយភាយនៅព័ត៌មានដែលទាក់ទងទៅនឹងសន្តិសុខ		ខុសប្លែកពីគេ	ការបន្ថែម	ស្មើ	ស្មើ	ស្មើ
ការគ្រប់គ្រងលើគុណភាពសន្តិសុខ	វិភាគលើហានិភ័យ		ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
	គ្រោងស្តារឡើងវិញនៅគ្រោះមហន្តរាយ និងនិរន្តន៍ភាពសន្តិសុខ		ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម
	ការប្រឹក្សាលើសន្តិសុខ		ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម

	ការកសាងនៅការយល់ដឹង	ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ស្មុល
	ការអប់រំ/ការហ្វឹកហ្វឺន	ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ស្មុល
	ការវាយតម្លៃលើផលិតផល ឬក៏ លិខិតបញ្ជាក់	ខុសប្លែកពីគេ	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម	ការបន្ថែម

Source: Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

៦.២ CSIRTs អន្តរជាតិ

ថ្មីៗនេះគឺមានចំនួននៃ CSIRT ជាអន្តរជាតិដ៏ប្រាកដមួយដែលត្រូវបានបង្កើតឡើងដើម្បីឆ្លើយតបទៅកាន់ឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រនានានៅជុំវិញពិភពលោក។ ខណៈពេលដែល CSIRT ជាតិអាចឆ្លើយតបទៅនឹងការលុកលុយនានា និងធ្វើនៅមុខងារផ្សេងទៀតរបស់ពួកគេ ការវាយប្រហារអន្តរជាតិស្នើឲ្យមានការគិតគូរនៃ CSIRT ជាអន្តរជាតិមួយ។

វេទិការនៃក្រុមសន្តិសុខឆ្លើយតបឧប្បទ្ទវហេតុ (FIRST)[55]

FIRST រួមមាន CERTs ភ្នាក់ងាររដ្ឋាភិបាល និងក្រុមហ៊ុនសន្តិសុខនានាពីប្រទេសចំនួន ៤១ ប្រទេស។ សមាជិករបស់វារួមមាន ១៩១ ស្ថាប័ន រួមមាន CERT/CC និង US-CERT។ FIRST គឺជាភ្នាក់ងារមួយសម្រាប់ការចែកចាយព័ត៌មាន និងការសហប្រតិបត្តិក្នុងចំណោមក្រុមឆ្លើយតបនឹងឧប្បទ្ទវហេតុ។គោលបំណងរបស់វាគឺធ្វើសកម្មភាពនានាលើកិច្ចការពារ និងឆ្លើយតបនឹងឧប្បទ្ទវហេតុ និងធ្វើឲ្យមានចំណាង់ក្នុងកិច្ចសហប្រតិបត្តិការក្នុងចំណោមសមាជិក ដោយផ្តល់ពួកគេជាមួយបច្ចេកវិទ្យាចំណេះដឹង និងឧបក្រណ៍នានាសម្រាប់ការឆ្លើយតបនឹងឧប្បទ្ទវហេតុ។ សកម្មភាពនានានៃ FIRST គឺមានដូចខាងក្រោម:

- ការអភិវឌ្ឍន៍ និងចែករំលែកការអនុវត្តន៍ វិធានការ ឧបករណ៍ ព័ត៌មានបច្ចេកវិទ្យា និងយុទ្ធវិធីដ៏ល្អបំផុតសម្រាប់ឆ្លើយតបនឹងឧប្បទ្ទវហេតុ និងការការពារ។

55 FIRST, "About FIRST," FIRST.org, Inc., http://www.first.org/about/.

- ធ្វើឲ្យមានចំណាប់អារម្មណ៍សម្រាប់ការអភិវឌ្ឍន៍នៅគោលការណ៍ សេវាកម្ម និងផលិតផលសន្តិសុខ ដែលមានគុណភាពល្អ
- ធ្វើការគាំទ្រ និងការអភិវឌ្ឍន៍សេចក្តីណែនាំនានារបស់សន្តិសុខកុំព្យូទ័រដ៏សាកសម។
- ជួយទៅលើរដ្ឋាភិបាល សហគ្រាស និងវិទ្យាស្ថានអប់រំដើម្បីបង្កើតនៅក្រុមឆ្លើយតបលើឧប្បទ្វរហេតុ និងធ្វើឲ្យវាមានភាពរីកចម្រើនឡើង និង
- ជួយសម្រួលលើការចែកចាយនៅបច្ចេកវិទ្យា បទពិសោធន៍ននា និងចំណេះដឹងក្នុងចំណោមសមាជិក នានាសម្រាប់បរិស្ថានអេឡិចត្រូនិចសុវត្ថិភាពមួយ។

CERT **អាស៊ីប៉ាស៊ីហ្វិច**[56]

ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រអាស៊ីប៉ាស៊ីហ្វិច គឺត្រូវបានបង្កើតឡើងនៅក្នុងខែ កុម្ភៈ ឆ្នាំ ២០០៣ ដើម្បីបម្រើជាបណ្តាញមួយនៃអ្នកជំនាញសន្តិសុខ ពង្រឹងការឆ្លើយតបឧប្បទ្វរហេតុ និងធ្វើឲ្យប្រសើរឡើងនៅការយល់ដឹងពីព័ត៌មានសន្តិសុខក្នុងតំបន់អាស៊ីប៉ាស៊ីហ្វិច។ សន្និសីទលើកទី១នៃ CSITRs អាស៊ីប៉ាស៊ីហ្វិចត្រូវបានប្រព្រឹត្តទៅនៅក្នុងប្រទេសជប៉ុននៅក្នុងឆ្នាំ ២០០២ APCERT គឺត្រូវបានធ្វើមួយឆ្នាំក្រោយមកនៅឯសន្និសីទក្នុងប្រទេសតៃប៉ិដែលត្រូវបានចូលរួមដោយ ១៤ CSIRTs អាស៊ីប៉ាស៊ីហ្វិច។ ដូចជានៅខែ សីហា ឆ្នាំ ២០០៧ APCERT មាន ១៤ សមាជិកស្របច្បាប់ និង ៦ សមាគមជាសមាជិក ។

សមាជិក បានយល់ស្របថាសព្វថ្ងៃឧបទ្វរហេតុសន្តិសុខកុំព្យូទ័រគឺធំធេង, បង្កឲ្យមានភាពស្មុកស្មាញ និងពិបាកដើម្បីត្រួតពិនិត្យសម្រាប់ពេលខ្លះនៅក្នុងស្ថាប័នមួយ ឬប្រទេសមួយ ហើយថាការឆ្លើយតបដ៏មានប្រសិទ្ធិភាពដ៏ច្រើនអាចត្រូវបានដាក់ពង្រាយដោយមានការសហការជាមួយសមាជិកដទៃទៀតនៃ APCERT។ ដូចជានៅក្នុងការចែង របស់ FIRST គោលគំនិតសំខាន់នៅក្នុង APCERT គឺភាពមានទំនាក់ទំនងប្រកបដោយភាពជឿទុកចិត្តនៅក្នុងរវាងសមាជិកទាំងអស់ចំពោះការផ្លាស់ប្តូរព័ត៌មាន និងការសហប្រតិបត្តិការ ជាមួយគ្នាទៅវិញទៅមក។ ដូច្នេះសកម្មភាពនានារបស់ APCERT គឺត្រូវបានរៀបចំឡើងដើម្បី:

56 APCERT, "Background," http://www.apcert.org/about/background/index.html.

- បន្ថែមនៅកិច្ចសហប្រតិបត្តិការក្នុងតំបន់អាស៊ីប៉ាស៊ីហ្វិច ព្រមទាំងអន្តរជាតិ
- ចូលរួមលើការអភិវឌ្ឍន៍នៅវិធានការនានាដើម្បីដោះស្រាយជាមួយទំហំធំនៃឧប្បទ្ទវហេតុ និងឧប្បទ្ទវហេតុសន្តិសុខបណ្តាញនៃតំបន់។
- ធ្វើឲ្យប្រសើរឡើងទៅលើការចែករំលែកសន្តិសុខព័ត៌មាន និងការផ្លាស់ប្តូរខាងបច្ចេកវិទ្យា រួមទាំងព័ត៌មានលើមេរោគកុំព្យូទ័រ អក្សរប្រកបដោយគ្រោះថ្នាក់ និងអ្វីដូចនេះផ្សេងទៀត។
- ធ្វើឲ្យប្រសើរឡើងលើការស្រាវជ្រាវរួមគ្នា ទៅលើបញ្ហាសាមញ្ញនានា។
- ជួយ CERT ផ្សេងទៀតនៅក្នុងតំបន់មួយនៅក្នុងការឆ្លើយតបយ៉ាងមានប្រសិទ្ធិភាពចំពោះឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រ និង
- ផ្តល់នៅដំបូន្មាន និងដំណោះស្រាយនានាទៅលើបញ្ហាដែលទាក់ទងទៅនឹងសន្តិសុខព័ត៌មាននៃតំបន់ និងការឆ្លើយតបចំពោះឧប្បទ្ទវហេតុ។

ការគ្រប់គ្រង CERT **របស់អឺរ៉ុប**[57]

ការគ្រប់គ្រង CERT (European Government CERT (EGC)) របស់អឺរ៉ុប គឺជាគណៈកម្មាធិការមិនមែនរដ្ឋាភិបាលដែលត្រូវបានសហការជាមួយ CERT ក្នុងបណ្តាប្រទេសនៅអឺរ៉ុប -សមាជិករបស់វាមាន ហ្វាំងឡង់ បារាំង អាល្លឺម៉ង់ ហុងគ្រី ញ៉ូដឺឡែន នរវែស ស្វ៊ែដន និងអង់គ្លេស។ តួនាទី និងភាពទទួលខុសត្រូវនានារបស់វាមានដូចជា:

- ចូលរួមអភិវឌ្ឍន៍វិធានការនានាដើម្បីដោះស្រាយលើទំហំធំធេងលើឧប្បទ្ទវហេតុ ឬក៏ឧប្បទ្ទវហេតុសន្តិសុខបណ្តាញនៃតំបន់។
- ជំរុញការចែករំលែកព័ត៌មាន និងការផ្លាស់ប្តូរព័ត៌មាន នៅក្នុងឧប្បទ្ទវហេតុសន្តិសុខ និងភាពគំរាមកំហែងនៃកូដប្រកបដោយគ្រោះថ្នាក់ និងភាពងាយរងគ្រោះ។
- កំណត់នៅតំបន់នៃចំណេះដឹង និងជំនាញដែលអាចត្រូវបានចែករំលែកនៅក្នុងក្រុម
- កំណត់នៅតំបន់នៃការស្រាវជ្រាវរួមគ្នា និងការអភិវឌ្ឍន៍លើកម្មវត្ថុដែល គឺជាផលប្រយោជន៍ចំពោះសមាជិកនានា និង
- ជំរុញឲ្យមានការបង្កើតការគ្រប់គ្រងលើ CSIRTs នៅក្នុងបណ្តាប្រទេសនៅអឺរ៉ុប។

57 EGC, http://www.egc-group.org.

ភ្នាក់ងារសន្តិសុខព័ត៌មាន និងបណ្តាញអឺរ៉ុប[58]

គោលបំណងនៃ ENISA គឺបន្ថែមនៅសន្តិសុខបណ្តាញ និងសន្តិសុខព័ត៌មាននៅក្នុងសហគមន៍អឺរ៉ុបតាមរយៈ ការបង្កើតនៃវប្បធម៌ NIS ។ វាគឺត្រូវបានបង្កើតឡើងនៅក្នុងខែមករា ឆ្នាំ ២០០៤ ដោយគណៈរដ្ឋមន្ត្រី និងសភាអឺរ៉ុប ដើម្បីឆ្លើយតបចំពោះ ឧក្រិដ្ឋកម្ម "Hi-tech" ។ វាមានតួនាទីដូចខាងក្រោម:

- ផ្តល់ការគាំទ្រដើម្បីធានានៅ NIS ក្នុងចំណោមសមាជិកនានានៃ ENISA ឬក៏ EU
- ជំរុញឲ្យមានការផ្លាស់ប្តូរប្រកបដោយស្ថេរភាពនៃព័ត៌មានរវាង ម្ចាស់ភាគហ៊ុននានា។ និង
- ធ្វើឲ្យប្រសើរឡើងនៅសហប្រតិបត្តិការនៃមុខងារផ្សេងៗ ដែលមានទំនាក់ទំនងទៅនឹង NIS។

ENISA គឺត្រូវបានរំពឹងថា នឹងចែកចាយចំពោះកិច្ចខិតខំប្រឹងប្រែងជាអន្តរជាតិនានាទៅលើការទប់ស្កាត់នៅមេរោគ និង Hacking និងការបង្កើតការត្រួតពិនិត្យ Online លើការគំរាមកំហែង។

៦.៣ CSIRTs ជាតិ

ប្រទេសមួចំនួនមានរៀបចំនៅ CSIRT ជាតិមួយ។តារាងលេខ១៣ រាយនៅប្រទេស និង CSIRT រៀងៗខ្លួនរបស់ពួកគេក៏ដូចជាគេហទំព័រដូច្នោះដែរ។

តារាងលេខ១៣.បញ្ជីនៃ CSIRT ជាតិ

ប្រទេស	ឈ្មោះផ្លូវការ	គេហទំព័រ
អាហ្សង់ទីន	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រនៃរដ្ឋបាលសាធារ ណរបស់អាហ្សង់ទីន	http://www.arcert.gov.ar
អូស្ត្រាលី	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័ររបស់ប្រទេសអូស្ត្រាលី	http://www.aucert.org.au
ប្រេស៊ីល	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័ររបស់ប្រេស៊ីល	http://www.cert.br

58 ENISA, "About ENISA," http://www.enisa.europa.eu/pages/About_ENISA.htm.

ប្រ៊ុណេដារ៉ូសាលីម	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័ររបស់ប្រ៊ុយណេ	http://www.brucert.org.bu
កាណាដា	ភាពរៀបចំបន្ទាន់នៅសុវត្ថិភាពសាធារណៈកាណាដា	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp
ឈីលី	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័ររបស់ឈីលី	http://www.clcert.cl
ចិន	ក្រុមបច្ចេកទេសឆ្លើយតបបន្ទាន់លើបណ្តាញកុំព្យូទ័រជាតិ មជ្ឈមណ្ឌលសហប្រតិបត្តិការនៃ ប្រទេសចិន	http://www.cert.org.cn
ដាណឺម៉ាក	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រប្រជាជនដាណឺម៉ាក	http://www.cert.dk
អែលសាវ៉ាដឺ	ក្រុមឆ្លើយតបសម្រាប់ ឧប្បទ្ទវហេតុសន្តិសុខកុំព្យូទ័រ	
ហ្វាំងឡង់	អាជ្ញាធរនិយតករគមនាគមន៍នៃប្រជាជនហ្វាំងឡង់	http://www.cert.fi
បារាំង	CERT រដ្ឋបាល	http://www.certa.ssi.gouv.fr
អាល្លឺម៉ង់	CERT-Bund	http://www.bsi.bund.de/certbund
ហុងកុង	មជ្ឈមណ្ឌលសហប្រតិបត្តិការ ឆ្លើយតបលើកុំព្យូទ័រ ហុងកុង	http://www.hkcert.org
ហុងគ្រី	CERT ហុងគ្រី	http://www.cert-hungary.hu
ឥណ្ឌា	CERT-In	http://www.cert-in.org.in
ឥណ្ឌូនេស៊ី	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រឥណ្ឌូនេស៊ី	http://www.cert.or.id
ជប៉ុន	មជ្ឈមណ្ឌលសហប្រតិបត្តិការ JPCERT	http://www.jpcert.or.jp
លីទីននី	LITNET CERT	http://cert.litnet.lt
ម៉ាឡេស៊ី	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័ររបស់ប្រទេសម៉ាឡេស៊ី	http://www.mycert.org.my
មិកស៊ិចកូ	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx

ញ៉ូដឺឡែន	មជ្ឈមណ្ឌលសម្រាប់ការការពារ ហេដ្ឋារចនាសម្ព័ន្ធ សំខាន់ៗ	http://www.ccip.govt.nz
ន័រវេស	អាជ្ញាធរសន្តិសុខជាតិន័រវេស	http://www.cert.no
ហ្វីលីពីន	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រហ្វីលីពីន	http://www.phcert.org
ប៉ូឡូញ	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រនៃប្រជាជនប៉ូឡូញ	http://www.cert.pl
កាតា	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រនៃប្រជាជនកាតា	http://www.qcert.org
ស៊ូឌីអារ៉ាប់ប៊ី	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រនៃប្រជាជនស៊ូឌីអារ៉ាប់ប៊ី	http://www.cert.gov.sa
សិង្ហបូរី	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រនៃប្រជាជនសិង្ហបូរី	http://www.singcert.org.sg
ស្លូវ៉ានី	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រនៃប្រជាជនស្លូវ៉ានី	http://www.arnes.si/english/si-cert
សាធារណៈរដ្ឋកូរ៉េ	មជ្ឈមណ្ឌលសហប្រតិបត្តិការ CERT កូរ៉េ	http://www.krcert.or.kr
អេស្ប៉ាញ	IRIS-CERT	http://www.rediris.es/cert
ស្វីតឌែន	មជ្ឈមណ្ឌលឧប្បទ្វរហេតុ នៃប្រទេសស្វីតឌែន	http://www.sitic.se
ថៃ	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រថៃ	http://www.thaicert.nectec.or.th
ទុយនេស៊ី	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រ - មជ្ឈមណ្ឌល សហប្រតិបត្តិការទុយនេស៊ី	http://www.ansi.tn/en/about_certtcc.Htm
ទួរគី	TP-CERT	http://www.uekae.tubitak.gov.tr
ចក្រភពអង់គ្លេស	VovCertUK	http://www.govcertuk.gov.uk
សហរដ្ឋអាមេរិក	ក្រុមឆ្លើយតបបន្ទាន់ លើកុំព្យូទ័រសហរដ្ឋអាមេរិក	http://www.us-cert.gov
វៀតណាម	ក្រុមឆ្លើយតបបន្ទាន់លើកុំព្យូទ័រវៀតណាម	http://www.vncert.gov.vn

Source: CERT, “National Computer Security Incident Response Teams,” Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

អ្វីដែលត្រូវអនុវត្តន៍

តើមាន CSIRT ជាតិក្នុងប្រទេសរបស់អ្នកដែរឬទេ ?

