सी०एस०आई०आर०टी० कैसे प्रतिपादित करें विषय पर एक चरणबद्ध अभिगम

उदाहरणों व परियोजना की योजना के रूप में एक सूची सहित

मोचन-योग्य WP2006/5.1(CERT-D1/D2)

विषय सूची

1. प्रबंधन सारांश

यह दस्तावेज़ व्यापार प्रबंधन, प्रक्रिया प्रबंधन और तकनीकी दृष्टिकोण जैसे सभी प्रासंगिक नज़रियों से एक कंप्यूटर सुरक्षा व घटना प्रत्युत्तर दल (सी० एस० आई० आर० टी०) बनाने की प्रक्रिया के बारे में विस्तारपूर्वक बताता है । यह दस्तावेज़ एनीसा (ई० एन० आई० एस० ए०) के कार्यकारी कार्यक्रम 2006 के पाठ 5.1 में जिन दो प्रस्तुतियों का विस्तारपूर्वक वर्णन किया गया है उन्हें लागू करता है :

- यह दस्तावेज़ : *सी० ई० आर० टी० या वैसी ही अन्य सुविधाओं को स्थापित करने के चरणबद्ध तरीके के उदाहरण सहित लिखित रिपोर्ट है ।* ***(सी० ई० आर० टी० - डी० 1)***
- पाठ 12 और बाह्य फ़ाइलें : *अंकयुक्त आकार में प्रक्रिया-चित्र का अंश जिससे प्रक्रिया-चित्र को असल में लागू करने में आसानी हो ।* **(सी० ई० आर० टी० - डी० 2)**

2. कानूनी पूर्वसूचना

इस बात को याद रखना चाहिए कि अगर अन्यथा न लिखा गया हो तो यह प्रकाशन लेखकों और संपादकों के विचारों और व्याख्याओं का प्रतिनिधित्व करता है । यदि इस प्रकाशन को एनीसा विनियमन (ई० सी०) संख्या 460/2004 के अनुसार अपनाया नहीं जाता तो इसे एनीसा या एनीसा के संगंठनों की किसी कार्रवाई के रूप में नहीं देखा जाना चाहिए । यह ज़रूरी नहीं कि यह प्रकाशन कोई पत्थर की लकीर हो और समय-समय पर इसका अद्यतन किया जा सकता है ।

जहाँ उपयुक्त है वहाँ तृतीय पक्षीय स्त्रोतों के उद्धरण दिये गए हैं । इस प्रकाशन में बाह्य वेबसाइटों सहित जिन बाहरी स्त्रोतों के संदर्भ दिये गए हैं एनीसा उनकी विषय-वस्तु के लिए ज़िम्मेदार नहीं है ।

यह प्रकाशन केवल शैक्षिक व जानकारी-संबंधी उद्देश्यों के लिए है । इस प्रकाशन में मौजूद जानकारी का जो भी उपयोग किया जा सकता है उसके लिए एनीसा या इसके लिए काम करने वाला कोई व्यक्ति दोनों ही ज़िम्मेदार नहीं हैं ।

3. आभार

एनीसा उन सभी संगठनों और व्यक्तियों की आभारी है जिन्होंने इस दस्तावेज़ को बनाने में भूमिका निभाई । निम्नलिखित योगदान देने वालों को विशेष तौर पर "धन्यवाद" दिया जाता है:

- हेन्क ब्रॉन्क, जिन्होंने एक परामर्शदाता के रूप में इस दस्तावेज़ का प्रथम संस्करण बनाया ।
- सी० ई० आर० टी०/ सी० सी० और ख़ासकर सी० आई० एस० आई० आर० टी० विकास दल, जिसने परिशिष्ट में मौजूद सर्वाधिक उपयोगी सामग्री और पाठ्यक्रम सामग्री का नमूना प्रदान किये ।
- एक-बक्से-में-सी०ई०आर०टी० प्रदान करने के लिए GovCERT.NL
- ट्रान्सिट दल जिन्होंने परिशिष्ट में मौजूद पाठ्यक्रम सामग्री का नमूना बनाने में सहयोग किया ।
- तकनीकी विभाग के सुरक्षा नीति प्रभाग के सहकर्मी जिन्होंने पाठ 6.6 बनाने में सहयोग किया
- वे अगनित लोग जिन्होंने इस दस्तावेज़ का पुनरावलोकन किया ।

4. उपसंहार

संचार संगठन-तंत्र (नेटवर्क) और जानकारी तंत्र आर्थिक और सामाजिक विकास के महत्त्वपूर्ण घटक बन गए हैं । अब कंप्यूटिंग और नेटवर्किंग बिजली या जल आपूर्ती की ही तरह ज़रूरी सुविधाएं बन गईं हैं ।

अतः संचार संगठन-तंत्रों व जानकारी तंत्रों की सुरक्षा और ख़ासकर उनकी सुरक्षा समाज के लिए बढ़ती चिंता का विषय है । इसका उद्गम तंत्र में जटिलताओं, दुर्घटनाओं, गल्तियों और युरोपियन यूनियन के नागरिकों के कल्याण हेतु महत्त्वपूर्ण भौतिक अवसंरचनाओं पर आक्रमण के कारण प्रमुख जानकारी तंत्रों में समस्याओं के जोख़िम से होता है ।

10 मार्च 2004 को एक युरोपीय संगठन-तंत्र व जानकारी की सुरक्षा के क्षेत्र में काम करने वाली एजेंसी (एनीसा या ई० एन० आई० एस० ए०) की स्थापना की गई[1] । इसका उद्देश्य समुदाय के

[1] युरोपीय नेटवर्क व जानकारी सुरक्षा एजेंसी स्थापित करने वाला युरोपीय संसद और पर्सिषद के 10 मार्च 2004 के विनियम (ई०सी०) संख्या 460/2004 । एक "युरोपीय सामुदायिक एजेंसी" एक ऐसी संस्था है जिसे

अंदर नेटवर्क व जानकारी सुरक्षा का उच्च एवं कारगर स्तर सुनिश्चित करना और युरोपियन यूनियन में नागरिकों, उपभोक्ताओं, कंपनियों और सार्वजनिक क्षेत्र के संस्थानों के लिए नेटवर्क व जानकारी सुरक्षा की संस्कृति विकसित करना था जिससे आंतरिक बाज़ार के सफल कार्य में सहयोग हो ।

अब कई सालों से युरोप में सी०ई०आर०टी०/ सी०एस०आई०आर०टी०, दुरुपयोग दलों और वार्प (डब्लयू० ए० आर० पी०) जैसे कई सुरक्षा समुदाय मिल कर एक अधिक सुरक्षित इंटरनेट की दिशा में कार्य कर रहे हैं । एनीसा का उद्देश्य एक उचित स्तर की सेवा गुणवत्ता सुनिश्चित करने संबंधी उपायों के बारे में जानकारी दे इन समुदायों की कोशिशों में सहायता करना है । इसके साथ-साथ एनीसा युरोपियन यूनियन के सदस्य राष्ट्रों और युरोपियन यूनियन की संस्थाओं को आई० टी० प्रयुक्ताओं के विशिष्ट समूहों को उपयुक्त सुरक्षा सेवाओं के अंतर्गत आने संबंधी प्रश्नों के बारे में सलाह देने की अपनी क्षमता को बढ़ाने का भी इरादा रखती है । अतः 2005 में प्रतिष्ठित तदर्थ सी० ई० आर० टी० सहयोग और सहायता कार्य-समूह की खोजों के आधार पर यह नया कार्य-समूह उन प्रश्नों का सामना करेगा जो विशिष्ट (श्रेणियों या समूहों के) प्रयोक्ताओं को पर्याप्त सुरक्षा सेवाएं ("सी० ई० आर० टी० सेवाएं") प्रदान करने से संबंधित हैं ।

आपको अपने सी० एस० आई० आर० टी० स्थापित करने में मदद करने वाली "*एक अतिरिक्त सूची के साथ एक सी० एस० आई० आर० टी० स्थापित करने का एक चरणबद्ध तरीक* " अपनी इस रिपोर्ट को प्रकाशित कर एनीसा नए सी० एस० आई० आर० टी० की स्थापना का समर्थन करती है ।

युरोपियन संघ द्वारा "सामुदायिक क्षेत्र" ("पहला स्तंभ") में विशिष्ट तकनीकी, वैज्ञानिक या प्रबंधन कार्य करने के लिए स्थापित किया गया है ।

4.1. *लक्षित श्रोता*

इस रिपोर्ट के प्राथमिक लक्ष्य समूह वे सरकारी और अन्य संस्थान हैं जो अपनी या अपने भागीदारों की आई० टी० अवसंरचनाओं की सुरक्षा के लिए सी० एस० आई० आर० टी० स्थापित करने का निर्णय लेते हैं ।

4.2. *इस दस्तावेज़ का उपयोग कैसे करें*

यह दस्तावेज़ इस बारे में जानकारी प्रदान करेगा कि एक सी० एस० आई० आर० टी० क्या है, यह क्या सेवाएं प्रदान कर सकता है और शुरूआत के लिए क्या करना ज़रूरी है । इससे पाठक को सी० एस० आई० आर० टी० कैसे स्थापित करना है, इसके ढांचे और इसकी अंतर्वस्तु का अच्छा और व्यावहारिक सिंहावलोकन मिलना चाहिए ।

पाठ 4 "उपसंहार"
इस रिपोर्ट का उपसंहार

पाठ 5 "सी० एस० आई० आर० टी० की योजना बनाने और स्थापना करने हेतु समग्र रणनीति"
यह पहला खंड एक सी० एस० आई० आर० टी० क्या है इसका विवरण प्रदान करता है । सी० एस० आई० आर० टी० जिन विभिन्न वातावरणों में काम कर सकेंगे और वे कौन-सी सेवाएं प्रदान कर सकते हैं यह उनके बारे में भी जानकारी प्रदान करेगा ।

पाठ 6 "*व्यापार योजना का विकास*"
यह पाठ प्रक्रिया स्थापित करने की दिशा में व्यापार प्रबंधन प्रस्ताव के बारे में विस्तारपूर्वक बताता है ।

पाठ 7 "*व्यापार योजना को बढ़ावा देना*"
इस पाठ में व्यापारिक मामले और वित्त एकत्रित करने संबंधी मुद्दों के बारे में चर्चा की जाएगी ।