១. ប្រសិនបើមាន ពិពណ៌នាវាគឺស្ថិតនៅក្នុងក្រុមនៃគំរូដែលវាត្រូវបានចាត់ទុកនៅក្នុងបន្ទាប់មកអំពីតើវាធ្វើការដូចម្តេច ប៉ាន់ប្រមាណរបៀបដែលវារងការប៉ះពាល់នៅក្នុងការបង្កើតមុខងារផ្សេងៗរបស់វា។

២. ប្រសិនបើគ្មាន កំណត់នៅគំរូ CSIRT មួយណាដែលសាកសមប្រើនៅក្នុងប្រទេសរបស់អ្នក និងពិពណ៌នាអ្វីនឹងត្រូវបានគេស្នើដើម្បីបង្កើត CSIRT នៅក្នុងប្រទេសរបស់អ្នក។

សាកល្បងខ្លួនឯង

១. អ្វីគឺជាមុខងារសំខាន់ៗនៃ CSIRTs ?

២. តើ CSIRTs អន្តរជាតិ និង CSIRTs ជាតិខុសគ្នាដូចម្តេច ?

៣. អ្វីគឺជាតម្រូវការសម្រាប់ការបង្កើត CSIRTs មួយ ?

៧. ទិវឌ្ឍន៍នៃអាយុកាលរបស់គោលការណ៍សន្តិសុខព័ត៌មាន

ចំនុចនេះមានគោលបំណងផ្តល់នៅ

. ការឲ្យនៅសេចក្តីសង្ខេបនៃដំណើរការបង្កើតច្បាប់សន្តិសុខព័ត៌មាន និង

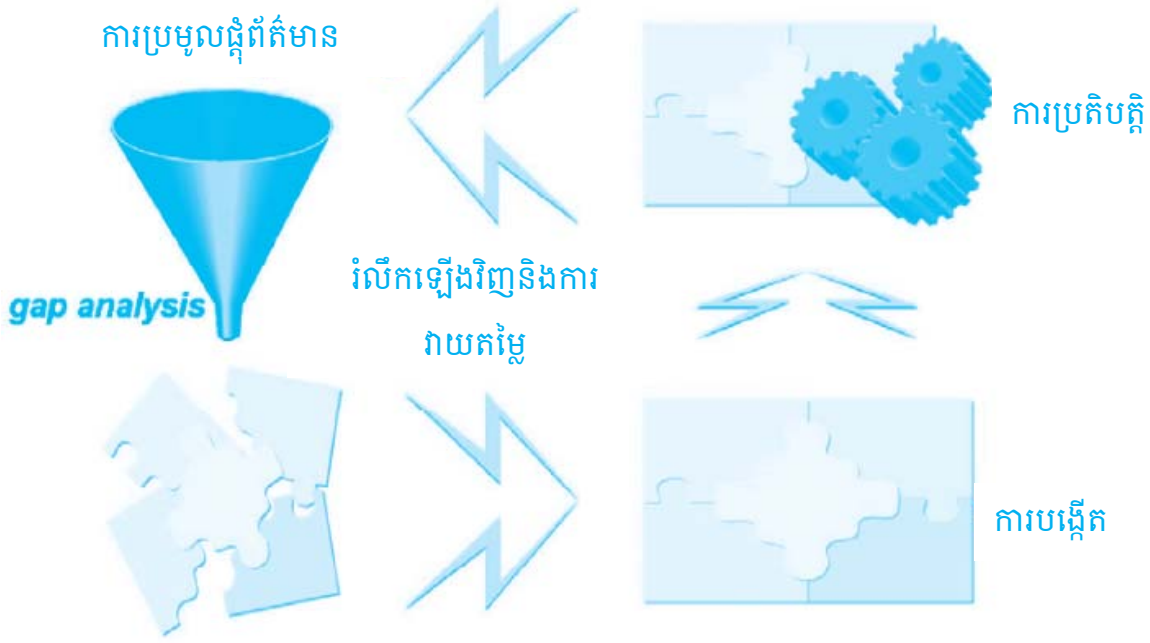
. ការពិភាក្សាលើបញ្ហានានាដែលអ្នកបង្កើតច្បាប់ត្រូវតែគិតគូចំពោះការបង្កើតច្បាប់សន្តិព័ត៌មាន។

អ្នកបង្កើតច្បាប់ត្រូវការធ្វើការគិតពិចារណាមួយចំនួន នៅក្នុងចំណោមពួកគេលើភាពសមហេតុផលមួយ សម្រាប់គោលការណ៍ច្បាប់ ធនធានដែលអាចរកបាន ទិសដៅរបស់គោលការណ៍ច្បាប់ ថវិការ និត តម្រូវការស្របច្បាប់នានា និងលទ្ធផលនៃគោលការណ៍ច្បាប់ដែលត្រូវបានរំពឹងទុក។ នៅក្នុងចំនុចនេះ ការគិតគួរទាំងនេះត្រូវបានលើកយកមកពិភាក្សានៅក្នុងបរិបទនៃដំណាក់កាលផ្សេងៗពីគ្នា នៃការបង្កើត ច្បាប់សន្តិសុខព័ត៌មាន។

វាគួរត្រូវបានកត់សម្គាល់ថាប្រទេសផ្សេងពីគ្នា នឹងមានបរិបទ និងការគិតគូរចំពោះគោលការណ៍ច្បាប់ខុស ប្លែក ពីគ្នាបន្តិចបន្តួច។ ដំណើរការបង្កើតច្បាប់បានពិពណ៌នានៅក្នុងចំនុចនេះគឺទៅតាមប្រភេទ និងផ្អែកលើការសន្មត់ថាគឺមិនមានគោលការណ៍ច្បាប់សន្តិសុខព័ត៌មានជាតិដែលមានស្រាប់នោះទេ។

ដូចនឹងគោលការណ៍ច្បាប់ផ្សេងទៀតដែរ វិវឌ្ឍន៍នៃអាយុកាលរបស់គោលការណ៍សន្តិសុខព័ត៌មានអាច ត្រូវបាន ចែកចេញជាបួនដំណាក់កាល: (១) ការប្រមូលផ្តុំនៅព័ត៌មាន និងការវិភាគលើចន្លោះប្រហោង (២)ការបង្កើតនៃគោលការណ៍ច្បាប់ (៣)ការអនុវត្តន៍នៃគោលការណ៍ច្បាប់ និង(៤) ត្រួតពិនិត្យ និងប្រតិកម្មតប (រូបទី១៩)។បន្ថែមលើនេះទៀតទំនងស្របច្បាប់ ស្ថាប័នសន្តិសុខព័ត៌មាន បច្ចេកវិទ្យាសន្តិសុខព័ត៌មាន និងអន្តរទំនាក់ទំនងក្នុងចំណោមពួកគេ។

រូបលេខ១៩.វិវឌ្ឍន៍នៃអាយុកាលរបស់គោលការណ៍សន្តិសុខព័ត៌មាន



៧.១ ការប្រមូលផ្តុំព័ត៌មាន និងការវាយតម្លៃលើចន្លោះប្រហោង

នៅក្នុងជំហានទីមួយនៅក្នុងការបង្កើតគោលការណ៍ច្បាប់សន្តិសុខព័ត៌មាន គឺជាការប្រមូលផ្តុំព័ត៌មាន និងការវិភាគលើខន្លោះប្រហោង។

នៅក្នុងការប្រមូលផ្តុំព័ត៌មាន វាគឺប្រើយ៉ាងមានប្រយោជន៍ដើម្បីរំលឹកឡើងវិញនៅឧទាហរណ៍នានានៃសន្តិសុខព័ត៌មាន និងគោលការណ៍ច្បាប់ដែលទាក់ទងដទៃទៀតជាមួយប្រទេសខ្លួនវា។

នៅក្នុងការវិភាគលើចន្លោះប្រហោង វាគឺសំខាន់ដើម្បីយល់អំពីហេដ្ឋារចនាសម្ព័ន្ធដែលមានស្រាប់ដែលទាក់ទងទៅនឹងសន្តិសុខព័ត៌មានដូចជាច្បាប់ និងប្រព័ន្ធដែលមានស្រាប់ ក៏ដូចជាតំបន់ និងចន្លោះប្រហោងនានាដែលត្រូវការបំពេញ។ វាគឺជាដំណាក់ការដ៏សំខាន់ពីព្រោះវាកំណត់នៅទិសដៅ ឬភាពជាចម្បងនៃគោលការណ៍ច្បាប់សន្តិសុខព័ត៌មានដែលត្រូវបានបង្កើតឡើង។

ប្រមូលផ្តុំព័ត៌មាន

ករណីប្រមូលផ្តុំពីនាយសមុទ្រ: នៅតំបន់ដែលករណីផ្សេងមានការជាប់ពាក់ព័ន្ធនៅក្នុងប្រទេសដទៃៗទៀត អ្នកបង្កើតច្បាប់គួរគិតទៅលើភាពស្រដៀងគ្នានៅក្នុង -

- កម្រិតនៃសន្តិសុខព័ត៌មានជាតិ
- ទិសដៅនៃការបង្កើតគោលការណ៍ច្បាប់
- ហេដ្ឋារចនាសម្ព័ន្ធ និងបណ្តាញ

ការគិតគូរពិភាពស្រដៀងគ្នាទាំងនេះ វត្ថុនានាដូចខាងក្រោមអាចត្រូវបានប្រមូលបាន:

- ព័ត៌មានចំពោះការបង្កើត និងការអភិវឌ្ឍន៍នៃស្ថាប័នានាដែលជាប់ពាក់ព័ន្ធនៅក្នុងសន្តិសុខព័ត៌មាន (មើលចំនុចទី៣ និង៦នៃគំរូនេះ)
- គោលការណ៍ច្បាប់ ច្បាប់ និងភាពស្របច្បាប់នានានៃស្ថាប័ននានៃសន្តិសុខព័ត៌មាន (មើលចំនុចទី៣)
- ត្រូវបានប្រើជាលក្ខណៈអន្តរជាតិនៅយុទ្ធវិធីសន្តិសុខព័ត៌មាន និងឧទាហរណ៍នានាពីប្រទេសផ្សេងៗ (មើលចំនុចទី៤)
- និន្នាការគំរាមកំហែង និងវិធានការទប់ស្កាត់ ឬត្រួតពិនិត្យនានាអាស្រ័យទៅលើប្រភេទនៃការវាយប្រហារ (មើលចំនុច ២ និងទី៦)
- វិធានការទប់ស្កាត់នានាសម្រាប់ការការពារឯកជនភាព (មើលចំនុចទី៥)

ការប្រមូលនៅឧបករណ៍ក្នុងស្រុកនានា: ទោះបីជាអ្នកបង្កើតច្បាប់ភាគច្រើនគឺមិនមែនជាអ្នកជំនាញនៅក្នុងសន្តិសុខព័ត៌មាន ប៉ុន្តែពួកគេធ្វើនៅសកម្មភាពជាច្រើនដែលទាក់ទង ឬជាប់ពាក់ព័ន្ធទៅនឹងសន្តិសុខព័ត៌មាន។ ជាពិសេសពួកគេប៉ិនប្រសប់ខាងផ្នែកច្បាប់ ផ្នែកស្របច្បាប់ និងគោលការណ៍ច្បាប់ទោរទន់ដោយផ្តោតទៅលើតំបន់ដ៏ជាក់លាក់នានា សហសម្ព័ន្ធក្នុងចំណោមពួកគេប្រហែលជាមិនអាចយើញជាក់ស្តែងភ្លាមចំពោះអ្នក បង្កើតច្បាប់ទាំងនោះ។ ដូច្នេះវាត្រូវការប្រមែប្រមូល វិភាគ និងវាយតម្លៃលើរាល់ច្បាប់ រាល់ភាពស្របច្បាប់ និងគោលការណ៍ច្បាប់នានាដែលត្រូវបានធ្វើឲ្យជាប់ទាក់ទង ឬជាប់ពាក់ព័ន្ធទៅនឹងសន្តិសុខព័ត៌មាន។

វិភាគលើចន្លោះប្រហោង

Sun Tzu's The Art of War និយាយថា "ស្គាល់សត្រូវរបស់អ្នក (Know Your enemy)" នេះមានន័យថា អ្នកគួរតែស្គាល់នៅដែនកំនត់របស់អ្នក ក៏ដូចដែលស្គាល់នៅសត្រូវរបស់អ្នក។ នៅក្នុងករណីនៃការបង្កើតច្បាប់សន្តិសុខព័ត៌មានក៏ដូចជាភាពងាយរងគ្រោះ និងភាពគំរាមកំហែងនានាចំពោះសន្តិសុខព័ត៌មាន។

ការវិភាគលើចន្លោះប្រហោងអាចត្រូវបានចែកចេញពីដំណាក់កាល:

១. យល់ដឹងពីសមត្ថភាព និងការប៉ុនប្រសប់របស់ប្រទេស - ឧទាហរណ៍ស្ថាប័ន និងធនធានមនុស្ស ក៏ដូចជាព័ត៌មាន និងហេដ្ឋារចនាសម្ព័ន្ធគមនាគមន៍ - នៅក្នុងតំបន់ទូទៅនៃសន្តិសុខព័ត៌មាន
២. កំនត់អត្តសញ្ញាណលើការគំរាមកំហែងពីខាងក្រៅចំពោះសន្តិសុខព័ត៌មាន។

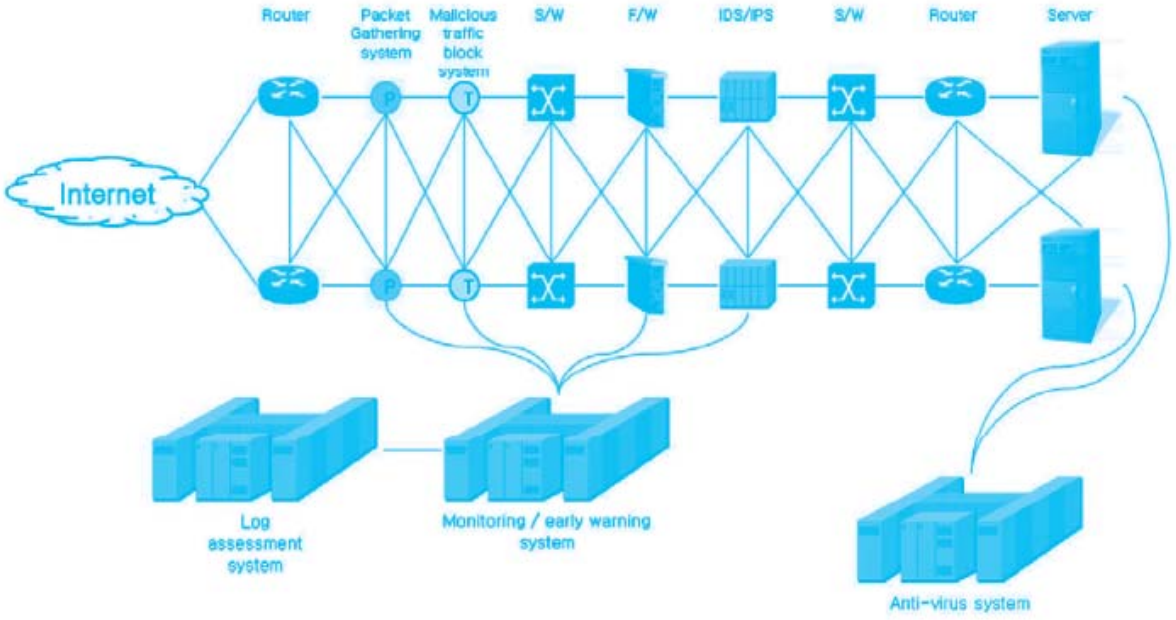
អ្នកបង្កើតច្បាប់ត្រូវការស្គាល់ជាមួយ**សន្តិសុខព័ត៌មាន ឬក៏ស្ថាប័ន និងធនធានមនុស្ស** - ឧទាហរណ៍គ្រឹះស្ថានឯកជន និងសាធារណៈនៅក្នុងតំបន់នានាដែលមានទំនាក់ទំនងចំពោះសន្តិសុខព័ត៌មាន។ ពួកគេគួរស្គាល់នៅស្ថាប័នផ្សេងដែលជាប់ពាក់ព័ន្ធនៅក្នុងការងារដែលមានទំនាក់ទំនងជាមួយសន្តិសុខព័ត៌មាន និងយល់ពីរយៈពេលរបស់ពួកគេនៃការងារ តួនាទី និងភាពទទួលខុសត្រូវនានា។ នេះគឺសំខាន់ដើម្បីកុំឲ្យជាន់គ្នាលើគម្រោងដែលមានស្រាប់សម្រាប់សន្តិសុខព័ត៌មាន។

នៅក្នុងចំនុចនេះផងដែរ ដែលអ្នកជំនួញនៅក្នុងសន្តិសុខព័ត៌មានគួរត្រូវបានកំនត់ និងត្រូវបានធ្វើជាលក្ខណៈបន្តើរៗ។ ដូចជាអ្នកជំនាញដែលមានប្រវត្តិតាមបែបផែនមួយៗតាមជំនាញខាងច្បាប់ គោលការណ៍ច្បាប់ បច្ចេកវិទ្យា អប់រំ និងជំនាញដែលទាក់ទងផ្សេងទៀត។

ហេដ្ឋារចនាសម្ព័ន្ធគមនាគមន៍ - ព័ត៌មានសំដៅទៅលើគ្រោង IT ដែលប្រមូល ដំណើរការរក្សាទុក ស្រាវជ្រាវ បញ្ជូន និងទទួលនៅប្រព័ន្ធគ្រប់គ្រងលើការត្រួតពិនិត្យអេឡិចត្រូនិច និងព័ត៌មាន។ យ៉ាងខ្លីនេះគឺជាប្រព័ន្ធ ព័ត៌មាន និងបណ្តាញ។ ការយល់នៅរូបរាងថ្មីនៃហេដ្ឋារចនាសម្ព័ន្ធ គមនាគមន៍ ព័ត៌មានគឺសំខាន់ពីចំនុចទស្សនៈខាងសេដ្ឋកិច្ច។ពីព្រោះតែការវិនិយោគដ៏ធំត្រូវការភ្ជាប់នៅទូទាំងប្រទេស

ការបង្កើតឲ្យមានស្រាប់នៃគមនាគមន៍ព័ត៌មានភាគច្រើនគឺមានផលប្រយោជន៍។ រូបរាងលេខ២០ បង្ហាញពីហេដ្ឋារចនាសម្ព័ន្ធគមនាគមន៍ព័ត៌មាន សាមញ្ញមួយសម្រាប់សន្តិសុខព័ត៌មាន។ វាមិនរួមនៅគ្រប់ផ្នែកដូចដែលបានស្នើ និងត្រូវបានបង្ហាញនៅទីនេះ ត្រឹមតែការគូសបង្ហាញនៅគោលគំនិតតែប៉ុណ្ណោះទេ។ កត់សម្គាល់លើភាពទំនាក់ទំនងគ្នាក្នុងចំណោមធាតុផ្សេងៗគ្នានៃបណ្តាញ។

រូបលេខ២០.គ្រោងប្រព័ន្ធ និងបណ្តាញសាមញ្ញមួយ



អ្នកបង្កើតច្បាប់ត្រូវការយល់ពីរបៀប ប្រព័ន្ធ និងបណ្តាញទឬទៅសម្រាប់ប្រព័ន្ធព័ត៌មាន ត្រូវបានបង្កើតឡើង។

ជំហានទី២នៅក្នុងការវិភាគលើចន្លោះប្រហោងគឺកំណត់នៅការគំរាមកំហែងពីខាងក្រៅចំពោះសន្តិសុខព័ត៌មាន។ដូចដែលបានបង្ហាញនៅក្នុងចំនុចទី២ ការគំរាមកំហែងនានាទៅលើព័ត៌មានសំខាន់គឺមិនត្រឹមតែកើនឡើងប៉ុន្តែផងដែរនោះបានក្លាយជាមានភាពដ៏ស្មុគស្មាញបំផុត។ អ្នកបង្កើតច្បាប់ត្រូវការដើម្បីយល់នៅការគំរាមកំហែងទាំងនេះដើម្បីអាចធ្វើការសម្រេចចិត្តថាវិធានការទប់ស្កាត់អ្វីគឺសំខាន់លើការប្រើប្រាស់។ ជាពិសេសអ្នកបង្កើតច្បាប់ត្រូវយល់:

- អត្រាដ៏មុតស្រួចនៃការគំរាមកំហែងនានាចំពោះសន្តិសុខព័ត៌មាន
- ប្រភេទនៃការវាយប្រហាថ្មីៗ និងសាមញ្ញបំផុត
- ប្រភេទនៃការគំរាមកំហែងនានា និងកម្រិតលើការរំពឹងទុករបស់ពួកគេនៃភាពខ្លាំងនៅក្នុងអនាគត។

ក្រោយពីធ្វើការវិភាគលើស្ថាប័នជាតិ, ធនធានមនុស្ស និង ហេដ្ឋារចនាសម្ព័ន្ធទំនាក់ទំនងពត៌មានវិទ្យា ព្រមទាំងការចាប់យកសមាសភាពគំរាមកំហែងក្នុងផ្នែកពត៌មានវិទ្យ វាមានសារៈសំខាន់ក្នុងការបង្វែរនូវសមាសភាពដែលមានលក្ខណៈទន់ខ្សោយ ។ វាកំពុងតែពង្រីកនូវប្រទេស ដែលអាចតទល់នឹងសមាសភាពគំរាមកំហែងខាងក្នុង ។ ការប្តេជ្ញានេះអាចធ្វើតាមរយៈការពិសោធន៍ខាងក្រោម

- មុខងារបច្ចុប្បន្នរបស់ CERT និងសមត្ថភាពនៃប្រតិកម្ម
- មុខងារបច្ចុប្បន្នរបស់អ្នកជំនាញសន្តិសុខពត៌មាន
- កំរិតនៃការសាងសង និង កំលាំងរបស់ប្រព័ន្ធសន្តិសុខពត៌មាន
- ច្បាប់ការពារប្រឆាំងនិងការចម្លងកម្មសិទ្ធពត៌មាន
- បរិស្ថានជុំវិញដើម្បីការពារកម្មសិទ្ធពត៌មាន

គោលបំនងនៃកំណត់នៃការវិភាគគឺ ដើម្បីអាចសំគាល់ពីការអនុវត្តវិធានការដែលផ្ទុយពីអ្វីដែលត្រូវបានយក ។ វាគួរតែត្រូវបានបញ្ជាក់ថា វាជាជំហានមូលដ្ឋានបំផុតក្នុងការតាក់តែងច្បាប់សន្តិសុខពត៌មាន ។

៧.២ ការកំនត់រូបមន្តច្បាប់សម្រាប់សន្តិសុខពត៌មាន

ការកំនត់នូវច្បាប់សន្តិសុខជាតិ គឺមានការចូលរួម (១) កំនត់នូវទិសដៅច្បាប់, (២) ការរួមគ្នារវាងស្ថាប័នសន្តិសុខពត៌មាន និង ការកំនត់តួនាទី និង ការទទួលខុសត្រូវ, (៣) ភាពច្បាស់នៃគ្រោងការច្បាប់សន្តិសុខពត៌មាន, (៤) បង្កើតនិងពិនិត្យឡើងវិញនូវច្បាប់ដើម្បីធ្វើឲ្យវា មានភាពត្រូវគ្នាជាមួយគោលការណ៍ដែលកំពុងអនុវត្ត, (៥) ផ្តល់ប្រាក់បំណាច់សំរាប់ការអនុវត្តច្បាប់សន្តិសុខ ។

១. ការកំនត់ទិសដៅច្បាប់នឹងការដំរុញទៅមុខ

ក្នុងករណីភាគច្រើន, ការស្វែងរកច្បាប់សន្តិសុខពត៌មាន គួរតែតម្រង់ទៅមុខយ៉ាងមុតមាំតាមរយៈរដ្ឋបាលជាជាងតាមផ្នែកឯកជន ។ ជាពិសេស, រដ្ឋាភិបាលគួរតែកំណត់ច្បាប់ ដើរតួជាអ្នកនាំមុខក្នុងការដាក់នូវហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ និងផ្តល់ ការគ្រាំទ្ររយៈពេលយូរ ។ វិស័យឯកជនចូលរួមទាន់ពេលដែលតាមគោលការណ៍គឺចូលរួមក្នុងការស្រាវ ជ្រាវ និង អភិវឌ្ឍន៍ និង កសាងប្រព័ន្ធ ។

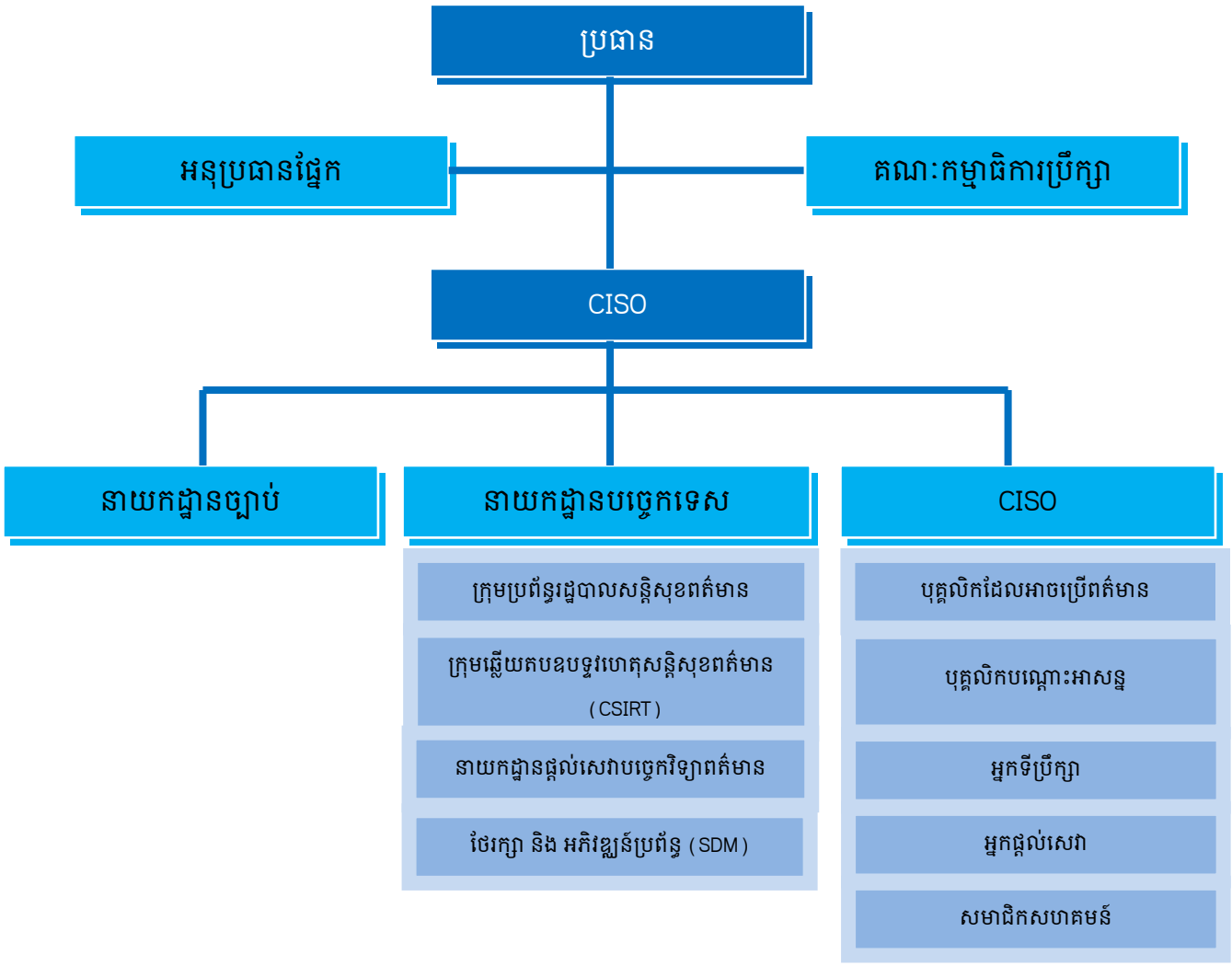
ការរៀបចំផែនការសម្រាប់ការចូលរួមរបស់វិស័យឯកជន រួមទាំងការលើកកម្ពស់ការយល់ដឹងជាមួយការលើកទឹកចិត្ត វិស័យឯកជនឲ្យទទួលនូវយុទ្ធវិធីសន្តិសុខពត៌មាន, នោះរដ្ឋាភិបាលគួរតែដើរតួជាអ្នក គាំទ្រ មិនមែនជាអ្នគ្រប់គ្រង ។ នេះរាមួបញ្ចូលទាំងការផ្សព្វផ្សាយវិធីណែនាំសន្តិសុខពត៌មាន ។

២. ការរួមគ្នារបស់ស្ថាប័នសន្តិសុខពត៌មាន និងការកំនត់នៅតួនាទីនិងការទទួលខុសត្រូវ[59]

នៅពេលដែលច្បាប់សន្តិសុខពត៌មានត្រូវបានដាក់ឲ្យប្រើ, ស្ថាប័នអនុវត្តន៍គួតែត្រូវបានបង្កើត ។ រូបភាព ទី ២១ បង្ហាញពីរចនាសម្ព័ន្ធនូវប្រភេទនៃស្ថាប័នសន្តិសុខពត៌មាន ។ រូបទី ២១ គំរូស្ថាប័នសន្តិសុខពត៌មាន

59 This section is drawn from Sinclair Community College, "Information Security Organization - Roles and Responsibilities," http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

រូបទី ២១ គំរូស្ថាប័នសន្តិសុខពត៌មានធម្មតាមួយ



សន្តិសុខពត៌មានជាតិមានខុសគ្នាបន្តិចបន្តួច ដោយពឹងលើបុគ្គលិកលក្ខណៈនិងវប្បធម៌នៃប្រទេសនីមួយៗ ។ ទោះបីជាយ៉ាងណាក៏ដោយ គោលការណ៍មូលដ្ឋានគឺដើម្បីធានានូវតួនាទីនិងការទទួលខុសត្រូវដ៏ច្បាស់លាស់មួយ ។

ស្ថាប័នរដ្ឋបាល

អនុប្រធានផ្នែក មានការទទួលខុសត្រូវសំខាន់លើការប្រមូលពត៌មាន ថែទាំ និង/ឬ កំនត់ការប្រើប្រាស់ ឬ “ធ្វើជាកម្មសិទ្ធិ” ដោយផ្នែករៀងខ្លួនរបស់គេ ។ ពួកគេប្រហែលកំនត់នូវមន្ត្រីសន្តិសុខពត៌មាន និងបុគ្គលផ្សេងទៀតដើម្បីជួយដល់មន្ត្រីសន្តិសុខពត៌មាន ក្នុងការអនុវត្តន៍ច្បាប់សន្តិសុខពត៌មាន ។ ការកំនត់

បុគ្គលទាំងនេះ ត្រូវតែធានាថាកម្មសិទ្ធពត៌មានដែលមានការគ្រប់គ្រងគឺត្រូវបានកំនត់នូវ ម្ចាស់កម្មសិទ្ធិ ដែលការប៉ាន់ស្មានលើហានិភ័យត្រូវបានធ្វើយ ហើយការសម្រាលលើដំណើរការដែល ពឹងផ្អែកលើ ហានិភ័យទាំងនោះត្រូវបានអនុវត្ត ។

អ្នកគ្រប់គ្រង (ប្រធាន អ្នកចាត់ការ ...។ល។) គ្រប់គ្រងបុគ្គលិក ជាមួយការប្រើប្រាស់ពត៌មាននិង បញ្ហា អនុវត្ត និង បង្គាប់ ការគ្រប់គ្រង សន្តិសុខពត៌មានដែលអាចអនុវត្តបានសម្រាប់ផ្នែកនានារបស់គេ ។ ពួកគេត្រូវតែធានាថា បុគ្គលិកទាំងអស់យល់ពីការទទួលខុសត្រូវរបស់គេរៀងៗខ្លួនលើសន្តិសុខពត៌មាន ហើយបុគ្គលិកនោះ មានតំរូវការចូលប្រើប្រាស់ដើម្បីធ្វើការងាររបស់គេ ។ អ្នកគ្រប់គ្រងគួរកំនត់ពេលត្រួតពិនិត្យ លើកម្រិត អ្នកចូលប្រើប្រាស់ទាំងអស់ដើម្បីធានាថាពួកគេមានធ្វើសកម្មភាពសមរម្យដើម្បីកែតំរូវ ភាពមិនស្របគ្នា ឬមិនជាក់លាក់ណាមួយ ។

មន្ត្រីប្រធានសន្តិសុខពត៌មាន (CISO) គឺមានតួនាទីធ្វើការសម្របសម្រួលនិងពិនិត្យលើច្បាប់សន្តិសុខ ពត៌មាន ។ ធ្វើការជិតស្និតជាមួយផ្នែកផ្សេងៗ, CISO អាចផ្តល់អនុសាសន៍ចំពោះអ្នកគ្រប់គ្រងលើ ផ្នែកជាក់លាក់ណាមួយដែលកំនត់នូវអ្នកតំណាងផ្សេងៗដើម្បី ត្រួតពិនិត្យ និងសម្របសម្រួលលើធាតុ ពិសេសណាមួយនៃច្បាប់ ។ CISO ក៏ជួយដល់ម្ចាស់កម្មសិទ្ធិពត៌មាននូវការអនុវត្តន៍សន្តិសុខពត៌មាន ក្នុង:

- បង្កើតនិងចែកចាយច្បាប់ប្រតិបត្តិ ដោយធ្វើការដំណើរការនិងប្រើនូវប្រភពពត៌មាន ។
- ដឹកនាំ/សម្របសម្រួលនូវការវាស់វែងនិងវិភាគលើសន្តិសុខពត៌មាន
- បង្កើតនូវការណែនាំដ៏សមហេតុផល និងការវាស់វែងដើម្បីការពារទិន្នន័យនិងប្រព័ន្ធនានា,
- ការជួយជាមួយការគ្រប់គ្រងនិងពិនិត្យ នូវភាពទន់ខ្សោយនៃប្រព័ន្ធសន្តិសុខ
- ដឹកនាំ/សម្របសម្រួលនូវសវនការសន្តិសុខពត៌មាន និង
- ជួយធ្វើការស៊ើបអង្កេត/រកដំណោះស្រាយ បញ្ហា និង/ឬ ការប្រព្រឹត្តល្មើសលើច្បាប់សន្តិសុខ ពត៌មានជាតិ ។

ស្ថាប័នបច្ចេកវិទ្យា

ក្រុមការងារប្រព័ន្ធរដ្ឋាបាលសន្តិសុខពត៌មាន អភិវឌ្ឍន៍ និង អនុវត្ត ការវាស់វែងដើម្បីធានាកិច្ចអនុវត្តន៍រដ្ឋបាលត្រួតពិនិត្យសន្តិសុខ ក្នុងការអនុញ្ញាតិឲ្យអ្នកមានភាគហ៊ុនអាចប្រើប្រាស់ពត៌មាន ខណៈពេលដែលជួបនូវភាពពេញលេញលក្ខណៈនៃច្បាប់ និង លក្ខណៈចាំបាច់, ក្នុងការការពារសិទ្ធិបុគ្គល, ភាពប៉ះពាល់និងពត៌មានសំខាន់ៗ ។

ក្រុមការងារអភិវឌ្ឍន៍ដំណើរការ និងស្តង់ដារដើម្បីផ្តល់ភាពអាចរកបាន, ការបញ្ចូលគ្នានិងភាពសម្ងាត់នូវប្រព័ន្ធពត៌មានរដ្ឋាបាល ដែលរួមទាំងដំណើរការសម្រាប់អ្នកប្រើប្រាស់ធ្វើការសំនូមពរការប្រើប្រាស់ដំបូង និង ការផ្លាស់ប្តូរ ការរៀបចំឯកសារនូវសិទ្ធិចូលប្រើប្រាស់របស់អ្នកប្រើប្រាស់ ហើយទាំងសិទ្ធិអ្នកប្រើប្រាស់(អ្នកគ្រប់គ្រង និង ការទទួលខុសត្រូវ និងដំណោះស្រាយដែលទាក់ទងនិងបញ្ហានានា ។ ក្រុមការងារគឺរួមទាំងមន្ត្រីផ្នែកសន្តិសុខពត៌មាននិង CISO ។ ក្រុមការងារត្រូវបានផ្តល់ការណែនាំដោយមន្ត្រីនាយកដ្ឋានសន្តិសុខពត៌មាន និង អ្នកចាត់ការប្រព័ន្ធរដ្ឋបាល ។

CSIRT ផ្តល់នូវពត៌មាននិងជួយដល់អ្នកកាន់ភាគហ៊ុន ក្នុងការអនុវត្តការវាស់វែងសកម្មភាពជាមុនដើម្បីកាត់បន្ថយនូវហានិភ័យចំពោះឧបទ្ទវហេតុសន្តិសុខនៃកុំព្យូទ័រ និង ក្នុងការស៊ើបអង្កេត ឆ្លើយតបនិងធ្វើឲ្យការខូចខាតមានកំរិតទាបបំផុតនៅពេលមានឧបទ្ទវហេតុផ្សេងៗកើតឡើង ។ CSIRT ក៏បានកំនត់និងណែនាំនូវសកម្មភាពតាមដានស្របពីនៃ CSIRT ក៏បង្កើតឡើងនូវក្រុមប្រតិបត្តិការដែលគ្រប់គ្រងអត្តសញ្ញាណដំបូង និង ការឆ្លើយតប, អទិភាពនៃភាពចាំបាច់និងការកំនត់នៃតំរូវការដែលត្រូវ ពង្រីក, និងក្រុមការងារគ្រប់គ្រងលើការឆ្លើយតបថ្នាក់ជាតិទៅលើឧបទ្ទវហេតុធំៗ និង សំខាន់ៗ ។ CISO និងបុគ្គលិកសមាជិកដែលទទួលអំនាចមកពីសេវាកម្មបច្ចេកវិទ្យាពត៌មានវិទ្យា និងការអភិវឌ្ឍន៍ប្រព័ន្ធនិងថែទាំ សុទ្ធតែជាផ្នែក នៃប្រតិបត្តិការ CSIRT ។ ក្រុមគ្រប់គ្រង **CSIRT** គឺបង្កើតឡើងដោយមន្ត្រីប្រធានពត៌មាន ប្រធានបូលីស នាយពត៌មានសាធារណៈ នាយកប្រធានសេវាកម្មបច្ចេកវិទ្យាពត៌មាន ប្រធានអភិវឌ្ឍន៍និងថែទាំប្រព័ន្ធ, CSICO, អ្នកគ្រប់ គ្រងប្រព័ន្ធនិងបណ្តាញ, អ្នកប្រឹក្សាច្បាប់, ទីប្រឹក្សាធនធានមនុស្ស, និងប្រតិភូដែលមានជំនាញខាង បច្ចេកទេសជាពិសេស អ្នកដែលតែងតាំងដោយអនុប្រធាន ។

បុគ្គលិក**នាយកដ្ឋានសេវាកម្មបច្ចេកវិទ្យាពត៌មាន** រួមទាំងប្រព័ន្ធនិងរដ្ឋបាលបណ្តាញ និងវិស្វករ និងអ្នកផ្តល់សេវាបច្ចេកទេស IT, អ្នកបច្ចេកទេសសម្រាប់ជួយអ្នកប្រើប្រាស់ និងរដ្ឋបាលទំនាក់ ទំនងតាមរយៈសម្លេង ។ ពួកគេទទួលខុសត្រូវលើការបញ្ចូលគ្នានូវ ឧបករណ៍សន្តិសុខពត៌មាន, ការត្រួតពិនិត្យនិងអនុវត្តន៍នៅក្នុងបរិយាកាសប្រព័ន្ធបណ្តាញ ។ ពួកគេទទួលរបាយការណ៍នូវសន្តិសុខពត៌មានដែលសង្ស័យថាមិនប្រក្រតី ឬមានឧបទ្ទវហេតុបណ្តាលមកពីអ្នកប្រើប្រាស់ ។

បុគ្គលិកសមាជិកអភិវឌ្ឍន៍ប្រព័ន្ធថែទាំ រួមទាំង អ្នកអភិវឌ្ឍន៍ និងរដ្ឋបាលប្រព័ន្ធទិន្នន័យ ។ ពួកគេអភិវឌ្ឍន៍, អនុវត្ត, បញ្ចូលគ្នា និងប្រតិបត្តិការអនុវត្តនូវសន្តិសុខខ្ពស់សម្រាប់ការគ្រប់គ្រងថ្នាក់

ផ្សេងៗ

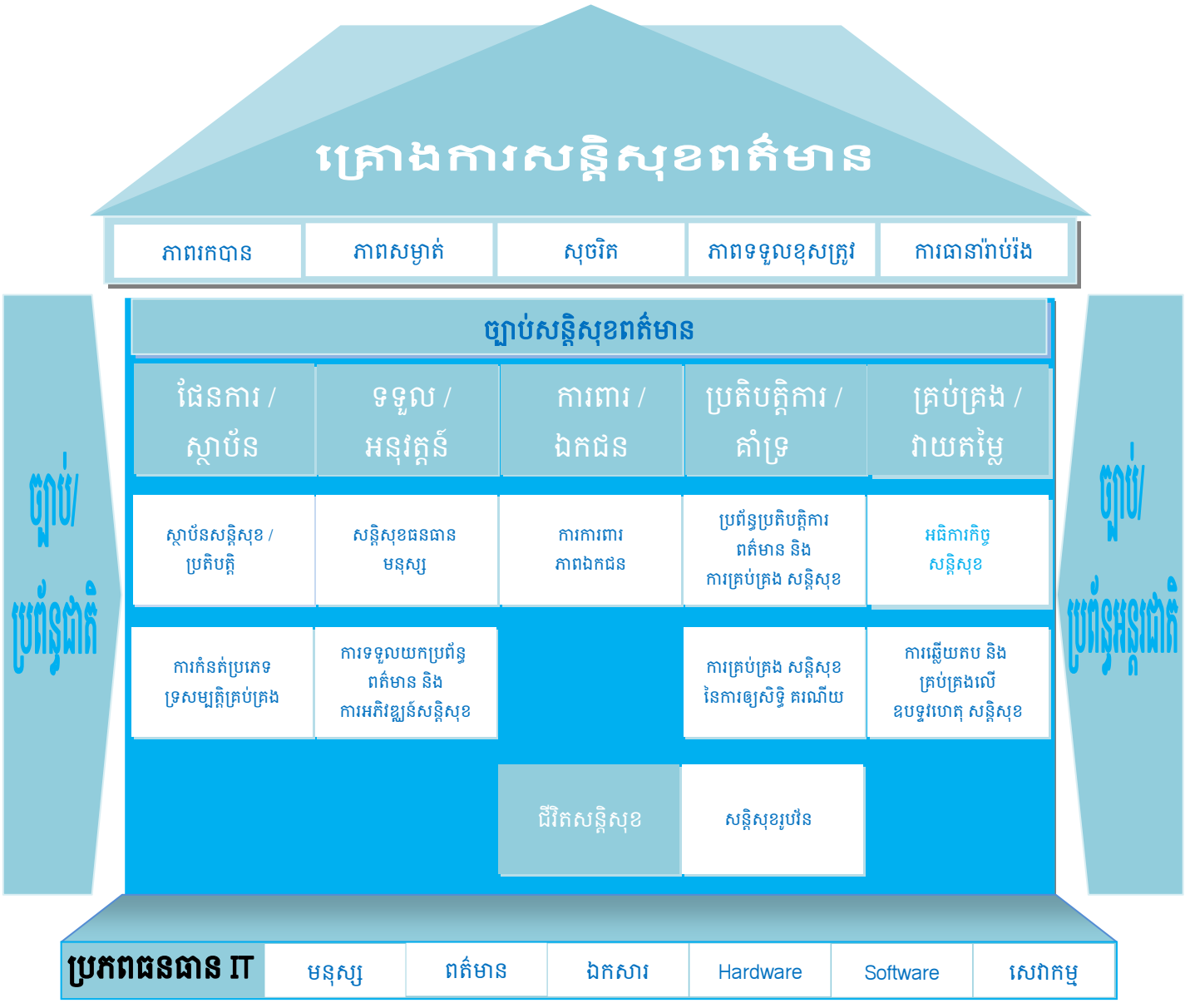
បុគ្គលិកដែលអាចប្រើប្រាស់ពត៌មាននិងប្រព័ន្ធពត៌មានត្រូវតែអនុវត្តតាមការគ្រប់គ្រងរបសច្បាប់ ជាតិ និងនីតិវិធី, ហើយនឹងការអនុវត្តន៍បន្ថែមឬនីតិវិធីដែលបង្កើតដោយអង្គភាពដឹកនាំ ឬ ប្រធាន ។ វារួមបញ្ចូលទាំងការការពារ លេខសម្ងាត់គណីយរបស់គេ និង របាយការណ៍ដែលសង្ស័យថា ប្រើប្រាស់ខុសក្នុងពត៌មាន ឬ ឧបទ្ទវហេតុសន្តិសុខពត៌មាន សម្រាប់ភាគីសមរម្យណាមួយ (ជាធម្មតាគឺអ្នកគ្រប់គ្រងរបស់គេ) ។

បុគ្គលិកសមាជិកបណ្តោះអាន្ន គឺត្រូវរាប់បញ្ចូលដូច បុគ្គលិកធម្មតា ហើយមានការទទួលខុសត្រូវខុសត្រូវដូចគ្នា ទាំងពេញម៉ោង និងក្រៅម៉ោង ក្នុងការប្រើប្រាស់ពត៌មាននិងប្រព័ន្ធពត៌មាន ។
អ្នកប្រឹក្សា, អ្នកផ្តល់សេវាកម្ម និងភាគីកិច្ចសន្យាទី ៣ ត្រូវបានអនុញ្ញាតិឲ្យប្រើប្រាស់ពត៌មាន ក្នុងទម្រង់ជា “តំរូវការនៃការចង់ដឹង” ជាមូលដ្ឋាន ។ ទិន្នន័យបណ្តាញដែលទាមទារដោយ ភាគីទី ៣ ត្រូវស្នើដោយ “អ្នកផ្តល់ជំនួយ” នៅក្នុងស្ថាប័នដែលធានាថា ភាគីអ្នកប្រើប្រាស់ទី ៣ យល់ពីការទទួលខុសត្រូវរៀងៗខ្លួន ពាក់ព័ន្ធនឹងទិន្នន័យបណ្តាយ, និងយល់ព្រមពីអនុប្រធាន ឬ ប្រធាន ។ អ្នកប្រើប្រាស់ត្រូវតែរក្សាទុកលេខសម្ងាត់ ឲ្យមានសុវត្ថិភាព និងអាចទុកចិត្តបានសម្រាប់សកម្មភាពផ្សេងៗនៃលទ្ធផលនៃការប្រើប្រាស់ ID របស់គេ ក្នុងរូបភាពសមស្របសម្រាប់ការគ្រប់គ្រងអ្នកប្រើប្រាស់នោះ ។

៣) ការកំនត់គ្រោងការងារសម្រាប់ច្បាប់សន្តិសុខពត៌មាន

គ្រោងការងារសន្តិសុខពត៌មាន គ្រោងការងារសន្តិសុខពត៌មានកំនត់នូវព្រំដែននៃច្បាប់សន្តិសុខពត៌មាន ។ វាធានាថា ច្បាប់យកនូវធនធាន IT មកធ្វើការពិចារណា (មនុស្ស, ឯកសារពត៌មាន, Hardware, Software, សេវាផ្សេងៗ) វាឆ្លុះបញ្ចាំងច្បាប់អន្តរជាតិ និង បទបញ្ជាផ្សេងៗ និង ជួបនឹងគោលការណ៍ពត៌មានដែល អាចរកបាន, ភាពលាក់ការ, ភាពសុច្ចរិត, ភាពទទួលខុសត្រូវនិងការធានា ។ រូបភាព ២២ បង្ហាញពីគ្រោង ការសន្តិសុខពត៌មាន

រូបទី ២២ បង្ហាញពីគ្រោង ការសន្តិសុខពត៌មាន



ច្បាប់សន្តិសុខពត៌មាន គឺជាចំនុចសំខាន់បំផុតនៃគ្រោងការសន្តិសុខពត៌មាន ។ ច្បាប់រួមបញ្ចូលជ្រាំផ្នែក ដែលនឹងពិភាក្សាដូចខាងក្រោម

a. **ផែនការ និង ស្ថាប័ន:** ក្នុងផ្នែកនេះគឺរួមទាំង សន្តិសុខនៃស្ថាប័ន និង ប្រតិបត្តិការ និង ការធ្វើចំណាត់ថ្នាក់ទ្រព្យសម្បត្តិនិងការគ្រប់គ្រង ។

ស្ថាប័ននិងប្រព័ន្ធ និងប្រតិបត្តិការ ដែលគ្របដណ្តប់:

- ស្ថាប័ននិងប្រព័ន្ធស្ថាប័នសន្តិសុខពត៌មានជាតិ
- និតិវិធីនៃស្ថាប័នសន្តិសុខពត៌មាននីមួយៗ
- ស្ថាប័ននិងការគ្រប់គ្រងសន្តិសុខពត៌មានជាតិ
- សហប្រតិបត្តិការជាមួយភ្នាក់ងារអន្តរជាតិពាក់ព័ន្ធ
- សហប្រតិបត្តិការជាមួយក្រុមជំនាញ

ការធ្វើចំណាត់ថ្នាក់ភាពជាម្ចាស់កម្មសិទ្ធិ និង គ្រប់គ្រង រួមបញ្ចូលទាំង

- ការផ្តល់ជាកម្មសិទ្ធិ និងចំណាត់ថ្នាក់ស្តង់ដា សម្រាប់ភាពជាម្ចាស់លើពត៌មានសំខាន់ៗ
- ការចុះបញ្ជីការអប់រំនិងការវាស់វែងហានិភ័យ នូវភាពជាម្ចាស់លើពត៌មានសំខាន់ៗ
- ការគ្រប់គ្រងលើសិទ្ធិប្រើប្រាស់លើភាពជាម្ចាស់លើពត៌មានសំខាន់ៗ
- ការផ្សាយ និងនាំចេញនូវទ្រពសម្បត្តិពត៌មានសំខាន់ៗ
- ការវាយតំលៃនិងទាញយកប្រើឲ្យអស់នូវទ្រព្យសម្បត្តិពត៌មានសំខាន់ៗ
- ការគ្រប់គ្រងសន្តិសុខឯកសារ

b. **ការទទួលយកនិង ការអនុវត្តន៍** ក្នុងផ្នែកនេះរួមបញ្ចូលទាំងសន្តិសុខ ធនធានមនុស្ស និង ការទទួលយកប្រព័ន្ធពត៌មាន និង ការអភិវឌ្ឍន៍សន្តិសុខ ។

សន្តិសុខធនធានមនុស្ស រួមបញ្ចូលការកំនត់នូវវិធីគ្រប់គ្រងក្នុងការរើសបុគ្គលិកថ្មីដែលរួមមាន -