पाठ 8 "*प्रचालन संबंधी और तकनीकी कार्य-प्रणालियों के उदाहरण*"
इस पाठ में जानकारी एकत्रित करने और इसे सुरक्षा-संबंधी समाचार-पत्र में तबदील करने की प्रक्रिया के बारे में विस्तारपूर्वक बताया गया है । यह पाठ घटना पर कार्रवाई करने के कार्य-प्रवाह का विवरण भी प्रदान करता है ।

पाठ 9 "*सी० एस० आई० आर० टी० प्रशिक्षण*"
यह पाठ उपलब्ध सी० एस० आई० आर० टी० प्रशिक्षण का सारांश देता है । उदाहरण के लिए नमूना पाठ्यक्रम सामग्री परिशिष्ट में दी गई है ।

पाठ 10 "*अभ्यास : एक परामर्श विज्ञप्ति बनाना*"

इस पाठ में मूल (या मुख्य) सी० एस० आई० आर० टी० सेवाओं में से एक - सुरक्षा बुलेटिन (या परामर्श विज्ञप्ति) बनाना - कैसे करनी चाहिए के बारे में एक अभ्यास है ।

पाठ 12 "परियोजना योजना का विवरण"

यह पाठ इस मार्गदर्शिका (गाइड) के साथ प्रस्तुत अतिरिक्त परियोजना योजना (सूची) की ओर इशारा करता है । इस योजना का लक्ष्य इस मार्गदर्शिका के कार्यान्वयन हेतु एक आसानी से इस्तेमाल किया जा सकने वाला उपकरण बनना है ।

4.3. इस दस्तावेज़ में प्रयुक्त परिपाटियां

पाठक के मार्गदर्शन के लिए प्रत्येक पाठ उन चरणों के सारांश के साथ शुरू होता है जो सी० एस० आई० आर० टी० की स्थापना की प्रक्रिया में अब तक उठाए गए हैं । यह सारांश नीचे दिए गए प्रकोष्ठक जैसे प्रकोष्ठों में बताए गए हैं :

हमने पहला कदम उठाया

प्रत्येक पाठ उठाए गए कदमों के एक व्यावहारिक उदाहरण के साथ ख़त्म होगा । इस दस्तावेज़ में "काल्पनिक सी० एस० आई० आर० टी०" किसी मध्यम-आकार की कंपनी या संस्थान के लिए एक स्वतंत्र छोटा सी० एस० आई० आर० टी० होगा । परिशिष्ट में इसका सारांश देखा जा सकता है ।

काल्पनिक सी० एस० आई० आर० टी०

5. सी० एस० आई० आर० टी० की योजना बनाने और स्थापना करने हेतु समग्र रणनीति

सी० एस० आई० आर० टी० स्थापित करने की प्रक्रिया की सफल शुरूआत के लिए उन संभावित सेवाओं की स्पष्ट संकल्पना करना ज़रूरी है जो दल अपने ग्राहकों, जिन्हें "सी० एस० आई० आर० टी० की दुनिया" में 'संघटक' के नाम से जाना जाता है, को प्रदान कर सकता है । अतः संघटकों की ज़रूरतों को समझना ज़रूरी है जिससे उन्हें उपयुक्त समयावधि और गुणवत्ता के अनुसार उपयुक्त सेवाएं प्रदान की जा सकें ।

5.1. सी० एस० आई० आर० टी० क्या है ?

सी० एस० आई० आर० टी० का अर्थ है कंप्यूटर सुरक्षा घटना प्रत्युत्तर दल । सी० एस० आई० आर० टी० शब्द को अधिकतर युरोप में सुरक्षित सी० ई० आर० टी० शब्द, जो संयुक्त राज्य अमरीका में सी० ई० आर० टी० समन्वयन केंद्र (सी० ई० आर० टी०/ सी० सी०) द्वारा पंजीकृत है, के लिए इस्तेमाल किया जाता है ।
इसी प्रकार के दलों के लिए कई अलग-अलग संक्षिप्तीकरण मौजूद हैं :

- सी० ई० आर० टी० या सी० ई० आर० टी०/ सी० सी० (कंप्यूटर आपातकालीन प्रत्युत्तर दल/ समन्वयन केंद्र)
- सी० एस० आई० आर० टी० (कंप्यूटर सुरक्षा घटना प्रत्युत्तर दल)
- आई० आर० टी० (घटना प्रत्युत्तर दल)
- सी० आई० आर० टी० (कंप्यूटर घटना प्रत्युत्तर दल)
- एस० ई० आर० टी (सुरक्षा आपातकालीन प्रत्युत्तर दल)

वैश्विक आई० टी० अवसंरचना में कीट (वॉर्म) का पहला बड़ा प्रकोप 1980 के दशक के अंत में हुआ था । वॉर्म का नाम मोरिस[2] रखा गया था और यह तेज़ी से फैला और इसने दुनिया-भर में बड़ी संख्या में आई० टी० तंत्रों को कारगर ढंग से संक्रमित किया ।

इस घटना ने एक जागरण कॉल की तरह काम किया : अचानक इस तरह के मामलों का सामना करने के लिए लोग तंत्र प्रशासकों और आई० टी० प्रबंधकों के बीच सहयोग और समन्वयन की बढ़ती ज़रूरत के प्रति जागरुक हुए । चूंकि समय एक बहुत गंभीर घटक था अतः आई० टी० सुरक्षा घटनाओं का सामना करने के लिए एक अधिक सुनियोजित और संरचनात्मक प्रस्ताव स्थापित करना ज़रूरी था । अतः "मोरिस घटना" के कुछ दिन बाद रक्षा उच्च अनुसंधान

[2] मोरिस वॉर्म के बारे में अधिक जानकारी http://en.wikipedia.org/wiki/Morris_worm

परियोजना एजेन्सी (डार्पा) ने पहले सी० एस० आई० आर० टी० की स्थापना की : पिट्सबर्ग (पेन्नसिलवेनिया) में कार्नेजी मेलॅन विश्वविद्यालय में स्थित सी० ई० आर० टी० समन्वयन केंद्र (सी० ई० आर० टी०/ सी० सी०[3]) ।

यह नमूना युरोप में शीघ्र ही अपनाया गया और 1992 में डच शैक्षिक प्रदाता सर्फ़नेट ने युरोप में सर्फ़नेट-सी० ई० आर० टी०[4] नामक पहले सी० एस० आई० आर० टी० की शुरूआत की । कई टीमों ने उसका अनुसरण किया और हाल में एनीसा की *युरोप[5] में सी० ई० आर० टी० की गतिविधियों की सूची* में युरोप में स्थित 100 से ज़्यादा ज्ञात दलों के नाम हैं जो इसका अनुसरण कर रहे हैं ।

समय के साथ-साथ सी० ई० आर० टी० ने अपनी क्षमताओं को बढ़ाया और चेतावनियों, सुरक्षा बुलेटिनों, प्रशिक्षण व सुरक्षा प्रबंधन सेवाओं सहित केवल एक प्रतिक्रिया दल से एक पूर्ण सुरक्षा सेवा प्रदाता बना । जल्द ही "सी० ई० आर० टी०" शब्द अपर्याप्त माना गया । नतीजतन 1990 के दशक के अंत में एक नया शब्द "सी० एस० आई० आर० टी०" बनाया गया । इस समय दोनों शब्दों (सी० ई० आर० टी० और सी० एस० आई० आर० टी०) का उपयोग समानार्थक शब्दों के रूप में किया जाता है जबकि सी० एस० आई० आर० टी० ज़्यादा सही शब्द है ।

5.1.1. *चुनाव-क्षेत्र शब्द*

अब से (सी० एस० आई० आर० टी० समुदायों में) एक सी० एस० आई० आर० टी० के ग्राहक-आधार के लिए 'चुनाव क्षेत्र' शब्द, जो कि प्रचलित शब्द है, का उपयोग किया जाएगा । एक अकेले ग्राहक को 'संघटक' व एक समूह को 'संघटक' के नाम से जाना जाएगा ।

5.1.2. सी० एस० आई० आर० टी० की परिभाषा

सी० एस० आई० आर० टी० सूचना प्रौद्योगिकी सुरक्षा विशेषज्ञों का एक दल है जिसका मुख्य कार्य कंप्यूटर सुरक्षा घटनाओं के प्रति प्रतिक्रिया करना है । यह उनकी देखभाल करने के लिए ज़रूरी सेवाएं प्रदान करता है और उल्लंघनों से उबरने में उनके घटकों की मदद करता है ।

जोख़िमों का शमन करने और आवश्यक प्रतिक्रियाओं की संख्या को यथासंभव कम करने के लिए अधिकतर सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र के लिए निरोधक और शैक्षिक सेवाएं भी प्रदान करते हैं । वे प्रक्रिया और यंत्र सामग्री के उपयोग में असुरक्षाओं के बारे में चेतावनियां जारी करते हैं और साथ-साथ वे प्रयोक्ताओं को उन आक्रमणों व वॉयरसों के बारे में भी बताते हैं जो

[3] सी०ई०आर०टी०-सी०सी०, http://www.cert.org
[4] सर्फ़नेट-सेर्ट: http://cert.surfnet.nl/
[5] एनीसा सूची http://www.enisa.europa.eu/ENISA%20CERT/index.htm

इन त्रुटियों का फ़ायदा उठाते हैं । अतः संघटक शीघ्रता से अपने तंत्रों की मरम्मत और उनका अद्यतन कर सकते हैं । संभावित सेवाओं की पूरी सूची के लिए पाठ *5.2 संभावित सेवाएं* देखें ।

5.1.3. अपने पास सी० एस० आई० आर० टी० होने के लाभ

अगर किसी संस्थान के पास एक समर्पित आई० टी० सुरक्षा दल हो तो उससे उसे बड़ी घटनाओं का शमन करने और उनसे बचने व इस तरह अपनी बहुमूल्य परिसंपत्तियों को बचाने में मदद मिलती है ।

इसके अलावा निम्नलिखित लाभ भी हो सकते हैं :