- វិធានការផ្ទុយនឹងសន្តិសុខពត៌មាន និង ការបណ្តុះបណ្តាលសន្តិសុខ
- ដំណើរការនៃចន្លោះប្រហោរនៃបទបញ្ជាសន្តិសុខ និង ច្បាប់
- ការគ្រប់គ្រងសន្តិសុខ លើការប្រើប្រាស់របស់ភាគីទី ៣
- ការគ្រប់គ្រងសន្តិសុខ លើការប្រើប្រាស់របស់បុគ្គលដែលជួលមកពីក្រុមហ៊ុនខាងក្រៅ
- ធ្វើការនិងគ្រប់គ្រងភាគីទី ៣ និង បុគ្គលិកដែលជួលពីខាងក្រៅ
- ការគ្រប់គ្រងលើសន្តិសុខ បន្ទប់កុំព្យូទ័រនិងឧបករណ៍
- ប្រើប្រាស់មធ្យោបាយងាយស្រួលសំខាន់ៗ និង អគារ
- ដំណើរការនៃឧបទ្ទវហេតុសន្តិសុខ

ការទទួលយកប្រព័ន្ធពត៌មាន និង ការអភិវឌ្ឍន៍សន្តិសុខ ទាមទារ -

- ការត្រួតពិនិត្យលើសន្តិសុខនៅពេលដែលប្រព័ន្ធពត៌មានមួយទទួលបាន
- ការគ្រប់គ្រងសន្តិសុខ សម្រាប់ខាងក្នុងអគារ និង បុគ្គលិកដែលជួលពីខាងក្រៅលើកម្មវិធី
- ប្រព័ន្ធដាក់ពាក្យសម្ងាត់ជាតិ (ចាក់លេខសម្ងាត់នឹងកូនសោរ....)
- ធ្វើការសាកល្បងក្រោយពេលកម្មវិធីត្រូវបានអនុវត្តន៍
- ផ្តល់យោបល់លើតម្រូវការរបស់សន្តិសុខ នៅពេលអនុវត្តន៍ការជួលបុគ្គលពីខាងក្រៅ
- ពិនិត្យបញ្ជាក់លើសន្តិសុខជាមួយការអភិវឌ្ឍន៍និងការទទួលយក

c. **ការការពារភាពឯកជន:** ការរាប់បញ្ចូលនូវការការពារភាពឯកជន នៅក្នុងច្បាប់សន្តិសុខពត៌មានគឺមិនមែនជាភាពចាំបាច់ទេ ។ ទោះជាយ៉ាងណាក៏ដោយ, ការបញ្ចូលវាគឺវាមានអត្ថប្រយោជន៍ពីព្រោះការការពារភាពឯកជនគឺជាបញ្ហាអន្តរជាតិ ។ ការផ្តល់ការការពារភាពឯកជនគួរតែ រួមបញ្ចូលទាំង:

- ការប្រមូលពត៌មានផ្ទាល់ខ្លួននិងការប្រើប្រាស់
- មានការយល់ស្របជាមុន នៅពេលនិយាយពីអត្ថប្រយោជន៍នៃភាពឯកជនរបស់គេ
- PIA

d. **ប្រតិបត្តិការ និង ការគាំទ្រ:** ក្នុងផ្នែកនេះគឺទាក់ទងនិងបច្ចេកទេសសន្តិសុខ និង រូបវ័ន ។ ការប្រើបណ្តាញ និង ប្រព័ន្ធត្រូវបានដាក់ កម្រិតជាលំអិត, និងសន្តិសុខរូបវ័ន របស់ពត៌មាន និង ហេដ្ឋារចនាសម្ព័ន្ធទំនាក់ទំនងត្រូវបានកំនត់ ។

ប្រតិបត្តិការ ប្រព័ន្ធពត៌មាន និង គ្រប់គ្រងសន្តិសុខ: រួមមាន:

- ប្រតិបត្តិការ និង ការគ្រប់គ្រងសន្តិសុខលើម៉ាស៊ីនមេ, បណ្តាញ, កម្មវិធី application និងប្រព័ន្ធទិន្នន័យ ។
- អភិវឌ្ឍន៍ ប្រព័ន្ធសន្តិសុខពត៌មាន
- Log និង back-up ដែលប្រឆាំងនឹងសកម្មភាពស្របច្បាប់
- ការគ្រប់គ្រងការរក្សាទុកពត៌មាន
- ការប្រើប្រាស់ Computer ចល័ត
- ស្តង់ដារសម្រាប់ការទុកដាក់នឹងសន្តិសុខទិន្នន័យក្នុង Computer

ការគ្រប់គ្រងការផ្តល់សិទ្ធិឲ្យ Account - សិទ្ធិចូលប្រើប្រាស់និងការគ្រប់គ្រង Account ត្រូវតែកំនត់ ដើម្បីធានានូវភាពសម្ងាត់ក្នុងការប្រើប្រាស់កន្លែងផ្ទុកពត៌មានរបស់ជាតិ ។ រួមបញ្ចូលទាំង -

. ការចុះបញ្ជី, ការលុប, ការគ្រប់គ្រងឯកសិទ្ធិសម្រាប់អ្នកប្រើប្រាស់ នៃប្រព័ន្ធពត៌មានជាតិ

. ការគ្រប់គ្រង Account និង ឯកសិទ្ធិ នៃការធ្វើ encrypt លើបណ្តាញ

សន្តិសុខរូបវ័ន: សន្តិសុខរូបវ័នគឺសំដៅលើការការពារពត៌មាន និង ការទំនាក់ទំនងដែលផ្ទុកពត៌មាន សំខាន់ៗ ។ វារួមមាន -

. វិធី ធ្វើឲ្យមានរូបសណ្ឋាន និង គ្រប់គ្រងលើផ្នែកសន្តិសុខ

. ការគ្រប់គ្រងលើការចូលប្រើប្រាស់និងបញ្ជូនលើ Computer កណ្តាល

. ការការពារពីការខូចខាតដែលបណ្តាលមកពីគ្រោះធម្មជាតិ និង មហន្តរាយផ្សេងៗ

e. **ការគ្រប់គ្រងនឹងការរាស់វែង** ក្នុងផ្នែកនេះនៃច្បាប់សន្តិសុខពត៌មាន ទាមទារនូវរូបមន្តស្តង់ដារ និង ដំណើរការសម្រាប់ការការពារឧបទ្ទវហេតុសន្តិសុខ និង គ្រប់គ្រង និង ឆ្លើយតបចំពោះ ឧបទ្ទវហេតុដែលកើតឡើង ។

អធិការកិច្ចសន្តិសុខរួមមាន -

- បង្កើតផែនការអធិការកិច្ចសន្តិសុខ
- ធ្វើការអនុវត្តអធិការកិច្ចសន្តិសុខក្នុងពេលណាមួយ
- កំនត់នូវប្រធានបទនៃអធិការកិច្ចសន្តិសុខ និង គោលដៅរបាយការណ៍

ការគ្រប់គ្រងនឹងឆ្លើយតបលើឧបទ្ទវហេតុសន្តិសុខ ទាមទារការកំនត់ -

- ការងារនិងតួនាទីរបស់ស្ថាប័ននីមួយៗ ក្នុងការធ្វើដំណើរការឧបទ្ទវហេតុសន្តិសុខ
- នីតិវិធីសម្រាប់ការអង្កេត និង សម្គាល់លើមុខសញ្ញានៃឧបទ្ទវហេតុសន្តិសុខ
- នីតិវិធីដំណើរការឧបទ្ទវហេតុសន្តិសុខនិង វិធីក្នុងការឆ្លើយតប
- ការរាស់វែងត្រូវបានធ្វើបន្ទាប់ពីដំណើរការឧបទ្ទវហេតុសន្តិសុខ

៤. ការបង្កើត និង/ឬ ការកែសម្រួលច្បាប់ ដើម្បីឲ្យមានស្ថេរភាពជាមួយច្បាប់សន្តិសុខ ពត៌មានច្បាប់

ត្រូវតែមានស្ថេរភាពជាមួយច្បាប់សន្តិសុខពត៌មាន ។ គួរតែមានច្បាប់គ្រប់គ្រងលើស្ថាប័នរដ្ឋ និង សហគ្រាសឯកជន ។ តារាង ១៤-១៦ បង្ហាញពីច្បាប់ដែលពាក់ព័ន្ធនិងសន្តិសុខពត៌មានក្នុងប្រទេស ជប៉ុន, សហភាពអឺរ៉ុប និង សហរដ្ឋអាមេរិច ។ ក្នុងប្រទេសជប៉ុន, អ្នកតំណាងឲ្យច្បាប់ IT គឺសកម្ម ភាពមូលដ្ឋានក្នុងការកំនត់ទំរង់ពត៌មានកំរិតទំនើប និង បណ្តាញទូរគមនាគមន៍សង្គម ។ ច្បាប់នេះគឺ ជាស្តង់ដារមូលដ្ឋានគ្រឹះ សម្រាប់សន្តិសុខពត៌មាននៅក្នុងប្រទេស និង រាល់ច្បាប់ទាំងអស់ដែលត្រូវតែ អនុលោមតាមវា ។

តារាងលេខ ១៤ ច្បាប់នានាដែលទាក់ទងទៅនឹងសន្តិសុខព័ត៌មាននៅក្នុងប្រទេសជប៉ុន

ច្បាប់នានា	ទិសដៅឧស្សាហកម្ម	ទិសដៅនៃភាពស្របច្បាប់	ការជាកពិន័យ
ច្បាប់ស្តីពីអ្នកមិនមានសិទ្ធិដំណើរការលើកុំព្យូទ័រ	រាល់ឧស្សាហកម្ម	សកម្មភាពដែលជំរុញឲ្យត្រួតពិនិត្យមើលការប្រើប្រាស់ដោយគ្មានសិទ្ធិអនុញ្ញាតិនិងផ្តល់ការផ្តត់ផ្តង់នៅពត៌មាន ID របស់បុគ្គលផ្សេងម្នាក់ទៀតដោយគ្មានលក្ខខណ្ឌ ។	
សកម្មភាពទៅលើការការពារពត៌មានផ្ទាល់ខ្លួន	សហគ្រាសឯកជនដែលប្រើពត៌មានឯកជនសម្រាប់គោលបំណងក្នុងការធ្វើជំនួញ	ការគ្រប់គ្រងលើពត៌មានឯកជន(អាសយដ្ឋាន, សារអេឡិចត្រូនិច, និងអ្វីផ្សេងទៀត)	ការទទួលខុសត្រូវចំពោះបទឧក្រិដ្ឋ, រឺក៏រួចខ្លួន
សកម្មភាពទៅលើការចុះហត្ថលេខាដែលធ្វើឡើងដោយប្រព័ន្ធអេឡិចត្រូនិច និងការចេញលិខិតបញ្ជាក់		ជួយសម្រួលដល់ការធ្វើពាណិជ្ជកម្មតាមប្រព័ន្ធអ៊ិនធើរណិត ដែលទទួលប្រយោជន៍បានពីប្រព័ន្ធនោះ រួមទាំង ការធ្វើជំនួញនៅលើបណ្តាញ	

តារាងលេខ ១៥: ច្បាប់នានាដែលជាប់ពាក់ព័ន្ធនឹងសន្តិសុខព័ត៌មាននៅសហគមន៍អឺរ៉ុប

ច្បាប់នានា	ការពិពណ៌នាជាលម្អិត
A Common Regulatory Framework (Directive 2002/21/EC)	. តំណាងឲ្យគម្រោងសម្រាប់ភាពស្របច្បាប់របស់បណ្តាញទូរគមនាគមន៍ និងសេវាកម្មផ្សេងៗ ។ . គោលបំនងចំពោះការការពារឯកជនតាមរយៈបណ្តាញគមនាគមសន្តិសុខ
EU Directive on Data Protection (Directive 1995/46/EC)	. ការណែនាំទៅលើដំណើរនៃការផ្លាស់ប្តូរបានដោយសេរីសម្រាប់ពត៌មានឯកជន ។ . ច្បាប់ជាមូលដ្ឋានគ្រឹះដែលកំនត់ទៅលើការទទួលខុសត្រូវរបស់ប្រទេសជាសមាជិក និងការទទួលស្គាល់នៅសិទ្ធិអំណាចចុងក្រោយនៃបុគ្គលម្នាក់ៗទៅលើពត៌មានឯកជនរបស់ពួកគេ ។

	. មានការដែនកំនត់ច្រើនជាង ស្តង់ដាររបស់សហរដ្ឋអាមេរិច ។
EU Directive on Electronic Signatures (Directive 1999/93/EC) EU Directive on Electronic Commerce (Directive 2000/31/EC)	. ការគ្រប់គ្រងលើការប្រើប្រាស់នៅការចុះហត្ថលេខាតាមប្រព័ន្ធ អេឡិចត្រូនិច ។ . ធ្វើឲ្យស្របតាមច្បាប់លើការអនុវត្តនៃពាណិជ្ជកម្មលើប្រព័ន្ធ អេឡិចត្រូនិច ។
Cybercrime Treaty	. សន្ធិសញ្ញាអន្តរជាតិដ៏ទូលំទូលាយស្តីអំពីរលកសញ្ញាឧក្រិដ្ឋកម្ម . កំណត់នៅក្នុងលក្ខណៈលម្អិតលើរាល់សកម្មភាពឧក្រិដ្ឋដែលប្រើ លើប្រព័ន្ធអ៊ិនធើរណិត និង ការជាកពិន័យលើការទំនាក់ទំនងគ្នារបស់ជនទាំងនោះ ។
	.ស្នើឲ្យអ្នកផ្តល់សេវាកម្មគមនាគមន៍ការហៅទិន្នន័យពី ប្រាំមួយខែ ទៅម្តៃបួនខែ(ត្រូវបានប្រកាសឲ្យអនុវត្តន៍ក្រោយការវាយប្រហាររបស់ ភេរករដាច់ដោយឡែកពីគ្នានៅក្នុង ម៉ាត្រីដ និង ឡុងដុង នៅក្នុងឆ្នាំ ២០០៤ និង ២០០៥) ។

តារាងលេខ ១៦: ច្បាប់នានាដែលទាក់ទងនឹងសន្តិសុខពត៌មាននៅក្នុង សហរដ្ឋអាមេរិច

ច្បាប់ផ្សេងៗ	ទិសដៅឧស្សាហកម្ម	ទិសដៅឲ្យស្របទៅតាមច្បាប់	ការពិន័យ
សកម្មភាពគ្រប់គ្រងសន្តិសុខព៌តមានសហព័ន្ធឆ្នាំ ២០០២	ភ្នាក់ងាររដ្ឋាបាលសហព័ន្ធ	ភ្នាក់រដ្ឋបាលពត៌មាន, ប្រព័ន្ធ IT , កម្មវិធីសន្តិសុខពត៌មាន	
សកម្មភាពទទួលខុសត្រូវនិងឯកជនភាពលើការធានារ៉ាប់រងសុខុមាលភាពឆ្នាំ ១៩៩៦	គ្រឹះស្ថានឱសថ និង អ្នកផ្តល់សេវាខាងឱសថ	ទិន្នន័យអេឡិចត្រូចនិចនៃពត៌មានអំពីឱសថផ្ទាល់ខ្លួន	ការទទួលខុសត្រូវចំពោះបទឧក្រិដ្ឋ, រឹក៏រួចខ្លួន
Gramm-Leach-Bliley Act of 1999	ស្ថាប័នហិញ្ញវត្ថុ	ពត៌មានឯកជនរបស់អតិថិជន	ការទទួលខុសត្រូវចំពោះបទឧក្រិដ្ឋ, រឹក៏រួចខ្លួន
Sarbanes-Oxley Act of	ក្រុមហ៊ុនដែលបានចុះ	ការត្រួតពិនិត្យផ្ទៃក្នុង	ការទទួលខុសត្រូវ

2002	បញ្ជីនៃ បណ្ណាគ ហ៊ុន របស់សហរដ្ឋ អាមេរិច	និងការរក្សាទុក ហិរញ្ញវត្ថុសាធារណ៍	ចំពោះបទឧក្រិដ្ឋ, រឺក៏ រួចខ្លួន
សកម្មភាពពត៌មានលើ ការប្រព្រឹត្តល្មើសនឹង សន្តិសុខរក្សាទុកទិន្នន័យ California 2003	ភ្ញាក់ងាររដ្ឋបាលនិង សហគ្រាសឯកជននៅ California	ពត៌មានឯកជនដែល ត្រូវបានបំលែងជា អក្សរមើលពុំយល់	សេចក្តីសុខសាន្ត នឹង ការឲ្យដំណឹងជាលាយ លក្ខណ៍អក្សរចំពោះ ជនរងគ្រោះ ។

៥. ការរៀបចំគម្រោងថវិកាសម្រាប់ដំណើរការគោលការច្បាប់ពត៌មាន

ការអនុវត្តន៍ដំណើរការនៃគោលការណ៍ច្បាប់មួយស្នើឲ្យមានថវិការ ។ តារាងលេខ ១៧ បង្ហាញថវិកា សម្រាប់សន្តិសុខពត៌មាននៅប្រទេសជប៉ុន និង សហរដ្ឋនៅក្នុងឆ្នាំថ្មីៗនេះ ។

តារាងលេខ ១៧: ថវិការចំណាយលើការការពារពត៌មាននៃប្រទេសជប៉ុន និង សហដ្ឋអាមេរិច

ជប៉ុន	២០០៤	២០០៥
ថវិការចំណាយប្រចាំឆ្នាំសរុប	៨៤៨,៩៦៧,០០០,០០០ យ៉ែន	៨៥៥, ១៩៥,០០០,០០០ យ៉ែន
ថវិការចំណាយលើសន្តិសុខ ពត៌មាន	២៦៧,០០០,០០០ យ៉ែន	២៨៨,០០០,០០០ យ៉ែន
ថវិការសរុបគិតជាភាគរយ	0.0៣%	0.0៣%
សហរដ្ឋអាមេរិច	២០០៦	២០០៧
ថវិការចំណាយប្រចាំឆ្នាំសរុប	២,៧០៩,០០០,០០០,០០០ដុល្លារ	២,៧៧0,០០០,០០០,០០០ដុល្លារ
ថវិការចំណាយលើសន្តិសុខ ពត៌មាន	៥,៥១២,០០០,០០០ដុល្លារ	៥,៧៥៩,០០០,០០០ដុល្លារ
ថវិការសរុបគិតជាភាគរយ	0.២0៣%	0.២0៨%

អ្វីដែលត្រូវអនុវត្តន៍

ប្រសិនបើប្រទេសរបស់អ្នកមានគោលការណ៍ច្បាប់សន្តិសុខពត៌មានមួយ, គួសបញ្ជាក់ពីការអភិវឌ្ឍន៍របស់វានៅក្នុងក្រុមនៃគំនិតទាំងប្រាំរបស់ការបង្កើតគោលការណ៍ ច្បាប់ សន្តិសុខ ពត៌មានដែលបានពិពណ៌នានៅខាងលើ ។ ថានោះគឺពិពណ៌នាអំពី:

១. ទិសដៅគោលការណ៍ច្បាប់
២. អង្គភាពសន្តិសុខពត៌មាន
៣. គម្រោងលើគោលការណ៍ច្បាប់
៤. ច្បាប់នានាដែលគាំទ្រចំពោះគោលការណ៍ច្បាប់សន្តិសុខពត៌មាន
៥. ការផ្តល់នៅគម្រោងថវិការសម្រាប់សន្តិសុខពត៌មាន

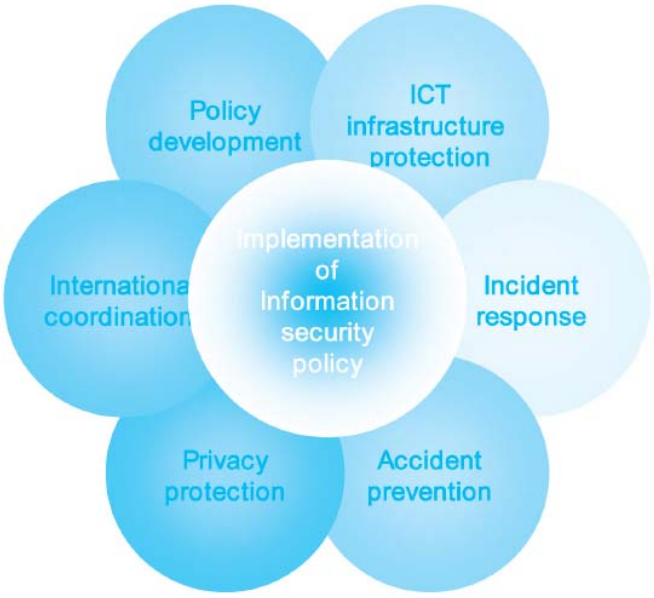
ប្រសិនបើប្រទេសរបស់អ្នកមិនមានគោលការណ៍សន្តិសុខពត៌មាន, បង្ហាញនៅគោលការណ៍ខ្លះៗ ដែលអាចប្រព្រឹត្តទៅបានសម្រាប់គំនិតនីមួយៗ ទាំងប្រាំខាងលើឆ្ពោះទៅរកការបង្កើតនៅគោល ការណ៍ច្បាប់ ។ ប្រើនៅសំនួរខាងក្រោមជាការនាំផ្លូវអ្នកដើម្បីធ្វើ :

១. អ្វីគឺជាទិសដៅនៃគោលការណ៍ច្បាប់សន្តិសុខពត៌មាននៅក្នុងប្រទេសរបស់អ្នក?
២. តើការបង្កើតឡើងដែលត្រូវបានរៀបចំនោះគឺវាត្រឹមត្រូវឬទេ ? តើស្ថាប័នមួយគួរតែត្រូវបានជាប់ពាក់ព័ន្ធ នៅក្នុងគោលការណ៍អភិវឌ្ឍន៍សន្តិសុខពត៌មាន និងការអភិវឌ្ឍន៍ក្នុងប្រទេសអ្នក ដែរឬទេ?
៣. តើអ្វីជាបញ្ហាជាក់លាក់មួយចំនួនដែលគួរដាក់ចូលទៅក្នុងគម្រោងគោលការណ៍ច្បាប់?
៤. តើច្បាប់ណាខ្លះដែលត្រូវបានអនុម័ត និង/ឬក៏ លុបចោលការគាំទ្រចំពោះគោលការណ៍ច្បាប់ សន្តិសុខ ?
៥. តើការគិតគូរលើគម្រោងថវិការ គួរត្រូវបានធ្វើការពិចារណាដែរឬអត់? កន្លែងណាដែលគម្រោង ថវិការគួរត្រូវបានលើកយកមកពិភាក្សា ?
អ្នកចូលរួមហ្វឹកហ្វឺនដែលមកពីប្រទេសជាមួយគ្នា អាចធ្វើសកម្មភាពនេះរួមគ្នា ។

៧.៣ ការប្រតិបត្តិ/ការអនុវត្តន៍គោលការណ៍ច្បាប់

ការអនុវត្តន៍ដ៏រលូននៃគោលការណ៍ច្បាប់សន្តិសុខពត៌មាន ស្នើឲ្យមានកិច្ចសហប្រតិបត្តិការនៅក្នុងចំណោម រដ្ឋាភិបាល, ឯកជន និង ភ្នាក់ងារអន្តរជាតិ ។ រូបរាងលេខ ២៣ បង្ហាញពីតំបន់ជាក់លាក់នានានៃការអនុវត្តគោលការណ៍ច្បាប់ពត៌មានដែលមានកិច្ចសហប្រតិបត្តិការគឺជាភាពចាំបាច់ ។

រូបលេខ ២៣: តំបន់សំរាប់កិច្ចសហប្រតិបត្តិការនៅក្នុងការអនុវត្តគោលការណ៍ច្បាប់សន្តិសុខពត៌មាន



ការអនុវត្តន៍គោលការណ៍ច្បាប់សន្តិសុខពត៌មាន

តារាងលេខ ១៨ តំណាងឲ្យរបៀបដែលរដ្ឋាភិបាល, វិស័យឯកជន, និង អង្គការអន្តរជាតិនានាបែងចែកនូវការអភិវឌ្ឍន៍គោលការណ៍ច្បាប់សន្តិសុខពត៌មានជាតិ

តារាងលេខ ១៨
កិច្ចសហប្រតិបត្តិការនៅក្នុងកិច្ចអភិវឌ្ឍន៍គោលការណ៍ច្បាប់សន្តិសុខពត៌មាន
(ឧទាហរណ៍)

វិស័យ	ការបែងចែកការងារនានាទៅលើការអភិវឌ្ឍន៍គោលការណ៍ច្បាប់
រដ្ឋាភិបាល	. យុទ្ធសាស្ត្រជាតិ និង អង្គភាពរៀបចំផែនការ: ធានាភាពត្រូវគ្នារវាងគោលការណ៍ពត៌មាន និង គម្រោងជាតិ ។ . អង្គភាពបច្ចេកវិទ្យា គមនាគមន និង ពត៌មាន: ធានានៅកិច្ចសហប្រតិបត្តិការនៃការបង្កើតគំរូបច្ចេកវិទ្យាសន្តិសុខព៌តមានរបស់ជាតិ ។ . អង្គភាពវិភាគនិន្នាការសន្តិសុខពត៌មាន: ជះត្រឡប់ទៅលើនិន្នាការសន្តិសុខ អន្តរជាតិនិងក្នុងស្រុក ព្រមទាំងការវិភាគនៅក្នុងគោលការណ៍ ។ . អង្គភាពវិភាគលើភាពស្របច្បាប់: ត្រួតពិនិត្យភាពស្របគ្នារវាងគោលការណ៍ច្បាប់សន្តិសុខព៌តមាននិងច្បាប់នានាដែលមានហើយ ។ . អង្គភាពព៌តមានជាតិ: កិច្ចសហប្រតិបត្តិការនៅក្នុងទិសដៅរៀបចំ និង ការបង្កើតយុទ្ធសាស្ត្រ ។ . ភ្ញាក់ងារស៊ើបអង្កេត: កិច្ចសហប្រតិបត្តិការនៅក្នុងដំណើរការនៃឧប្បទ្ទវហេតុសន្តិសុខ ។
វិស័យឯកជន	. ក្រុមហ៊ុនប្រឹក្សាសន្តិសុខពត៌មាន: ប្រើនៅភ្ញាក់ងារជំនាញនៅក្នុងការបង្កើតច្បាប់សន្តិសុខពត៌មាន ។ . ទីពិសោធន៍បច្ចេកវិទ្យាសន្តិសុខពត៌មានឯកជន: បង្កើតគំរូបច្ចេកវិទ្យាដែលជាប់ទាក់ទងទៅនឹងសន្តិសុខព៌តមាន ។ . នាយកដ្ឋានសន្តិសុខពត៌មាន នៃមហាវិទ្យាល័យ និង/ឬ ថ្នាក់បញ្ចប់: ផ្តល់នៅជំនាញនៅក្នុងការបង្កើតគោលការណ៍ច្បាប់ ។
អង្គការអន្តរជាតិ	. ធានាភាពចុះសម្រុងគ្នាជាមួយគំរូគោលការណ៍ច្បាប់អន្តរជាតិ . សហប្រតិបត្តិការឆ្លើយតបលើការគម្រាមកំហែង និង ឧប្បទ្ទវហេតុអន្តរជាតិ ។

ការការពារនិងការគ្រប់គ្រងលើហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានវិទ្យានិងទំនាក់ទំនង

ការប្រើប្រាស់ពត៌មានឲ្យមានប្រសិទ្ធិភាព(ការប្រមូល, ការរក្សាទុក ។ល។) ទាមទារមានរដ្ឋបាលត្រឹមត្រូវ និងការការពារលើហេដ្ឋារចនាសម្ព័ន្ធ ១ ។ ច្បាប់សន្តិសុខពត៌មានដ៏ល្អមួយមិនមានប្រយោជន៍មិនមានហេដ្ឋារចនាសម្ព័ន្ធ IC ។

ការគ្រប់គ្រងនិងការការពារដ៏មានប្រសិទ្ធិភាពលើហេដ្ឋារចនាសម្ព័ន្ធពត៌មានវិទ្យា និង ទំនាក់ទំនងទាមទារនូវការសហការគ្នារវាង ប្រព័ន្ធបណ្តាញ, ប្រព័ន្ធ និង អ្នគ្រប់គ្រងលើផ្នែក IT ។ វាក៏មានអត្ថប្រយោជន៍ពីសហប្រតិបត្តិការ រវាង ស្ថាប័នសាធារណ និង ឯកជន ។ (តារាងលេខ ១៩)

តារាងលេខ ១៩ សហប្រតិបត្តិការរដ្ឋបាលនិងការការពារ លើរចនាសម្ព័ន្ធពត៌មានវិទ្យានិង ទំនាក់ទំនង (ឧទាហរណ៍)

វិស័យ	ការបែងចែកការងារនានាទៅលើការអភិវឌ្ឍន៍គោលការណ៍ច្បាប់
រដ្ឋាភិបាល	. បណ្តាញទំនាក់ទំនងនិង៍ពត៌មានដែលពាក់ព័ន្ធនឹងស្ថាប័ន: កំនត់នូវសមាសភាពនិងកម្រិតនៃសន្តិសុខរបស់ពត៌មានជាតិនិងបណ្តាញទំនាក់ទំនង ។ . ទីពិសោធន៍បច្ចេកវិទ្យាទំនាក់ទំនងនិងពត៌មានវិទ្យា: ចែកចាយគំរូសាធារណ: និងទទួលយកនូវបច្ចេកវិទ្យាដែលប្រើប្រាស់ធនធានបាន
វិស័យឯកជន	. អ្នកផ្តត់ផ្តង់ ISP: សហការក្នុងសមាសភាពនៃព័ត៌មានវិទ្យាជាតិ និង បណ្តាញទំនាក់ទំនង ។ . ទីពិសោធន៍ពត៌មានវិទ្យា និងទំនាក់ទំនង: ផ្តល់នូវសេវាកម្ម អភិវឌ្ឍន៍បច្ចេកទេសនិងសហប្រតិបត្តិការ ក្នុងប្រតិបត្តិការពត៌មានបិតថេរ និង ហេដ្ឋារចនាសម្ព័ន្ធទំនាក់ទំនងនិង បច្ចេកវិទ្យាសន្តិសុខ ។
អង្គការអន្តរជាតិ	. ធានាភាពចុះសម្រុងគ្នាជាមួយគំរូគោលការណ៍ច្បាប់អន្តរជាតិ . សហប្រតិបត្តិការឆ្លើយតបលើការគម្រាមកំហែង និង ឧប្បទ្ទវហេតុអន្តរជាតិ ។

ទប់ទល់និងការឆ្លើយតបនឹងការគម្រាមកំហែងនិងឧបទ្ទវហេតុ

ការឆ្លើយតបដ៏មានប្រសិទ្ធិភាពលើការគម្រាមកំហែង និង រំលោភលើសន្តិសុខពត៌មានវិទ្យា គឺទាមទារនូវសហប្រតិបត្តិការរវាងស្ថាប័នពត៌មានជាតិ ភ្នាក់ងារស៊ើបអង្កេតនិង ស្ថាប័នច្បាប់ ព្រមទាំងអង្គការដែលដឹកនាំលើការត្រួតពិនិត្យឧបទ្ទវិហេតុសន្តិសុខ និងការគណនាការខូចខាត ។ វាក៏មានសារៈសំខាន់ក្នុងការសហការជាមួយស្ថាប័នដែលអាចវិភាគលើភាពទន់ខ្សោយនៃបច្ចេកទេស និង បង្កាប់នូវប្រតិវិធានការបច្ចេកទេស ។

តារាងលេខ ២0

សហប្រតិបត្តិការក្នុងការឆ្លើយតបលើឧបទ្ទវហេតុសន្តិសុខពត៌មានវិទ្យា (ឧទាហរណ៍)

ផ្នែក	វិភាគទាន
ស្ថាប័នរដ្ឋាភិបាល	. ស្ថាប័នឆ្លើយតបនឹងឧបទ្ទវហេតុសន្តិសុខ: ផ្តល់នូវការវិភាគស្ថានការ, ឆ្លើយតបនឹងឧបទ្ទវហេតុ hacking, និង បច្ចេកវិទ្យាដើម្បីឆ្លើយតបទៅនឹងការប្រព្រឹត្តល្មើសនិងឧបទ្ទវហេតុ ។ . ស្ថាប័នពត៌មានជាតិ: វិភាគនិងត្រួតពិនិត្យ លើសន្តិសុខពត៌មានដែលពាក់ព័ន្ធនិង ការប្រព្រឹត្តល្មើស និង ឧបទ្ទវហេតុ ។ . ភ្នាក់ងារស៊ើបអង្កេត: សហប្រតិបត្តិការជាមួយស្ថាប័ន រួមទាំងការចាប់ចង និងកាត់ទោសអ្នកដែលគេចោទ ។ . ស្ថាប័នដែលផ្តល់នូវការវាយតម្លៃលើសន្តិសុខ: ត្រួតពិនិត្យ ពីសុវត្ថិភាពនិងភាពជឿជាក់នៃបណ្តាញពត៌មាន និង សន្តិសុខពត៌មានដែលមានមូលដ្ឋានលើផលិតផល ។ . ស្ថាប័នអប់រំសន្តិសុខពត៌មានវិទ្យា: វិភាគលើមូលហេតុនៃឧបទ្ទវហេតុសន្តិសុខពត៌មានវិទ្យា និង អប់រំមនុស្សឲ្យការពារនូវឧបទ្ទវហេតុដែលកើតឡើងជ្រួន ៗ
វិស័យឯកជន	. ស្ថាប័នឆ្លើយតបឧបទ្ទវហេតុឯកជន: ផ្តល់នូវការឆ្លើយតប នឹង ជួយផ្នែកបច្ចេកទេស ។ . ភ្នាក់ងារស៊ើបអង្កេតឯកជន: សហប្រតិបត្តិការជាមួយភ្នាក់ងារស៊ើបអង្កេតថ្នាក់ជាតិ ។
ស្ថាប័នអន្តរជាតិ	. ក្នុងករណីវាជាការគម្រាមកំហែងនិងឧបទ្ទវហេតុថ្នាក់អន្តរជាតិ: រាយ ការ និង សហប្រតិបត្តិការជាមួយប៉ូលីសអន្តរជាតិ, CERT/CC