- सूचना प्रौद्योगिकी से संबंधित सुरक्षा मुद्दों के लिए संस्थान के अंदर (संपर्क-स्थल, प्वांइट ऑफ़ कांटेक्ट या पी० ओ० सी०) केंद्रीयकृत समन्वयन होना ।
- सूचना प्रौद्योगिकी घटनाओं का केंद्रीयकृत और विशेषज्ञता-प्राप्त सामना करना और उनके प्रत्युत्तर देना ।
- सुरक्षा-संबंधी घटनाओं से शीघ्र उबरने में प्रयोक्ताओं का समर्थन और मदद करने के लिए अपने पास दक्षता होना ।
- मुकद्दमे की स्थिति में कानूनी मुद्दों का सामना करना और प्रमाण संभाल कर रखना ।
- सुरक्षा के क्षेत्र में होने वाले विकासों पर नज़र रखना ।
- चुनाव-क्षेत्र कें अंदर आई० टी० सुरक्षा (जानकारी निर्माण) के लिए सहयोग को बढ़ावा देना ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 0)
सी० एस० आई० आर० टी० क्या है, यह समझना : नमूने के तौर पर प्रस्तुत सी० एस० आई० आर० टी० को कम से कम 200 कर्मचारियों वाले मध्यम-आकार के संस्थान की सेवा करनी होगी । संस्थान का अपना अलग सूचना प्रौद्योगिकी विभाग है और उसी देश में दो अन्य शाखाएं हैं । कंपनी में सूचना प्रौद्योगिकी एक प्रमुख भूमिका निभाती है क्योंकि इसका उपयोग आंतरिक संचार, आंकड़ा संगठन-तंत्र और 24x7 ई-व्यापार के लिए किया जाता है । संस्थान का अपना अलग संगठन-तंत्र (नेटवर्क) है और इसके पास दो अलग-अलग इंटरनेट सेवा प्रदाताओं के माध्यम से इंटरनेट के साथ एक अतिरिक्त संयोजन (कॅनैक्शन) है ।

5.1.4. विभिन्न प्रकार के सी० एस० आई० आर० टी० वातावरणों का विवरण

हमने पहला कदम उठाया

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।

>> अगला कदम है इस प्रश्न का उत्तर देना : "सी० एस० आई० आर० टी० की सेवायें किस क्षेत्र को दी जाएंगी ?"

सी० एस० आई० आर० टी० (किसी भी अन्य व्यापर की तरह) शुरू करते समय इस बात का स्पष्ट होना अत्यावश्यक है कि चुनाव-क्षेत्र कौन-से हैं और सी० एस० आई० आर० टी० सेवायें किस प्रकार के वातावरण के लिए विकसित की जाएंगी । इस समय हम निम्नलिखित 'क्षेत्रों' को पहचानते हैं, वर्णानुक्रमानुसार सूचीबद्ध :

- शैक्षिक क्षेत्र का सी० एस० आई० आर० टी०
- व्यापारिक सी० एस० आई० आर० टी०
- सी० आई० पी० / सी० आई० आई० पी० क्षेत्र का सी० एस० आई० आर० टी०
- सरकारी क्षेत्र का सी० एस० आई० आर० टी०
- आंतरिक सी० एस० आई० आर० टी०
- सैन्य क्षेत्र सी० एस० आई० आर० टी०
- राष्ट्रीय सी० एस० आई० आर० टी०
- लघु व मध्यम आकार की औद्योगिक इकाइयां (एस० एम० ई०) क्षेत्र का सी० एस० आई० आर० टी०
- विक्रेता सी० एस० आई० आर० टी०

शैक्षिक क्षेत्र का सी० एस० आई० आर० टी०

ध्यान का केंद्र

शैक्षिक क्षेत्र का सी० एस० आई० आर० टी० शैक्षिक व शिक्षा संस्थानों, जैसे विश्वविद्यालय या अनुसंधान सुविधाएं, और उनके परिसर इंटरनेट वातावरणों को सी० एस० आई० आर० टी० सेवायें प्रदान करता है ।

संघटक

कर्मचारी और विश्वविद्यालयों के विद्यार्थी इस प्रकार के सी० एस० आई० आर० टी० के विशिष्ट संघटक हैं ।

व्यापारिक सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक व्यापारिक सी० एस० आई० आर० टी० अपने संघटकों को व्यापारिक तौर पर सी० एस० आई० आर० टी० सेवायें प्रदान करता है । एक इंटरनेट सेवा प्रदाता के लिए सी० एस० आई० आर० टी० अधिकतर अंतिम-प्रयोक्ता ग्राहकों (डॉयल-इन, ए० डी० एस० एल०) को दुरुपयोग सेवाएं और अपने व्यावसायिक ग्राहकों को सी० एस० आई० आर० टी० सेवायें प्रदान करता है ।

संघटक

आमतौर पर व्यापारिक सी० एस० आई० आर० टी० अपनी सेवायें उन संघटकों को प्रदान करते हैं जो उन्हें पैसा देते हैं ।

सी० आई० पी० / सी० आई० आई० पी० क्षेत्र सी० एस० आई० आर० टी०

ध्यान का केंद्र

इस क्षेत्र के सी० एस० आई० आर० टी० अपना ध्यान मुख्यतः बहुत गंभीर जानकारी की सुरक्षा और/ या बहुत गंभीर जानकारी और अवसंरचना की सुरक्षा पर केंद्रित करते हैं । अधिकतर मामलों में यह विशेषज्ञताप्राप्त सी० एस० आई० आर० टी० सरकारी सी० आई० पी० विभाग के साथ निकट सहयोग करता है । यह देश के सभी बहुत गंभीर सूचना प्रौद्योगिकी क्षेत्रों में काम करता है और उस देश के नागरिकों की सुरक्षा करता है ।

संघटक

सरकार; अत्यधिक महत्त्वपूर्ण सूचना प्रौद्योगिकी व्यापार; नागरिक

सरकारी क्षेत्र सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक सरकारी सी० एस० आई० आर० टी० सरकारी एजेंसियों को और कुछ देशों में नागरिकों को सेवायें प्रदान करता है ।

संघटक

सरकार और संबंधित सरकारी एजेंसियां; कुछ देशों में नागरिकों को चेतावनी देने की सेवायें भी प्रदान की जातीं हैं (उदाहरण के लिए, बेल्जियम, हंगरी, हॉलैंड, ब्रिटेन या जर्मनी) ।

आंतरिक सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक आंतरिक सी० एस० आई० आर० टी० केवल अपने मेज़बान संस्थान को सेवायें प्रदान करता है । यह क्षेत्र की बजाय कार्य को ज़्यादा विस्तारपूर्वक बताता है । उदाहरण के लिये कई दूरसंचार प्रणाली संस्थान और बैंक अपनी खुद की आंतरिक सी० एस० आई० आर० टी० चलाते हैं । आमतौर पर उनके पास जनता के लिए वेबसाइट नहीं होती ।

संघटक

मेज़बान संस्थान के आंतरिक कर्मचारी व उसका सूचना प्रौद्योगिकी विभाग

सैन्य क्षेत्र सी० एस० आई० आर० टी०

ध्यान का केंद्र

इस क्षेत्र में सी० एस० आई० आर० टी० उन सैन्य संगठनों को सेवायें प्रदान करता है जिन पर उस सूचना प्रौद्योगिकी अवसंरचना की ज़िम्मेदारियां होतीं हैं सैन्य उद्देश्यों के लिए जिसकी ज़रूरत होती है ।

संघटक

सैन्य संस्थानों के कर्मचारी या बहुत निकटवर्ती इकाइयां जैसे रक्षा विभाग

राष्ट्रीय सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक ऐसी सी० एस० आई० आर० टी० जिसका ध्यान राष्ट्र पर केंद्रित है और जिसे किसी देश के लिए सुरक्षा संपर्क-स्थल माना जाता है । कुछ मामलों में सरकारी सी० एस० आई० आर० टी० राष्ट्रीय संपर्क-स्थलों के रूप में भी काम करते हैं (जैसे इंग्लैंड में युनीरास) ।

संघटक

आमतौर पर इस प्रकार के सी० एस० आई० आर० टी० के सीधे संघटक नहीं होते क्योंकि राष्ट्रीय सी० एस० आई० आर० टी० पूरे देश के लिए केवल एक मध्यस्थ की भूमिका निभाता है ।

लघु व मध्यम आकार की औद्योगिक इकाइयां (एस० एम० ई०) क्षेत्र सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक स्व-संगठित सी० एस० आई० आर० टी० जो अपनी खुद के व्यापार की शाखाओं या उसी तरह के अन्य प्रयोक्ता समूह को सेवायें प्रदान करता है ।

संघटक

लघु व मध्यम आकार की औद्योगिक इकाइयां और उनके कर्मचारी या फिर विशेष रुचि वाले समूह जैसे किसी देश की "शहरों और नगरपालिकाओं की संस्था" इन सी० एस० आई० आर० टी०ओं के संघटक हो सकते हैं ।

विक्रेता सी० एस० आई० आर० टी०

ध्यान का केंद्र

एक विक्रेता सी० एस० आई० आर० टी० अपना ध्यान विक्रेता-विशिष्ट उत्पादों के समर्थन करने पर केंद्रित करता है । आमतौर पर इसका उद्देश्य असुरक्षाओं को हटाने और त्रुटियों के संभावित नकारात्मक प्रभावों का शमन करने के लिए समाधान विकसित व प्रदान करना होता है ।

संघटक

उत्पाद के मालिक

जैसा कि राष्ट्रीय सी० एस० आई० आर० टी० के बारे में अनुच्छेद में बताया गया है एक दल एक से अधिक क्षेत्र में काम कर सकता है । इसका चुनाव-क्षेत्र और उसकी ज़रूरतों के विश्लेषण जैसी बातों पर प्रभाव पड़ता है ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 1)
शुरुआती चरण शुरुआती चरण में नये सी० एस० आई० आर० टी० की योजना एक ऐसे आंतरिक सी० एस० आई० आर० टी० के तौर पर बनाई जाती है जो मेज़बान कंपनी, स्थानीय सूचना प्रौद्योगिकी विभाग और कर्मचारियों को अपनी सेवाएं प्रदान करता है । यह दफ़्तर की विभिन्न शाखाओं के बीच सूचना प्रौद्योगिकी सुरक्षा संबंधी घटनाओं पर कार्रवाई का समर्थन व समन्वयन भी करता है ।

5.2. वे संभावित सेवाएं जो एक सी० एस० आई० आर० टी० प्रदान कर सकता है

हमने पहले दो कदम उठाए हैं

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?