ការការពារឧបទ្ទវហេតុសន្តិសុខពត៌មានវិទ្យា

ការការពារលើការរំលោភលើសន្តិសុខពត៌មានវិទ្យា និង ឧបទ្ទវហេតុរួមទាំងការត្រួតពិនិត្យ ការអប់រំ និង ការផ្លាស់ប្តូរការគ្រប់គ្រង ។ CSIRT ជាតិ គឺ ជាស្ថាប័នត្រួតពិនិត្យសំខាន់ ។ ផ្នែកសំខាន់មួយគឺការ ផ្សព្វផ្សាងរវាងច្បាប់ពត៌មានវិទ្យា ។ ម្យ៉ាងវិញទៀត វាសំខាន់ក្នុងការអប់រំរដ្ឋាភិបាល និង បុគ្គលិកវិស័យឯកជន ព្រមទាំងសាធារណៈទូទៅ អំពីច្បាប់សន្តិសុខពត៌មាន ។ វាប្រហែលជាចាំបាច់ ក្នុងការផ្លាស់ប្តូរអាកប្បកិរិយា និង ឥរិយាបទដែលប៉ះទង្គិចនឹងសន្តិសុខពត៌មាន។ ការអប់រំសន្តិសុខ ពត៌មាន និង ការផ្លាស់ប្តូរការគ្រប់គ្រងត្រូវបានកំនត់នៅក្នុង US.SP800-16 (តំរូវការសម្រាប់ការហ្វឹកហ្វឺន ផ្នែកសន្តិសុខបច្ចេកវិទ្យាពត៌មាន)

តារាងលេខ ២១:
សហប្រតិបត្តិការរំលោភលើសន្តិសុខពត៌មានទិងការការពារឧបទ្ទវហេតុ (ឧទាហរណ៍)

ផ្នែក	សហប្រតិបត្តិការ
ស្ថាប័នរដ្ឋាភិបាល	. ភ្នាក់ងារត្រួតពិនិត្យ: បន្តការត្រួតពិនិត្យលើបណ្តាញ និង ការការពារ ការគម្រាមកំហែងសន្តិសុខកម្រិតខ្ពស់ ។ . ភ្នាក់ងារប្រមូល: ការចែករំលែកពត៌មានជាមួយស្ថាប័នអន្តរជាតិ និង តំបន់សន្តិសុខ . ស្ថាប័នហ្វឹកហ្វឺន: ការហ្វឹកហ្វឺនដែលកំនត់ពេលដូចគ្នា ដើម្បីអភិវឌ្ឍន៍ សមត្ថភាពក្នុងការឆ្លើយតបបានលឿនទៅលើការរំលោភសន្តិសុខពត៌មាន និង ឧបទ្ទវហេតុ ។
ស្ថាប័នឯកជន	. អ្នកផ្តល់ ISP អ្នកគ្រប់គ្រងសន្តិសុខ និង ក្រុមហ៊ុនកំចាត់មេរោគ: ផ្តល់នូវស្ថិតិចរាចរណ៍, ពត៌មានប្រភេទនៃការវាយហារ និង ទិន្នន័យរបស់ worms/មេរោគ ។
វិស័យអន្តរជាតិ	. ផ្តល់នូវព៌តមាននៃប្រភេទការវាយប្រហារ, ទិន្នន័យ worms/មេរោគ និងប្រភេទ មេរោគ ផ្សេងៗទៀតដែរ ។

សន្តិសុខឯកជន

សហប្រតិបត្តិការ គឺត្រូវការសម្រាប់ការបង្កើតនូវការរាស់រែងការការពារអ៊ិនធើណិតឯកជន, ការការពារ ឧបទ្ទវហេតុពត៌មានឯកជនក្នុងតំបន់, ការការពារពត៌មានជីវសាស្ត្រឯកជន និង ការធ្វើរបាយការណ៍លើការរំលោភលើឯកជនភាព ។

តារាងលេខ ២២:

សហប្រតិបត្តិការរំលោភលើសន្តិសុខពត៌មានឯការការពារឧបទ្ទវហេតុ (ឧទាហរណ៍)

ផ្នែក	សហប្រតិបត្តិការ
ភ្នាក់ងារដ្ឋាភិបាល	. ស្ថាប័នវិភាគលើប្រព័ន្ធ: ធ្វើជំនួញទាក់ទងនឹងពត៌មានឯកជន និងការវិភាគទៅលើទំនោរនៃការការពារពត៌មាន ខាងក្នុងនិងខាងក្រៅ ។ . ស្ថាប័នរៀបចំផែនការ: ជំរុញប្រព័ន្ធ/ច្បាប់ បច្ចេកទេស/ការរាស់រែងលើផ្នែករដ្ឋបាល, និងការគ្រប់គ្រងលើស្តង់ដារ . ជំនួយផ្នែកបច្ចេកទេស: សហប្រតិបត្តិការ អ្នកមានអាជ្ញាប័ណ្ណប្រើ ប្រាស់ រលកសញ្ញា សម្រាប់ជំនួញ . ស្ថាប័នសេវាកម្ម: ជួយក្នុងការសហប្រតិបត្តិការសម្រាប់ការដោះស្រាយលើការរំលោភឯកជនភាព និង Spam
ស្ថាប័នឯកជន	. ស្ថាប័នឯកជនសន្តិសុខពត៌មានផ្ទាល់ខ្លួន: ការទាមទារឲ្យចុះបញ្ជី និងរៀបចំនូវសមាគមសហប្រតិបត្តិការសំរាប់សន្តិសុខពត៌មានផ្ទាល់ខ្លួន ។ . ការប្រឹក្សាពីសន្តិសុខពត៌មានផ្ទាល់ខ្លួន ។
ស្ថាប័នអន្តរជាតិ	. សហប្រតិបត្តិការដើម្បីប្រើនូវ ស្តង់ដារ សន្តិសុខពត៌មានផ្ទាល់ខ្លួនអន្តរជាតិ ។

ការសម្របសម្រួលអន្តរជាតិ

សន្តិសុខពត៌មានគឺមិនអាចសម្រេចបានតាមរយៈលទ្ធិភាពរបស់ប្រទេសតែមួយនោះទេ ដោយសារការរំលោភលើសន្តិសុខមានទំនោរទៅរករូបភាពជាអន្តរជាតិ ។ ដូច្នេះការសម្របសម្រួលអន្តរជាតិ ក្នុងការការពារសន្តិសុខពត៌មាន, ទាំងផ្នែកឯកជន និងរដ្ឋាភិបាលត្រូវ តែកើតឡើង ។

សម្រាប់ផ្នែកឯកជន, ស្ថាប័នអន្តរជាតិដែលទាក់ទងក្នុងការជំរុញ និងការពារសន្តិសុខពត៌មានគឺ CERT/CC ។ ក្នុងចំណោមរដ្ឋាភិបាល ENISA (សម្រាប់សហភាពអឺរ៉ុប) និង ITU មានគោលដៅទៅរកការលើតម្កើងសហប្រតិបត្តិការសន្តិសុខពត៌មានក្នុងចំនោមប្រទេសជាច្រើន ។

ក្នុងប្រទេសនីមួយៗ គឺត្រូវតែមានស្ថាប័នរដ្ឋាភិបាលដែលមានតួនាទីសម្រួលដល់ការសហប្រតិបត្តិការរវាងរដ្ឋាភិបាល និង ស្ថាប័នឯកជន ជាមួយភ្ញាក់ងារនឹងស្ថាប័នអន្តរជាតិ ។

អ្វីដែលត្រូវអនុវត្តន៍

១. កំនត់ភ្ញាក់ងាររដ្ឋាភិបាល និងស្ថាប័នឯកជននៅក្នុងប្រទេសរបស់អ្នកដែលធ្វើសហប្រតិបត្តិការនៅក្នុងការអនុវត្តន៍ច្បាប់សន្តិសុខពត៌មានជាតិ ។ កំនត់សម្គាល់នៅស្ថាប័នអន្តរជាតិដែលគេត្រូវ ការធ្វើសហប្រតិបត្តិការផងដែរ ។

២. សម្រាប់ផ្នែកនីមួយៗ នៃសហប្រតិបត្តិការលើការអនុវត្តន៍ច្បាប់ពត៌មាននិងបង្ហាញនៅក្នុងរូបភាពទី ២៣, បង្ហាញពីសកម្មភាពជាក់លាក់ ឬ សកម្មភាពរបស់ភ្ញាក់ងារទាំងអស់នេះ និងស្ថាប័ន ដែលអាចទទួលរ៉ាប់រងនូវការងារនេះ ។

សិក្ខាកាមចូលរួមដែលមកពីប្រទេសតែមួយអាចធ្វើកិច្ចការនេះជាមួយគ្នា

៧.៤ ពិនិត្យនិងការវាយតម្លៃលើច្បាប់ស់សន្តិសុខពត៌មាន

ជំហានចុងក្រោយនៃការតាក់តែងច្បាប់សន្តិសុខពត៌មានគឺ ការវាយតម្លៃលើច្បាប់ និងការបន្តែមបង្រ្កប់លើផ្នែកអភិវឌ្ឍន៍ ។ ការពិនិត្យឡើងវិញលើច្បាប់ គឺមានសារៈសំខាន់ក្រោយពីប្រសិទ្ធិភាពនៃច្បាប់ សន្តិសុខពត៌មានត្រូវបានកំនត់ ។

ការប្រើប្រាស់ស្ថាប័នសាខនកម្ម

តួនាទីរបស់ស្ថាប័ន គឺធ្វើការប៉ាន់ប្រមាណនឹងវាយតម្លៃលើច្បាប់ ។ ស្ថាប័នបែបនេះគួរតែ ធ្វើសាវនកម្ម ជាប្រចាំលើច្បាប់សន្តិសុខពត៌មានជាតិ ។ ម្យ៉ាងវិញទៀត ស្ថាប័ននេះគួរតែជាស្ថាប័នឯករាជ្យ នៃស្ថាប័ន តាក់តែងច្បាប់សន្តិសុខព៌តមាន និងការអនុវត្តន៍របស់ ស្ថាប័ន ។

ការកែសម្រួលច្បាប់សន្តិសុខពត៌មាន

បញ្ហាជាធម្មតាត្រូវបានកំនត់ក្នុងពេលធ្វើសាវនកម្មច្បាប់ ។ គួរតែមានការប្រព្រឹត្តទៅក្នុងការកែសម្រួល ច្បាប់ដើម្បីលើកឡើងនូវបញ្ហាទាំងនេះ ។

ការប្រែប្រួលបរិស្ថាន

វាមានសារៈសំខាន់ក្នុងការតបទៅកនឹងការប្រែប្រួលក្នុងច្បាប់បរិស្ថាន ។ បំរែបំរួលកើតឡើងពីការគម្រាម កំហែងអន្តរជាតិ និងធ្វើឲ្យមានភាពទន់ខ្សោយ, បំរែបំរួលលើហេដ្ឋារចនាសម្ព័ន្ធ IT, ផ្លាស់ប្តូរលំដាប់ នៃពត៌មានសំខាន់ៗ, និងការផ្លាស់ប្តូរដ៏សំខាន់ដែលត្រូវបានឆ្លុះបញ្ចាំងភ្លាមនៅក្នុងច្បាប់សន្តិសុខពត៌មាន ជាតិ ។

សាកល្បងខ្លួនឯង

១) តើភាពខុសគ្នានៃដំណាក់កាលខួបជីវិតនៃច្បាប់សន្តិសុខពត៌មានប៉ះពាល់គ្នាយ៉ាងដូច ម្តេច? តើអ្នកអាចរំលងដំណាក់កាលទាំងនោះឬទេ? ហេតុអ្វីបានអាច? ហេតុអ្វីមិនអាច?

២) ហេតុអ្វីបានជាសហប្រតិបត្តិការ ក្នុងចំណោមកត្តាផ្សេងៗ បានជាសារៈសំខាន់ក្នុងការ អភិវឌ្ឍន៍ និង អនុវត្តន៍ច្បាប់សន្តិសុខពត៌មាន?

ឧទ្ទេសនាមន្ត

ឯកសារស្វែងយល់បន្ថែម

Butt, Danny, ed. 2005. *Internet Governance: Asia-Pacific Perspectives*. Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University. http://www.cert.org/csirts/csirt_faq.html.

CERT. Security of the Internet. Carnegie Mellon University. http://www.cert.org/encyc_article/tocencyc.html.

Dorey, Paul and Simon Perry, ed. 2006. *The PSG Vision for ENISA*. Permanent Stakeholders Group. http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

ESCAP. Module 3: Cyber Crime and Security. http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Europa. Strategy for a secure information society (2006 communication). European Commission. http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Information and Privacy Office. 2001. *Privacy Impact Assessment: A User's Guide*. Ontario: Management Board Secretariat. http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Information Security Policy Council. *The First National Strategy on Information Security*. 2 February 2006. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ITU and UNCTAD. 2007. Challenges to building a safe and secure Information Society. In *World Information Society Report 2007*, 82-101. Geneva: ITU. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, Georgia. 2004. *Steps for Creating National CSIRTs*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek. 2003. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/03hb001.pdf.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Paris: OECD. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Shimeall, Tim and Phil Williams. 2002. *Models of Information Security Trend Analysis*. Pittsburgh: CERT Analysis Center. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

The White House. 2003. *The National Strategy to Secure Cyberspace*. Washington, D.C.: The White House. http://www.whitehouse.gov/pcipb.

ការកត់សម្គាល់ផ្សេងៗសម្រាប់អ្នកបង្រៀន

ដូចជាបានកត់សម្គាល់រួចមកហើយ នៅក្នុងអត្ថបទខាងលើដែលមានឈ្មោះថា “អំពីមេរៀនជាបន្តបន្ទាប់” បាននិយាយថានៅក្នុងមេរៀននេះក៏ដូចនឹងមេរៀនដទៃទៀតដែរ គឺត្រូវបានរៀបចំឡើងដោយឲ្យពីគុណតម្លៃផ្សេងៗ គ្នាសម្រាប់ អ្នកសិក្សា និង ស្ថិតនៅក្រោមលក្ខខណ្ឌជាតិខុសៗគ្នា និងបំរែបំរួលរបស់វា ។ មេរៀន ទាំងនេះគឺត្រូវបានរៀបចំឡើង ដោយវិធីផ្សេងៗ អាចជា Online ឬ off-line នៅក្នុងផ្នែកមួយ ឬផ្នែកទាំងមូលរបស់មេរៀន ។ មេរៀនទាំងនេះអាចត្រូវ បានសិក្សាដោយឯកតោភាគី និង ដោយក្រុមអ្នកហ្វឹកហ្វឺន ទៅតាមស្ថាប័ននានាក៏ដូចជានៅក្នុងការិយាល័យរបស់ រដ្ឋាភិបាល ។ ប្រវត្តិនៃអ្នកហ្វឹកហ្វឺនដូចជានៅក្នុងពេលសិក្សា នៃវគ្គនីមួយៗ គឺដូចដែលមានបង្ហាញរួចមកហើយនៅក្នុង មាតិកា ។

ការ “សម្គាល់” ទាំងនេះផ្តល់ឲ្យអ្នកសិក្សានៅគំនិតមួយចំនួន និង ជាការស្នើនៅពត៌មានសម្រាប់មេរៀនឲ្យកាន់តែមានប្រសិទ្ធិភាពឡើង ។ សម្រាប់ការណែនាំអំពីយុទ្ធសាស្ត្រនិងវិធីទៅលើការហ្វឹកហ្វឺនគឺមាននៅក្នុងសៀវភៅក្បួន សម្រាប់ ការណែនាំនានា ដែលដូចជាវគ្គងាយស្រួលមួយសម្រាប់មេរៀនរបស់កម្មវិធីសិក្សាជាន់ខ្ពស់នៃ អាយស៊ីធី ពិសេស សម្រាប់ថ្នាក់ដឹកនាំក្នុងជួររដ្ឋាភិបាល ។ សៀវភៅក្បួននេះគឺអាចរកបាននៅក្នុងគេហទំព័រ: http://www.unapcict.org/academy ។

រចនាសម្ព័ន្ធវគ្គសិក្សា

សម្រាប់រយៈពេល ៩0 នាទី

ផ្តល់នូវគំនិតមូលដ្ឋានទូទៅនិងស្តង់ដារអន្តរជាតិ ឬ គោលការណ៍នៃសន្តិសុខពត៌មាននិងការការពារឯកជនភាព(ផ្នែកទី១ និង ទី ៥ នៃមេរៀន) ។ បញ្ជាក់ពីតម្រូវការសម្រាប់ភាពសមរម្យនិងសន្តិសុខពត៌មានដ៏មានសុវត្ថិភាព និង ច្បាប់ការពារឯកជនភាព ។

សម្រាប់រយៈពេល ៣ ម៉ោង

ចែកចេញជា ២ផ្នែក ។ ក្នុងផ្នែកទី ១ ផ្តោតទៅលើគំនិតមូលដ្ឋាន និង និន្នាការក្នុងសន្តិសុខពត៌មាន រួមទាំងការពិពណ៌នាពីការវិភាគលើការសំដៅទៅលើការគម្រាមកំហែងសន្តិសុខពត៌មាន(ផ្នែកទី ២) ។ ក្នុងផ្នែកទី ២ គឺផ្តោតទៅលើគំនិតមូលដ្ឋាន និង គោលការលើការការពារឯកជនភាព ធ្វើឲ្យមានភាពងាយស្រួលដល់ការពិភាក្សាលើបញ្ហាដែលប៉ះពាល់លើការការពារឯកជនភាព បរិយាយសង្ខេប លើការប៉ាន់ប្រមាណពីភាពប៉ះទង្គិចលើឯកជន ។

រយៈពេលពេញមួយថ្ងៃ (៦ម៉ោង)