>> अब अगला कदम इस प्रश्न का उत्तर देना है कि *घटकों को कौन-सी सेवायें प्रदान की जानी चाहिए* ।

एक सी० एस० आई० आर० टी० कई सेवायें प्रदान कर सकता है परंतु अब तक कोई भी मौजूदा सी० एस० आई० आर० टी० वे सब सेवायें प्रदान नहीं कर रहा । अतः उपयुक्त सेवाओं के समूह का चुनाव करना एक महत्त्वपूर्ण निर्णय है ।

जैसा कि सी० ई० आर० टी० /सी० सी० द्वारा प्रकाशित "सी० एस० आई० आर० टी० के लिए निर्देश-पुस्तिका" में परिभाषित किया गया है, नीचे आप सभी ज्ञात सी० एस० आई० आर० टी० सेवाओं का सिंहावलोकन देखेंगे ।[6]

[6] सी०ई०आर०टी०/सी०सी० सी०एस०आई०आर०टी० पुस्तिका http://www.cert.org/archive/pdf/csirt-handbook.pdf

प्रतिक्रियात्मक सेवायें	**सक्रिय सेवायें**	**शिल्पकृति पर कार्रवाई**
• **सतर्कादेश और चेतावनियां** • **घटना पर कार्रवाई करना** • **घटना का विश्लेषण** • **घटना प्रत्युत्तर सहायता** • **घटना प्रत्युत्तर समन्वयन** • घटना-स्थल पर घटना-प्रत्युत्तर • सुभेद्यता पर कार्रवाई • सुभेद्यता विश्लेषण • सुभेद्यता प्रत्युत्तर • सुभेद्यता प्रत्युत्तर समन्वयन	• **घोषणाएं** • तकनीक पर नज़र रखना • सुरक्षा लेखा-परीक्षा या मूल्यांकन • सुरक्षा का विन्यास व देखभाल • सुरक्षा उपकरणों का विकास • घुसपैठ का पता लगाने की सेवायें • सुरक्षा-संबंधी जानकारी का वितरण	• *शिल्पकृति विश्लेषण* • *शिल्पकृति प्रत्युत्तर* • *शिल्पकृति प्रत्युत्तर समन्वयन* ***सुरक्षा गुणवत्ता प्रबंधन*** • *जोखिम विश्लेषण* • *व्यापार निरंतरता और विपदा से उबरना* • *सुरक्षा परामर्श* • *ज्ञान-वर्धन* • *शिक्षा/ प्रशिक्षण* • *उत्पाद का मूल्यांकन या प्रमाणीकरण*

चित्र 1. सी० ई० आर० टी०/ सी० सी० से सी० एस० आई० आर० टी० सेवाओं की सूची[7]

महत्त्वपूर्ण सेवायें (गहरे अक्षरों में अंकित) : प्रतिक्रियात्मक और सक्रिय सेवाओं के बीच अंतर किया जाता है । सक्रिय सेवाओं का उद्देश्य जानकारी फैला कर और प्रशिक्षण द्वारा घटनाओं को होने से रोकना है जबकि प्रतिक्रियात्मक सेवाओं का लक्ष्य घटनाओं पर कार्रवाई करना और उनसे होने वाली हानि का शमन करना है ।

शिल्पकृति पर कार्रवाई में तंत्र में पाई गई किसी भी ऐसी फ़ाइल या वस्तु, जैसे वॉयरस, वॉर्म्स, स्क्रिप्ट्स, ट्रोजन, इत्यादि, का विश्लेषण शामिल है जो दुर्भावनाशील कार्यों में लिप्त हो सकती है । इसमें मालवेयॅर को आगे फैलने से रोकने और जोख़िम का शमन करने के लिए कार्रवाई करना और इससे उत्पन्न होने वाली जानकारी का विक्रेताओं व अन्य पक्षों, जिनकी इसमें रुचि हो, वितरण करना भी शामिल है ।

सुरक्षा व गुणवत्ता सेवायें वे सेवायें हैं जिनके दीर्घकालीन लक्ष्य होते हैं और इनमें परामर्श देना और शैक्षिक उपाय शामिल हैं ।

सी० एस० आई० आर० टी० सेवाओं के विस्तृत स्पष्टीकरण के लिए परिशिष्ट देखें ।

7 सी०ई०आर०टी०/सी०सी० से सी०एस०आई०आर०टी० सेवाओं की सूची : http://www.cert.org/csirts/services.html

अपने घटकों के लिए सही सेवाओं का चुनाव करना एक महत्त्वपूर्ण चरण है और इसके बारे में पाठ *6.1 वित्तीय नमूने को परिभाषित करना* में आगे चर्चा की जाएगी ।

अधिकतर सी० एस० आई० आर० टी० अपने घटकों के लिए 'संकेत और चेतावनियां' बांट कर, 'घोषणाएं' कर और 'घटनाओं पर कार्रवाई' प्रदान कर शुरुआत करते हैं । आमतौर पर यह महत्त्वपूर्ण सेवायें घटकों के साथ एक अच्छी छवि और ध्यान मूल्य प्रदान करतीं हैं और इन्हें मुख्यतः असली 'मूल्य वर्धन' माना जाता है ।

'प्रायोगिक'-घटकों के एक छोटे समूह से शुरुआत करना, एक शुरुआती समयावधि के दौरान महत्त्वपूर्ण सेवाएं प्रदान करना और बाद में प्रतिपुष्टि का निवेदन करना एक अच्छा अभ्यास है । जिन प्रायोगिक प्रयोक्ताओं की इसमें रुचि है वे आमतौर पर रचनात्मक प्रतिपुष्टि देते हैं और पूर्णतयाः उपयुक्त सेवायें विकसित करने में मदद करते हैं ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 2)

सही सेवायें चुनना

शुरुआती चरण में यह निर्णय लिया जाता है कि नया सी० एस० आई० आर० टी० मुख्यतः कर्मचारियों को कुछ महत्त्वपूर्ण सेवाएं देने पर अपना ध्यान केंद्रित करेगा ।

यह निर्णय लिया जाता है कि प्रायोगिक-चरण के बाद सेवा पोर्टफ़ोलियो के विस्तार पर विचार किया जा सकता है और कुछ 'सुरक्षा प्रबंधन सेवायें' जोड़ी जा सकतीं हैं । यह निर्णय प्रायोगिक-संघटकों से प्राप्त प्रतिपुष्टि के आधार पर और गुणवत्ता आश्वासन विभाग के साथ निकट सहयोग द्वारा लिया जाएगा ।

5.3. चुनाव-क्षेत्र और उद्देश्य कथन का विश्लेषण

हमने पहले तीन कदम उठाए हैं :

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।

>> अगला चरण इस प्रश्न का उत्तर देना है कि *सी० एस० आई० आर० टी० को शुरु करने के लिए किस तरह का नज़रिया चुनना चाहिये ?*

अगले चरण सही संचार माध्यमों को चुनने के उद्देश्य से चुनाव-क्षेत्र पर एक अधिक गहन दृष्टि डालना है :

- घटकों को संचार प्रस्ताव की परिभाषा बताना है
- उद्देश्य कथन परिभाषित करना
- यथार्थवादी कार्यान्वयन/ परियोजना योजना बनाना
- सी० एस० आई० आर० टी० सेवायें परिभाषित करना
- संस्थानात्मक ढांचा परिभाषित करना
- जानकारी सुरक्षा नीति परिभाषित करना
- उचित कर्मचारियों को नौकरी पर रखना
- अपने सी० एस० आई० आर० टी० दफ़्तर का उपयोग करना
- अन्य सी० एस० आई० आर० टी०ओं के बीच सहयोग और संभावित राष्ट्रीय पहलों को खोजना

निम्नलिखित अनुच्छेदों में इन चरणों पर अधिक विस्तारपूर्वक चर्चा की जाएगी और व्यापार व परियोजना योजना में आगत के रूप में इनका उपयोग किया जा सकता है ।

5.3.1. चुनाव-क्षेत्र की ओर संचार प्रस्ताव

जैसा कि पहले कहा गया है चुनाव-क्षेत्र की ज़रूरतों और उन तक जानकारी पहुँचाने के लिए सर्वाधिक उपयुक्त संचार माध्यमों सहित अपनी संचार-रणनीति को जानना बहुत ज़रूरी है ।

प्रबंधन सिद्धांत को लक्षित समूह का विश्लेषण करने संबंधी इस समस्या के कई संभव प्रस्तावों के बारे में पता है । इस दस्तावेज़ में हम उन में से दो का विस्तारपूर्वक वर्णन करेंगे : स्वॉट (एस० डब्लयू० ओ० टी०) - और पेस्ट (पी० ई० एस० टी०) विश्लेषण ।

स्वॉट विश्लेषण

स्वॉट विश्लेषण रणनीति की योजना बनाने का एक ऐसा उपकरण है जिसका उपयोग किसी परियोजना या व्यापार या किसी अन्य ऐसी परिस्थिति जिसमें निर्णय लेने की ज़रूरत हो से संबंधित **क्ष**मताओं (एस०), **क**मज़ोरियों (डब्लयू), **मौ**कों (ओ०) और **ख**तरों (टी०) का मूल्यांकन करने के लिए किया जाता है । इस तकनीक का श्रेय अल्बर्ट हम्फ्री को जाता है जिसने फ़ॉर्च्यून 500 कंपनियों के आंकड़ों का उपयोग कर 1960 और 70 के दशक में स्टैनफ़ॉर्ड विश्वविद्यालय की अनुसंधान परियोजना का नेतृत्व किया था ।[8]

क्षमता	**कमज़ोरी**
मौके	**खतरे**

चित्र **2.** स्वॉट विश्लेषण

[8] विकिपीडिया पर स्वॉट विश्लेषण : http://en.wikipedia.org/wiki/SWOT_analysis

पेस्ट विश्लेषण

पेस्ट विश्लेषण एक और महत्त्वपूर्ण और बड़े स्तर पर उपयोग में लाया जाने वाला उपकरण है जिससे एक सी० एस० आई० आर० टी० जिस वातावरण में काम कर रही है उसकी राजनीतिक, आर्थिक, सामाजिक-सांस्कृतिक तकनीकी परिस्थितियों को समझने के लिए चुनाव-क्षेत्र का विश्लेषण किया जाता है । इससे यह पता लगाने में मदद मिलेगी कि क्या योजना अब भी वातावरण से मेल खाती है और शायद इससे गलत मान्यताओं के आधार पर किये गए कार्यों से बचने में मदद मिलती है ।