ក្រោយពីពិនិត្យគំនិតសំខាន់ៗ និង គោលការណ៍របស់សន្តិសុខពត៌មាន និង ការការពារឯកជនភាព, សំដៅលើការអភិវឌ្ឍន៍និងការអនុវត្តលើច្បាប់សន្តិសុខពត៌មាន(ផ្នែកទី ៧) ។ អ្នកអាចចាប់ផ្តើមដោយសួរសំនួរអំពីទំនាក់ទំនងនៃច្បាប់នៃគោលការណ៍របស់សន្តិសុខពត៌មាន និង ការការពារឯកជនភាព ។ បន្ទាប់មកបង្ហាញត្រួសៗពីខួបជីវិតនៃច្បាប់សន្តិសុខពត៌មានមុនពេលផ្តោតទៅលើដំណើរការ នៃការបង្កើតរូបមន្តច្បាប់ ។ អ្នកដែលចូលរួមដែលមកពីប្រទេសដែលមានច្បាប់សន្តិសុខពត៌មានប្រហែលជាត្រូវបានសួរដើម្បីប៉ាន់ ប្រមាណមើលច្បាប់នេះ ក្នុងន័យគោលការណ៍ និង ដំណើរការនៃការពិភាក្សា, ខណៈដែលអ្នកដែលមក ពីប្រទេសដែលមិនមានច្បាស់សន្តិសុខពត៌មាន អាចនឹងត្រូវឲ្យធ្វើគម្រោងពីទិដ្ឋភាពខ្លះនៃច្បាប់នេះ (មើលសកម្មភាពសិក្សានៅចុងក្រោយនៃផ្នែកទី ៧.២)

រយៈពេល ២ ថ្ងៃ

ថ្ងៃទី ១ នឹងត្រូវធ្វើដូចដែលបានរៀបរាប់ខាងលើ, ខណៈដែលថ្ងៃទី ២ អាចនឹងផ្តោតទៅសកម្មភាពនិងគរុកោសល្យនៃសន្តិសុខពត៌មាន (ផ្នែកទី ៣ និង ទី ៤), ជាពិសេសគឺការបង្កើត CSIRTs(ផ្នែកទី ៦) ។ ឧទាហរណ៍ពីប្រទេសផ្សេងៗ អាចនឹងធ្វើការវិភាគដោយល្អិតល្អន់, ហើយអ្នកចូលរួមត្រូវបានលើកទឹកចិត្តក្នុការកំនត់នូវគំរូ CSIRT ដែលសមស្របជាងគេ និង ដើម្បីបង្កើតនូវយន្តការសន្តិសុខជាក់លាក់សម្រាប់បរិបទក្នុងប្រទេសរបស់គេ ។

ភាពអន្តរកម្ម

វាមានសារៈសំខាន់ក្នុងការធ្វើអន្តរកម្មនិងធ្វើកិច្ចការអ្នកចូលរួម ។ មេរៀនផ្តល់នូវពត៌មានដែលមានប្រយោជន៍ជាច្រើន ប៉ុន្តែការហ្វឹកហ្វឺនសិក្ខាកាមគឺទាមទារនូវការវិភាគដិតដល់លើពត៌មាននេះហើយប្រើវានៅកន្លែងដែលត្រូវការវា ។ ករណីសិក្សាខ្លះត្រូវបានផ្តល់នៅក្នុងមេរៀន និងបើអាចទៅរួចករណីសិក្សាទាំងនេះត្រូវបានពិភាក្សាក្នុងចំណោមជាគំនិតនិងគោលការណ៍នៃសន្តិសុខពត៌មាន ។ ប៉ុន្តែសិក្ខាកាមត្រូវបានចំរុញឲ្យស្វែងយល់បញ្ហាពិតប្រាកដ និងបញ្ហានៅក្នុងសន្តិសុខពត៌មាននិងការការពារឯកជនភាព ពីបរិបទផ្ទាល់ខ្លួនរបស់ពួកគេ ។

អំពី KISA

ភ្នាក់ងារសន្តិសុខពត៌មានកូរ៉េ (KISA) ត្រូវបានបង្កើតឡើងនៅឆ្នាំ ១៩៩៦ ដោយរដ្ឋាភិបាលដែលជាមជ្ឈមណ្ឌលដ៏ល្អឥតខ្ចោះសម្រាប់ប្រទេសជាតិទាំងមូល ក្នុងការជំរុញនូវប្រសិទ្ធិភាពនៃការតាក់តែងច្បាប់ទទួលខុសត្រូវសម្រាប់លើកកម្ពស់សន្តិសុខពត៌មាន ។ មុខងាររបស់វារួមទាំងការការពារនិងឆ្លើយតបទៅនឹងការរំលោភលើប្រព័ន្ធអ៊ិនធើរណិត ការឆ្លើយតបទៅលើ Spam , ការការពារឯកជនភាព(privacy protection), ហត្ថលេខាអេឡិចត្រូនិច, ការការពារលើហេដ្ឋារចនាសម្ព័ន្ធដែលមានភាពសំ ខាន់, ការវាយតម្លៃលើផលិតផលសន្តិសុខពត៌មាននិង ការគាំទ្រលើឧស្សាហកម្ម, ច្បាប់ស៊ីជំរៅនិងការអភិវឌ្ឍន៍បច្ចេកវិទ្យា, និង ការលើកកម្ពស់ស្មារតីយល់ដឹងលើការបង្កើតសង្គមពត៌មានដែលមានសុវត្ថិភាពនឹងជឿទុកចិត្តបាន ។

UN-APCICT

មជ្ឈមណ្ឌលហ្វឹកហ្វឺនអាស៊ីប៉ាស៊ីហ្វិចរបស់អង្គការសហប្រជាជាតិ សម្រាប់វិស័យ បច្ចេកវិទ្យា ពត៌មាន និង គមនាគមន៍ សម្រាប់ការអភិវឌ្ឍន៍ (UN-APCICT) គឺផ្នែកមួយនៃគណៈគម្មាធិការសង្គមនិងសេដ្ឋកិច្ច ប្រចាំការនៅតំបន់អាស៊ីប៉ាស៊ីហ្វិច (ESCAP) ។ UN-APCICT មានបំណងដើម្បីពង្រឹងសមាជិក ក្នុងតំបន់របស់ ESCAP ដើម្បីប្រើនៅវិស័យ ICT លើការអភិវឌ្ឍន៍សង្គមសេដ្ឋកិច្ចរបស់ពួកគេ តាមរយៈការកសាងសមត្ថភាពតាមស្ថាប័ននិងធនធានមនុស្ស ។ ការងារ របស់ UN-APCICT គឺផ្តោតលើគោលការណ៍ សំខាន់បី:

១. ការហ្វឹកហ្វឺន បន្ថែមនៅចំណេះដឹង នឹង ជំនាញផ្នែក ICT នៃអ្នកបង្កើតច្បាប់ និង សាស្ត្រាចារ្យ ICT រួមទាំងពង្រឹង សមត្ថភាពអ្នកបង្ហាត់ ICT និង វិទ្យាស្ថានហ្វឹកហ្វឺនលើវិស័យ ICT ។
២. ស្រាវជ្រាវ ខិតខំធ្វើការវិភាគលើការសិក្សានានាដែលទាក់ទងនឹងការអភិវឌ្ឍន៍ធនធានមនុស្សនៅក្នុង វិស័យ ICT និង
៣. ការផ្តល់នៅដំបូលន្ទាន ផ្តល់នៅសេវាកម្មឲ្យនៅដំបូលន្ទាននៅលើកម្មវិធីអភិវឌ្ឍធនធានមនុស្សនានា ចំពោះ សមាជិក ESCAP និង សមាជិកនានារបស់សមាគម ។

UN-APCICT មានទីតាំងនៅ អ៊ីចន(Incheon), សាធារណរដ្ឋកូរ៉េ

http://www.unapcict.org

ESCAP

ESCAP គឺជាដៃមួយរបស់អង្គការសហប្រជាជាតិសម្រាប់ការអភិវឌ្ឍន៍ក្នុងតំបន់ និង ចាត់ទុកថាជា មជ្ឈមណ្ឌលអភិវឌ្ឍ សង្គមនិងសេដ្ឋកិច្ចដ៏សំខាន់របស់អង្គការសហប្រជាជាតិប្រចាំតំបន់អាស៊ីប៉ាស៊ីហ្វិច។ អណាត្តិរបស់វា គឺ សហការប្រតិបត្តិការផ្តត់ផ្តងរវាងសមាជិកទាំង ៥៩ និង ៩ សហគមន៍ ។ ESCAP ផ្តល់នៅយុទ្ធសាស្ត្រតភ្ជាប់រវាង សាកលលោក និង កម្មវិធីរួមទាំងបញ្ហានានាជាមួយរាប់កម្រិតរបស់ ប្រទេស ។ វាផ្តល់នៅការគាំទ្រប្រទេសក្នុងតំបន់ ក្នុង ការពង្រឹងទីតាំងនានានៃតំបន់ និង កម្មវិធី កំសាន្តនៅក្នុងតំបន់នានា ដើម្បីធ្វើឲ្យទៅជាការប្រកួតប្រជែងផ្នែក សង្គមសេដ្ឋកិច្ចតែមួយគត់នៅក្នុង

សាកលភាវូបនីយកម្មរបស់ពិភពលោក ។ ការិយាល័យរបស់ ESCAP នៅក្នុងទីក្រុង បាងកក (Bangkok), ប្រទេសថៃ ។

http://www.unescap.org

កម្មវិធីសិក្សាជាន់ខ្ពស់ខ្ពស់នៃ អាយស៊ីធី ពិសេសសម្រាប់ថ្នាក់ដឹកនាំក្នុងជួររដ្ឋាភិបាល

http://www.unapcict.org/academy

កម្មវិធីសិក្សានេះគឺជាភាពទូលំទូលាយមួយនៃវគ្គហ្វឹកហ្វឺនលើវិស័យ ICT សម្រាប់ការអនុវត្តន៍ ដែលមានប្រាំបីមេរៀន និង មានគោលបំណងដើម្បីផ្តល់ឲ្យអ្នកបង្កើតច្បាប់ជាច្រើននៅចំណេះដឹងនិងជំនាញពិសេសចំពោះឱកាសអនុភាពដ៏ពេញលេញដែលបានបង្ហាញដោយ ICTs ដើម្បីសម្រេចបាននៅគោលបំនងរាប់រយរបស់ជាតិ និង ជាស្ពានចម្លងក្នុង ការបែងចែកជាលក្ខណៈឌីជីថល ។

មេរៀនទី ១-ការតភ្ជាប់រវាងការអនុវត្តលើវិស័យ ICT និងការអភិវឌ្ឍន៍ដ៏សំខាន់

ធ្វើឲ្យលេចឡើងនៅចំនុចសម្រាប់ការសម្រេចចិត្តនិងបញ្ហាសំខាន់ៗនានា, ពីច្បាប់ទៅកាន់ការអនុវត្ត ដោយការប្រើ ICTs សម្រាប់សម្រេចបាននៅគោលបំនងអភិវឌ្ឍន៍រាប់លាន ។

មេរៀនទី ២-ICT សម្រាប់ការអភិវឌ្ឍន៍ ប្រតិបត្តិការ និង ការគ្រប់គ្រង

ផ្តោតលើការបង្កើតច្បាប់ ICTD និង គ្រប់គ្រង, និងផ្តល់នៅពត៌មានយ៉ាងសំខាន់លើការរំពឹងទុកនានានៃ ច្បាប់ជាតិ យុទ្ធសាស្ត្រ គម្រោងការណ៍នានាដើម្បីជំរុញ ICTD

មេរៀនទី ៣-ការអនុវត្តនៅប្រព័ន្ធរដ្ឋាភិបាលអេឡិចត្រូនិច (e-Government)

ធ្វើការវិភាគលើ មនោភាព គោលការណ៍ និងប្រភេទនៃការអនុវត្តនានា ។ វាពិភាក្សាផងដែលនៅរបៀបម៉េច ដែលប្រព័ន្ធ e-government គឺត្រូវបានកសាង និង កំណត់លើការបង្កើត

មេរៀនទី ៤-និន្នាការនានារបស់ ICT សម្រាប់ថ្នាក់ដឹកនាំរដ្ឋាភិបាល

ផ្តល់នៅការគិតគូចូលទៅក្នុងនិន្នាការថ្មីៗនៅក្នុងវិស័យ ICT និង ទិសដៅអនាគតរបស់វា ។ វាក្រឡេកមើល ផងដែល លើការពិចារណានានាអំពីបច្ចេកវិទ្យា និង គោលការណ៍ច្បាប់ នៅពេលធ្វើការសម្រេចចិត្តសម្រាប់ ICTD ។

មេរៀនទី ៥-ការគ្រប់គ្រងប្រព័ន្ធ អ៊ីនធើរណិត

ពិភាក្សាទៅលើការអភិវឌ្ឍន៍នៃគោលការណ៍ច្បាប់និងវិធីសាស្ត្រនានាជាអន្តរជាតិដែលគ្រប់គ្រងការប្រើប្រាស់ និង ដំណើរការនៃប្រព័ន្ធ អ៊ីនធើរណិត ។

មេរៀនទី ៦-បណ្តាញ និង សុវត្ថិភាពព័ត៌មាន និង ឯកជន

បង្ហាញអំពីបញ្ហា និង និន្នាការនានានៃសុវត្ថិភាពព័ត៌មាន, និង ដំណើរការប្រតិបត្តិបង្កើតគំរូយុទ្ធសាស្ត្រមួយ សម្រាប់សុវត្ថិភាពព័ត៌មាន

មេរៀនទី ៧- ការគ្រប់គ្រង់គម្រោង ICT នៅក្នុងទ្រឹស្តី និង អនុវត្តន៍

ណែនាំអំពីគំនិតមួយចំនួនលើការគ្រប់គ្រងគម្រោង ដែលជាប់ទាក់ទងចំពោះគម្រោង ICTD, រួមមានពីរបៀបដំណើរការប្រតិបត្តិ វិន័យមួយចំនួនលើការគ្រប់គ្រងគម្រោងដែលបានប្រើជាទូទៅ។

មេរៀនទី ៨- ជម្រើសលើការផ្តល់មូលនិធិនៃ ICT សម្រាប់ការអភិវឌ្ឍន៍

ស្វែករកនៅជម្រើសនានាលើការផ្តល់នៅមូលនិធិសម្រាប់ ICTD និង គម្រោង e-government ។ ដៃគូឯកជនសាធារណ៍ គឺវាសំខាន់ដូចទៅនឹងជម្រើសលើការផ្តល់មូលនិធិដ៏មានប្រយោជន៍មួយក្នុងការអភិវឌ្ឍប្រទេសមួយចំនួន ។

មេរៀនទាំងនេះគឺបាននឹងកំពុងធ្វើទៅតាមការសិក្សានៅក្នុងតំបន់ដោយដៃគូ *Academy* ថ្នាក់ជាតិដើម្បីធានាថាមេរៀនទាំងនោះគឺត្រូវគ្នា និង ជួបនឹងការចង់បានរបស់អ្នកបង្កើតច្បាប់នៅក្នុងប្រទេសផ្សេងៗជាច្រើន ។ មេរៀនទាំងនេះ គឺបានត្រូវគេបកប្រែទៅជាភាសាផ្សេងៗ ។ ច្រើនជាងនេះ មេរៀនទាំងនេះត្រូវបានធ្វើការកែតម្រូវឲ្យទាន់សភាពការជារឿយៗ ដើម្បីធានាថាវាត្រូវគ្នានឹងសេចក្តីត្រូវការរបស់អ្នកច្បាប់ និងមេរៀនមេរៀនថ្មីៗទៀតដែលត្រូវបានគេអភិវឌ្ឍ ដែលផ្តោតលើ ICTD សម្រាប់សតវត្សទី ២១ ។

APCICT Virtual Academy (AVA □ http://ava.unapcict.org)

- ទម្រង់សិក្សាពីចម្ងាយតាមប្រព័ន្ធ Online សម្រាប់ *Academy*
- ត្រូវបានបង្កើតឡើងដើម្បីធានាថាមេរៀនរបស់ *Academy* រួមមាន ការបង្រៀនជាក់ស្តែងការធ្វើបទបង្ហាញ និងមេរៀនសិក្សានីមួយៗ គឺអាចរកបាននៅលើប្រព័ន្ធ Online ។
- អាចឲ្យអ្នកសិក្សា សិក្សាលើខ្លឹមសារនានាទៅតាមសមត្ថភាពរបស់ខ្លួនពួកគេផ្ទាល់ ។

មជ្ឈមណ្ឌលសហប្រតិបត្តិការលើប្រព័ន្ធអេឡិចត្រូនិច (e-Co Hub – http://www.unapcict.org/ecohub)

- ប្រភពធនធាន និង ការចែករំលែកចំណេះដឹងបណ្តាញសម្រាប់ ICTD
- ផ្តល់នៅភាពងាយស្រួលក្នុងការដំណើរការលើប្រភពចំណេះដឹងដែលផ្តល់ដោយមេរៀន ។
- អ្នកប្រើប្រាស់អាចចូលរួមការពិភាក្សាលើប្រព័ន្ធ Online និង ក្លាយជាផ្នែកមួយនៃសហគមន៍ online របស់ e-Co Hub នៃការអនុវត្ត ដែលរក្សានៅការចែករំលែក និង ការពង្រីកនៅចំណេះដឹងផ្អែកលើ ICTD ។

ចុះឈ្មោះតាមប្រព័ន្ធ Online ដើម្បីទទួលបានប្រយោជន៍ពេញលេញពីសេវាកម្មនានាដែលបានផ្តល់នៅក្នុង AVA និង e-Co Hub ជាមួយគេហទំព័រ http://www.unapcict.org/join_form