राजनीतिक	**आर्थिक**
• पर्यावरण/ वातावरण संबंधी मुद्दे • वर्तमान कानून गृह बाज़ार • भविष्य के कानून • युरोपीय/ अंतर्राष्ट्रीय कानून • विनियामक संस्थान और प्रक्रियाएं • सरकारी नीतियां • सरकारी अवधि और बदलाव • व्यापारिक नीतियां • वित्त सुलभ कराना, अनुदान और पहलें • गृह बाज़ार में मत का समर्थन करने के लिए प्रभाव डालना/ दबाव डालने वाले समूह • दबाव डालने वाले अंतर्राष्ट्रीय समूह	• गृह अर्थव्यवस्था की स्थिति • गृह अर्थव्यवस्था के रुझान • विदेशी अर्थव्यवस्थाएं और रुझान • कर संबंधी सामान्य मुद्दे • उत्पाद/ सेवाओं संबंधी विशिष्ट कर • मौसम पर निर्भरता/ मौसम संबंधी मुद्दे • बाज़ार और व्यापार चक्र • विशिष्ट औद्योगिक घटक • व्यापार मार्ग और वितरण संबंधी रुझान • ग्राहक/ अंतिम प्रयोक्ता चालक • ब्याज और विनिमय दरें
सामाजिक	**तकनीकी**
• जीवनशैली संबंधी रुझान • जनसंख्या संबंधी आंकड़ों का अध्ययन • उपभोक्ता मनोवृतियां और मत • मीडिया के नज़रिये • सामाजिक घटकों को प्रभावित करने वाले कानूनी बदलाव • ब्रांड, कंपनी, प्रौद्योगिकी छवि • ग्राहकों के खरीदारी की शैलियां • फ़ैशन और आदर्श • महत्त्वपूर्ण घटनाएं और प्रभाव • खरीद तक पहुँच और रुझान • प्रजातीय/ धार्मिक घटक	• प्रतिस्पर्धी प्रौद्योगिकी विकास • अनुसंधान हेतु वित्त सुलभ कराना • संबंधित/ निर्भर तकनीकें • प्रतिस्थापन तकनीक/ समाधान • प्रौद्योगिकी की परिपक्वता • उत्पादन परिपक्वता और क्षमता • जानकारी और संचार • उपभोक्ताओं की खरीद की क्रिया-प्रणालियां / प्रौद्योगिकी • प्रौद्योगिकी संबंधी कानून • नवप्रवर्तन की क्षमता • तकनीक तक पहुँच, लाइसैंस प्रदान

• विज्ञापन और प्रचार	करना, पेटेंट • बौद्धिक सम्पत्ति संबंधी मुद्दे

चित्र 3. *पेस्ट विश्लेषण का नमूना*

पेस्ट विश्लेषण का विस्तृत विवरण विकीपीडिया[9] पर देखा जा सकता है ।

दोनों उपकरण संघटकों की ज़रूरत का एक व्यापक और निश्चित ढांचे वाला सिंहावलोकन प्रस्तुत करते हैं । नतीजे व्यापारिक प्रस्ताव को पूर्ण करेंगे और इससे सी० एस० आई० आर० टी० स्थापित करने के लिए वित्त सुलभ कराने में मदद मिलेगी ।

संचार के मार्ग

विश्लेषण में एक महत्त्वपूर्ण विषय जोड़ा जाना चाहिए और वह है संचार और जानकारी वितरण के संभावित तरीके ("चुनाव-क्षेत्र से विचारों का आदान-प्रदान कैसे किया जाए?")

अगर हो सके तो संघटकों से नियमित व्यक्तिगत भेंट पर विचार करना चाहिए । यह एक जाना-माना तथ्य है कि आमने-सामने की बैठकों से सहयोग आसान होता है । अगर दोनों पक्ष इन बैठकों में मिल कर काम करने को तैयार हों तो इससे परस्पर रिश्तों में अधिक खुलापन आएगा ।

आमतौर पर सी० एस० आई० आर० टी० संचार माध्यमों के एक समूह का प्रचालन करते हैं । निम्नलिखित असल में उपयोगी साबित हुए और इन पर विचार किया जा सकता है :

- सार्वजनिक वेबसाइट
- वेबसाइट पर बंद सदस्य क्षेत्र
- घटनाओं की जानकारी देने के लिए वेब-प्रपत्र
- ई-मेल भेजने हेतु सूचियां
- व्यक्ति को ध्यान में रखते हुए भेजी गईं ई-मेल
- फोन / फ़ैक्स
- एस० एम० एस०
- 'पुराने ढर्रे के' कागज़ पर लिखे गए पत्र
- मासिक या वार्षिक रिपोर्टें

[9] विकिपीडिया में पेस्ट विश्लेषण : http://en.wikipedia.org/wiki/PEST_analysis

घटनाओं पर कार्रवाई करने (चुनाव-क्षेत्र से घटना की रिपोर्टें प्राप्त करने के लिए, अन्य दलों के साथ समन्वय करने के लिए या फिर शिकार को प्रतिपुष्टि या सहायता देने के लिए) को आसान बनाने के लिए ई-मेल, वेब-प्रपत्र, फ़ोन या फ़ैक्स के अलावा अधिकतर सी० एस० आई० आर० टी० अपनी सुरक्षा-संबंधी चेतावनियां सार्वजनिक तौर पर उपलब्ध वेबसाइट और मेलिंग लिस्ट द्वारा भी भेजते हैं ।

! अगर हो सके तो जानकारी सुरक्षित ढंग से वितरित की जानी चाहिए । उदाहरण के लिए ई-मेल पर पी० जी० पी० द्वारा अंकीय (डिजिटल) हस्ताक्षर किये जा सकते हैं और घटना संबंधी संवेदनशील आंकड़े हमेशा कूट-संकेतबद्ध (एन्क्रिप्ट) कर भेजे जाने चाहिए ।

अधिक जानकारी के लिए पाठ *8.5 उपलब्ध सी० एस० आई० आर० टी० उपकरण* देखें । साथ-ही *RFC2350*[10] का पाठ *2.3* भी देखें ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 3क)

चुनाव-क्षेत्र और उपयुक्त संचार माध्यमों का विश्लेषण करना

प्रबंधन और चुनाव-क्षेत्र के कुछ प्रमुख व्यक्तियों के साथ एक विचार-विमर्श सत्र से स्वॉट विश्लेषण के लिए पर्याप्त आगत उत्पन्न हुई । इससे इस निष्कर्श पर पहुँचे कि महत्त्वपूर्ण सेवाओं की ज़रूरत है :

- सतर्कादेश और चेतावनियां
- घटना पर कार्रवाई करना (विश्लेषण, प्रत्युत्तर सहायता और प्रत्युत्तर समन्वयन)
- घोषणाएं

यह सुनिश्चित किया जाना चाहिए कि जानकारी सही तरह से संगठित ढंग से वितरित की जाती है जिससे यह चुनाव-क्षेत्र के जितने बड़े भाग तक पहुँच सके पहुँचे । इस लिए निर्णय लिया जाता है कि सतर्कादेश, चेतावनियां और घोषणाएं सुरक्षा प्रस्तावों के रूप में इस कार्य हेतु ख़ासतौर पर बनाई गई एक वेबसाइट पर प्रकाशित की जाएंगी और मेलिंग सूची द्वारा वितरित की जाएंगी । सी० एस० आई० आर० टी० घटना की रिपोर्टें ई-मेल, फोन और फ़ैक्स द्वारा प्राप्त करने को आसान बनाता है । अगले चरण के लिए एक एकीकृत वेब-प्रपत्र बनाने की योजना है ।

नमूने के तौर पर किए गए स्वॉट विश्लेषण को देखने के लिए अगला पृष्ठ देखें ।

[10] http://www.ietf.org/rfc/rfc2350.txt

क्षमता • कंपनी में कुछ ज्ञान है । • उन्हें योजना पसंद है और वे सहयोग करने के लिए तैयार हैं । • प्रबंधन परिषद् द्वारा सहायता और वित्त सुलभ कराना ।	**कमज़ोरी** • विभिन्न विभागों और शाखाओं में विचारों का कुछ ख़ास आदान-प्रदान नहीं है । • सूचना प्रौद्योगिकी घटनाओं से कोई समन्वयन नहीं • बहुत से 'छोटे-छोटे विभाग'
मौके • ढांचा-रहित संवेदनशीलता जानकारी की बाढ़ • समन्वयन की बहुत अधिक आवश्यकता • घटनाओं के कारण होने वाले नुक़्सानों को कम करना • सूचना प्रौद्योगिकी सुरक्षा संबंधी मामलों में कई खुले छोर • कर्मचारियों को सूचना प्रौद्योगिकी सुरक्षा के बारे में शिक्षित करना	**खतरे** • कुछ ख़ास धन उपलब्ध नहीं • कर्मचारियों की कम संख्या • उच्च अपेक्षाएं • संस्कृति

चित्र 4. *स्वॉट विश्लेषण का नमूना*

5.3.2. उद्देश्य कथन

सी० एस० आई० आर० टी० सेवाओं के बारे में चुनाव-क्षेत्र की ज़रूरतों और इच्छाओं का विश्लेषण करने के बाद अगला चरण एक उद्देश्य कथन लिखना होना चाहिए ।

एक उद्देश्य कथन संस्थान द्वारा अपने संघटकों को प्रदान किए जाने वाले उत्पादों और सेवाओं को ध्यान में रखते हुए समाज में संस्थान का मूल कार्य विस्तारपूर्वक बताता है । यह नई सी० एस० आई० आर० टी० के अस्तित्व और कार्य को स्पष्ट तौर पर बताने में मदद करता है ।

उद्देश्य कथन को बहुत ज़्यादा बंधा हुआ बनाए बिना संक्षिप्त बनाना एक अच्छा अभ्यास है क्योंकि आमतौर पर कुछ सालों तक इसमें कोई बदलाव नहीं आएगा ।

चालू सी० एस० आई० आर० टी०ओं के उद्देश्य कथनों में से कुछ उदाहरण नीचे दिए गए हैं :

"<सी० एस० आई० आर० टी० का नाम> कंप्यूटर सुरक्षा घटनाओं का जोखिम कम करने और जब इस तरह की घटनाएं हों तो उनका प्रत्युत्तर देने के सक्रिय उपाय लागू करने के लिए अपने <घटकों (अपने घटकों को परिभाषित करें)> को जानकारी और मदद प्रदान करती है ।"

"सूचना प्रौद्योगिकी संबंधी सुरक्षा घटनाओं को होने से रोकने और उनका प्रत्युत्तर देने के लिए <संघटकों> को सहायता प्रदान करना"[11]

शुरूआत के लिए उद्देश्य कथन एक बहुत ही महत्त्वपूर्ण और ज़रूरी चरण है । एक सी० एस० आई० आर० टी० को क्या जानकारी प्रकाशित करनी चाहिए इसके विस्तृत विवरण के लिए कृपया *RFC2350*[12] का पाठ *2.1* देखें ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 3ख)
काल्पनिक सी० एस० आई० आर० टी० के प्रबंधन ने निम्नलिखित उद्देश्य कथन बनाया है : *"काल्पनिक* सी० एस० आई० आर० टी० *कंप्यूटर सुरक्षा घटनाओं के जोखिम को कम करने और साथ-साथ जब इस तरह की घटनाएं हों तो उनका प्रत्युत्तर देने के लिए अपनी मेज़बान कंपनी के कर्मचारियों को जानकारी और मदद प्रदान करता है ।"* इसके द्वारा काल्पनिक सी० एस० आई० आर० टी० यह स्पष्ट करता है कि यह एक आंतरिक सी० एस० आई० आर० टी० है और इसका प्रमुख कार्य सूचना प्रौद्योगिकी की सुरक्षा से संबंधित मुद्दों का सामना करना है ।

[11] Govcert.nl का उद्देश्य कथन : http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6. व्यापार योजना का विकास करना

हमने निम्नलिखित कदम उठायें हैं :

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।
4. वातावरण और घटकों का विश्लेषण
5. उद्देश्य कथन परिभाषित करना

>> अगला चरण व्यापार योजना परिभाषित करना है

विश्लेषण का नतीजा आपको चुनाव-क्षेत्र की ज़रूरतों और (मानी हुई) कमज़ोरियों का एक अच्छा सिंहावलोकन प्रदान करता है इसलिए इसे अगले चरण की आगत के तौर पर लिया जाता है ।

6.1. वित्तीय नमूना परिभाषित करना

विश्लेषण के बाद शुरूआत के लिए कुछेक मूल सेवाओं को चुना गया । अब अगला चरण वित्तीय नमूने के बारे में सोचना है : सेवा प्रदान करने के कौन-से प्राचल उपयुक्त और देय दोनों ही हैं ।

एक उत्कृष्ट विश्व में चुनाव-क्षेत्र की ज़रूरतों के अनुसार वित्त उपलब्ध कराया जाएगा परंतु असल में जो सेवायें प्रदान की जा सकती हैं उनका पोर्टफ़ोलियो एक आवंटित बजट के अनुरूप बनना चाहिए । इसलिए वित्तीय मुद्दों की योजना बना कर शुरूआत करना अधिक यथार्थवादी होगा ।

6.1.1. लागत का नमूना

लागत को प्रभावित करने वाले दो मुख्य घटक हैं सेवा घंटे निश्चित करना और काम पर लगाए जाने वाले कर्मचारियों की संख्या (और गुणवत्ता) । क्या 24x7 घटना प्रत्युत्तर और तकनीकी सहायता प्रदान करने की ज़रूरत है या फिर यह सेवाएं केवल काम के समय प्रदान की जाएंगी ?

अपेक्षित उपलब्धता और दफ़्तर के उपकरणों के आधार पर (उदाहरण के लिए क्या घर से काम करना संभव है ?) एक ऑन-कॉल ड्यूटी रोस्टर या फिर योजनाबद्ध ड्यूटी रोस्टर के साथ काम करना लाभदायक हो सकता है ।

एक शोचनीय दृश्यलेख यह हो सकता है कि सक्रिय और प्रतिक्रियात्मक सेवायें दोनों ही दफ़्तर के समय के दौरान प्रदान करना । दफ़्तर के समय के अलावा कॉल-ड्यूटी पर मौजूद एक कर्मचारी द्वारा केवल सीमित सेवायें ही प्रदान की जाएंगी, उदाहरण के लिए केवल गंभीर विपदाओं और घटनाओं के होने पर ।

अन्य सी० एस० आई० आर० टी० दलों के साथ अंतर्राष्ट्रीय सहयोग खोजना भी एक और विकल्प हो सकता है । "सूर्य के अनुसार" सहयोग कार्य के उदाहरण पहले ही मौजूद हैं । उदाहरण के लिये युरोपीय और अमरीकी दलों के बीच सहयोग लाभदायक सिद्ध हुआ है और यह एक-दूसरे की क्षमताओं का लाभ उठाने का अच्छा तरीका प्रदान करता है । उदाहरण के लिए सॅन माइक्रोसिस्टम सी० एस० आई० आर० टी०, जिनकी दुनिया के अलग-अलग समय-क्षेत्रों में कई शाखाएं हैं (परंतु सभी एक ही सी० एस० आई० आर० टी० दल के सदस्य हैं) दुनिया-भर में दलों द्वारा पारी पर लगातार काम कर 24x7 सेवाएं प्रदान करता है । इससे लागत सीमित होती है क्योंकि दल हमेशा केवल सामान्य कार्य-समय के दौरान ही काम करते हैं और दुनिया के "सोए हुए भाग" को भी सेवाएं प्रदान करते हैं ।

चुनाव-क्षेत्र के साथ 24x7 सेवाओं की ज़रूरत का विशेषतौर पर गहन विश्लेषण करना एक अच्छा अभ्यास है । रात के समय दिए गए सतर्कादेशों और चेतावनियों की कोई ख़ास तुक नहीं बनती जबकि आदाता उन्हें केवल अगले दिन सुबह ही पढ़ेगा । "एक सेवा की ज़रूरत" और "एक सेवा की चाह" में बहुत ही कम फ़र्क है परंतु कार्य-समय से कर्मचारियों की संख्या और ज़रूरी सुविधाएं बहुत प्रभावित होती हैं और इनका लागत-नमूने पर बड़ा प्रभाव पड़ता है ।

6.1.2. आय का नमूना

जब लागत पता हो तो आय के संभावित नमूनों के बारे में सोचना एक अच्छा अगला कदम हो सकता है : जिन सेवाओं की योजना बनाई गई है उन्हें चलाने के लिए वित्त कहाँ से आएगा ? मूल्यांकन हेतु कुछ संभावनाएं निम्नलिखित हैं :

मौजूदा संसाधनों का उपयोग

कंपनी के अन्य भागों में पहले से मौजूद संसाधनों का मूल्यांकन करना हमेशा लाभप्रद होता है । क्या ऐसे उपयुक्त कर्मचारी पहले से ही काम कर रहे हैं (उदाहरण के लिए पहले से मौजूद सूचना प्रौद्योगिकी विभाग में) जिनके पास ज़रूरी पृष्ठभूमि और दक्षता है ? शायद प्रबंधन के साथ चर्चा कर शुरूआत के चरण में इन कर्मचारियों को सी० एस० आई० आर० टी० में भेजने के लिए व्यवस्था की जा सकती है या फिर वे तदर्थ आधार पर सी० एस० आई० आर० टी० को सहायता प्रदान कर सकते हैं ।

सदस्यता शुल्क

एक और संभावना है - चुनाव-क्षेत्र को अपनी सेवाएं एक वार्षिक/ त्रैमासिक सदस्यता शुल्क के आधार पर बेचना । अतिरिक्त सेवाओं के लिए शुल्क प्रति-प्रयोग के आधार पर दिया जा सकता है, उदाहरण के लिये परामर्श सेवाएं या सुरक्षा ऑडिट ।

एक और विचार करने योग्य दृश्यलेख यह है : चुनाव-क्षेत्र (आंतरिक) के लिए सेवायें मुफ़्त में प्रदान की जाती हैं परंतु बाह्य ग्राहकों को प्रदान की जाने वाली सेवाओं के लिए भुगतान करना पड़ सकता है । एक और तरीका यह हो सकता है कि परामर्श और जानकारी पत्र सार्वजनिक वेबसाइट पर प्रकाशित किये जाएं और उनका एक "केवल सदस्य" प्रभाग हो जिसमें विशेष और अधिक विस्तृत या उपयुक्त जानकारी हो ।

यह प्रमाणित किया जा चुका है कि दरअसल "प्रति सी० एस० आई० आर० टी० सेवा के लिए अभिदान" अभ्यास का सीमित उपयोग है और वह भी काफ़ी वित्त प्रदान करने के लिए, ख़ासकर शुरूआती दौर में । उदाहरण के लिए दल और उपकरण के लिए ऐसे कुछ तय मूल व्यय हैं जिनका भुगतान पहले करना होता है । सी० एस० आई० आर० टी० सेवायें बेच कर इन व्ययों के लिए वित्त एकत्रित करना मुश्किल है और इसके लिए "ब्रेक-ईवन प्वांइट" पता लगाने के लिए बहुत विस्तृत वित्तीय विश्लेषण की ज़रूरत है ।

सहायिकी (सब्सिडी)

एक और विचार करने योग्य संभावना सरकार या सरकारी संगठन द्वारा प्रदान की जाने वाली परियोजना सहायिकी के लिए आवेदन करना चूंकि आजकल अधिकतर देशों के पास सूचना प्रौद्योगिकी सुरक्षा परियोजनाओं के लिए वित्त उपलब्ध है । गृह मंत्रालय से संपर्क करना एक अच्छी शुरूआत हो सकती है ।

बेशक विभिन्न स्थान संबंधी नमूनों का मिश्रण संभव है ।

6.2. संस्थानात्मक ढांचा परिभाषित करना

किसी सी० एस० आई० आर० टी० का उपयुक्त संगठनात्मक ढांचा काफ़ी हद तक मेज़बान संस्थान और चुनाव-क्षेत्र के पहले से मौजूद ढांचे पर निर्भर करता है । यह स्थायी या तदर्थ आधार पर नौकरी पर रखे जाने वाले कुशल विशेषज्ञों की उपलब्धता पर भी निर्भर करता है ।

एक विशेष सी० एस० आई० आर० टी० दल में निम्नलिखित भूमिकाएं परिभाषित करता है :

सामान्य

- महाप्रबंधक

कर्मचारी

- दफ़्तर का प्रबंधक
- लेखाकार
- संचार परामर्शदाता
- कानूनी परामर्शदाता

प्रचालक तकनीकी दल

- तकनीकी दल का नेता
- तकनीकी सी० एस० आई० आर० टी० तकनीकज्ञ जो सी० एस० आई० आर० टी० सेवाएं प्रदान करते हैं
- अनुसंधानकर्ता

बाह्य परामर्शदाता

- ज़रूरत पड़ने पर काम पर रखे जाते हैं

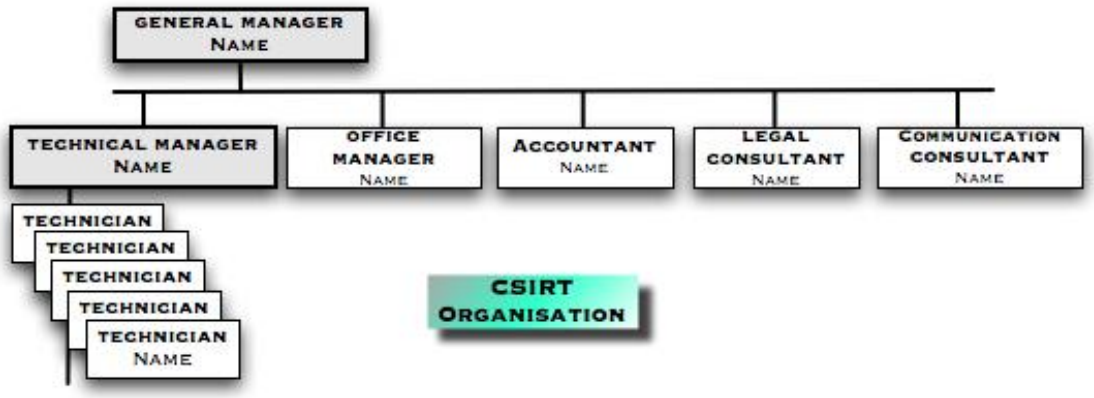
कर्मचारियों में कानूनी विशेषज्ञ का होना, ख़ासतौर पर सी० एस० आई० आर० टी० के शुरूआती दौर में, विशेषतौर पर मददगार होता है । इससे लागत तो ज़रूर बढ़ जाएगी परंतु अंत में समय का और कानूनी मुश्किलों से बचाव होगा ।

चुनाव-क्षेत्र में दक्षता की विविधता के आधार पर, और साथ ही जब मीडिया में सी० एस० आई० आर० टी० की महत्त्वपूर्ण छवि हो तो, दल में एक संचार विशेषज्ञ का होना भी बहुत उपयोगी सिद्ध हुआ है । यह विशेषज्ञ घटकों या मीडिया-सहयोगियों के लिए कठिन तकनीकी मुद्दों को अधिक आसानी से समझ में आने वाले संदेशों में परिवर्तित करने पर अपना ध्यान केंद्रित कर सकते हैं । संचार विशेषज्ञ तकनीकी विशेषज्ञों को चुनाव-क्षेत्र से प्रतिपुष्टि भी प्रदान करता है अतः वह एक इन दोनों समूहों के मध्य "अनुवादक" और "मददगार" के तौर पर भी काम कर सकता/सकती है ।

नीचे प्रचालन सी० एस० आई० आर० टी०ओं द्वारा प्रयुक्त संस्थानात्मक नमूनों के कुछ उदाहरण दिये गए हैं ।

6.2.1. स्वतंत्र व्यापारिक नमूना

सी० एस० आई० आर० टी० को चालू किया गया और यह एक ऐसे स्वतंत्र संस्थान के तौर पर काम करता है जिसका अपना प्रबंधन और अपने कर्मचारी हैं ।

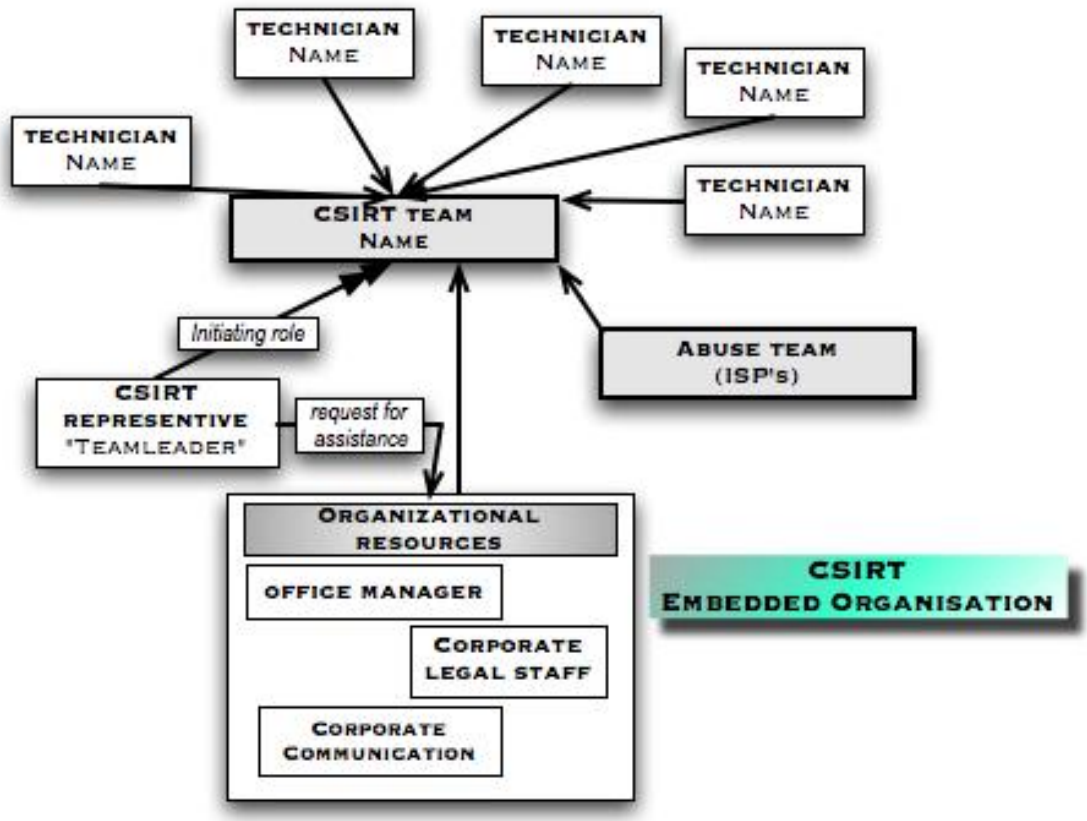


चित्र 5. *स्वतंत्र व्यापारिक नमूना*

6.2.2. जड़ा हुआ नमूना

अगर एक पहले से मौजूद संस्थान में सी० एस० आई० आर० टी० की शुरूआत करनी है तो इस नमूने, उदाहरण के लिए पहले से मौजूद सूचना प्रौद्योगिकी विभाग का उपयोग कर, का उपयोग किया जा सकता है । दल का नेता सी० एस० आई० आर० टी० का नेतृत्व करता है और वह सी० एस० आई० आर० टी० की गतिविधियों के लिए उत्तरदायी है । घटनाओं को सुलझाते समय या फिर सी० एस० आई० आर० टी० गतिविधियों पर काम करते समय दल का नेता ज़रूरी तकनीकज्ञों को एकत्रित करता है । वह एक पहले से मौजूद संस्थान में अंदर से विशेषज्ञों की सहायता के लिए निवेदन कर सकता/ सकती है ।

विशिष्ट परिस्थितियों के उत्पन्न होने पर इस नमूने को उनके अनुरूप भी बनाया जा सकता है । ऐसा होने पर दल को एक पूर्वनिश्चित संख्या या पूर्णावधि समतुल्य (एफ० टी० ई०) आवंटित किया गया है । उदाहरण के लिये, एक इंटरनेट सेवा प्रदाता का दुरुपयोग काउंटर निःसंदेह एक या (अधिकतर मामलों में) एक से ज़्यादा पूर्णावधि समतुल्य के लिए पूरे समय का काम है ।

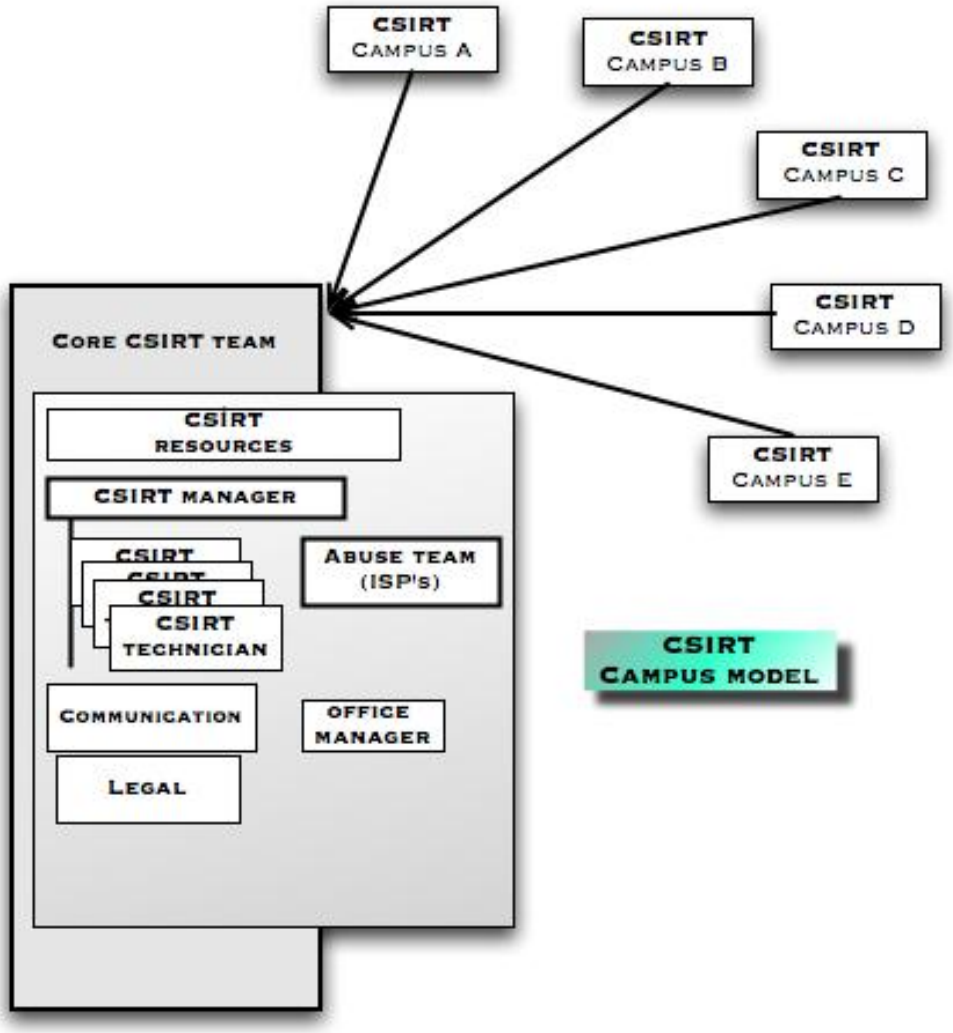


चित्र 6. *संस्थानात्मक जड़ा हुआ नमूना*

6.2.3. परिसर नमूना

जैसा कि नाम से पता लगता है, आम तौर पर परिसर नमूना शैक्षिक और अनुसंधान सी० एस० आई० आर० टी०ओं द्वारा अपनाया जाता है । अधिकतर शैक्षिक और अनुसंधान संस्थानों में एक क्षेत्र या फिर पूरे देश में अलग-अलग जगहों पर फैली विभिन्न विश्वविद्यालय और परिसर सुविधाएं शामिल होतीं हैं (जैसा कि एन० आर० ई० एन०, राष्ट्रीय अनुसंधान संगठन-तंत्र, के मामले में है) । आमतौर पर यह संस्थान एक-दूसरे से स्वतंत्र होते हैं और अक्सर वे अपने खुद के सी० एस० आई० आर० टी० चलाते हैं । आमतौर पर यह सी० एस० आई० आर० टी० एक 'माँ' या मूल सी० एस० आई० आर० टी० की छत्रछाया में संगठित होते हैं । मूल सी० एस० आई० आर० टी० समन्वयन करता है और बाह्य विश्व के लिए एकमात्र संपर्क-स्थल है । अधिकतर मामलों में मूल सी० एस० आई० आर० टी० उपयुक्त परिसर सी० एस० आई० आर० टी० को घटना संबंधी जानकारी वितरित करने के अलावा मूल सी० एस० आई० आर० टी० सेवायें भी प्रदान करेगा ।

कुछ सी० एस० आई० आर० टी० अपनी मूल सी० एस० आई० आर० टी० सेवायें अन्य परिसर सी० एस० आई० आर० टी०ओं के साथ भी वितरित करते हैं जिससे मूल सी० एस० आई० आर० टी० की अतिरिक्त लागत कम रहती है ।



चित्र 7. *परिसर नमूना*

6.2.4. स्वैच्छिक नमूना

यह संगठनात्मक नमूना एक ऐसे लोगों (विशेषज्ञों) के समूह का विस्तारपूर्वक विवरण देता है जो एक-दूसरे (और अन्य लोगों को) सलाह और सहारा देने के लिए स्वैच्छिक आधार पर साथ मिल कर काम करते हैं । यह एक ढीला समुदाह है और भाग लेने वालों के अभिप्रेरण पर बहुत ज़्यादा निर्भर करता है ।

उदाहरण के लिये यह नमूना वार्प (डबल्यू० ए० आर० पी०) समुदाय[13] द्वारा अपनाया गया है ।

[13] वॉर्प पहल http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_02.htm#12

6.3. उचित कर्मचारियों को नौकरी पर रखना

प्रदान की जाने वाली सेवाओं और सहारे के स्तर के बारे में निर्णय लेने और एक संगठनात्मक नमूना चुनने के बाद अगला चरण है सही संख्या में काम के लिए कुशल लोगों को ढूंढना ।

इस नज़रिये से कितने तकनीकी कर्मचारियों की ज़रूरत होगी इस बारे में असली अंक प्रदान करना लगभग असंभव है परंतु प्रमुख मूल्यों का अनुसरण करना एक अच्छा प्रस्ताव सिद्ध हुआ है :

- परामर्श-पत्रों के वितरण और घटना पर कार्रवाई करने की दो मूल सेवायें प्रदान करने के लिए : कम से कम **4** एफ० टी० ई० ।
- दफ़्तर के समय में एक पूर्ण सेवा सी० एस० आई० आर० टी० और तंत्र की देखभाल करने के लिए : कम से कम **6 से 8** एफ० टी० ई० ।
- एक ज़्यादा कर्मचारियों वाली 24x7 पारी (दफ़्तर के समय के अलावा 2 पारियां) के लिए कम से कम लगभग **12** एफ० टी० ई० ।

इन संख्याओं में बीमारी, छुट्टियों इत्यादी जैसी व्यतिरिक्तियां भी शामिल हैं । स्थानीय सामूहिक श्रम अनुबंधों को जाँचना भी आवश्यक है । अगर लोग दफ़्तर के समय के बाहर काम कर रहे हैं तो इससे जो अतिरिक्त भत्ता देना पड़ सकता है उसके रूप में अतिरिक्त लागत पड़ सकती है ।

एक सी० एस० आई० आर० टी० के लिए तकनीकी विशेषज्ञों के प्रमुख कौशलों का एक संक्षिप्त सिंहावलोकन नीचे दिया गया है :

आम तकनीकी कर्मचारी की नौकरी के विवरण के मद :

व्यक्तिगत कौशल

- लचीला, रचनात्मक और दल के साथ मिल कर काम करने का गुण ।
- प्रभावशाली विश्लेषणात्मक कौशल
- कठिन तकनीकी बातें आसान शब्दों में समझाने की क्षमता
- गोपनीयता और एक विधि-संबंधी विषय पर काम करने के लिए अच्छा अनुभव
- प्रबंध करने संबंधी अच्छे कौशल
- तनाव सहन करने की क्षमता
- विचार का आदान-प्रदान करने और लेखन के प्रभावशाली कौशल
- खुले दिमाग वाला/ वाली और सीखने के लिए तैयार

तकनीकी कौशल

- इंटरनेट प्रौद्योगिकी और प्रोटोकॉलों का विस्तृत ज्ञान
- लिनक्स और युनिक्स तंत्रों (चुनाव-क्षेत्र के उपकरण के अनुसार) का ज्ञान
- विंडोज़ तंत्रों (चुनाव-क्षेत्र के उपकरण के अनुसार) का ज्ञान
- संगठन-तंत्र अवसंरचना उपकरण (राउटर, स्विच, डी० एन० एस०, प्रोक्सी, मेल, इत्यादी) का ज्ञान
- इंटरनेट अनुप्रयोगों (एस० एम० टी० पी०, एच०टी०टी०पी०(एस०), एफ० टी० पी०, टेलनेट, एस० एस० एच, इत्यादि) का ज्ञान
- सुरक्षा संबंधी खतरों (डी० डॉस०, फिशिंग, डिफ़ेसिंग, स्निफ़िंग, इत्यादि) का ज्ञान
- जोखिम निर्धारण और व्यावहारिक कार्यान्वयनों का ज्ञान

अतिरिक्त कौशल

- 24x7 या कॉल ड्यूटी पर काम करने के लिए तैयार (सेवा नमूने के आधार पर)
- अधिकतम यात्रा दूरी (दफ़्तर में आपातकालीन उपलब्धता के मामले में ; अधिकतम यात्रा समय)
- शैक्षिक स्तर
- सूचना प्रौद्योगिकी सुरक्षा के क्षेत्र में काम करने का अनुभव

काल्पनिक सी० एस० आई० आर० टी० (चरण 4)
व्यापार योजना परिभाषित करना

वित्तीय नमूना

चूंकि कंपनी का एक 24x7 ई-व्यापार है और साथ ही एक 24x7 काम करने वाला सूचना प्रौद्योगिकी विभाग है अतः दफ़्तर के समय के दौरान पूर्ण सेवा और दफ़्तर के समय के अलावा बाकी समय पर कॉल-ड्यूटी प्रदान करने का निर्णय लिया जाता है । चुनाव-क्षेत्र के लिए सेवायें मुफ़्त प्रदान की जाएंगी परंतु प्रायोगिक और मूल्यांकन चरण के दौरान बाह्य ग्राहकों को सेवायें प्रदान करने की संभावना का मूल्यांकन किया जाएगा ।

आय का नमूना

शुरूआती- और प्रायोगिक- चरण के दौरान सी० एस० आई० आर० टी० को एक मेज़बान कंपनी के माध्यम से वित्त प्रदान किया जाएगा । प्रायोगिक- और मूल्यांकन चरण के दौरान बाह्य ग्राहकों को सेवायें बेचने की संभावना सहित अतिरिक्त वित्त सुलभ कराने के बारे में चर्चा की जाएगी ।

संस्थानात्मक नमूना

मेज़बान संस्थान एक छोटी कंपनी है इसलिए एक जड़ा हुआ नमूना चुना गया है ।
दफ़्तर के समय के दौरान तीन कर्मचारी मूलभूत-सेवायें (सुरक्षा परामर्शों का वितरण और घटना पर कार्रवाई/ उसका समन्वयन) प्रदान करेंगे ।

कंपनी के सूचना प्रौद्योगिकी विभाग में पहले से ही उपयुक्त कौशलों वाले लोग काम कर रहे हैं । उस विभाग के साथ एक अनुबंध किया जाता है जिससे नये सी० एस० आई० आर० टी० जब भी ज़रूरत पड़े तब तदर्थ आधार पर सहायता का निवेदन कर सके । साथ ही उनके ऑन-काल तकनीकज्ञों की दूसरी पंक्ति का इस्तेमाल किया जा सकता है ।
पूरे समय काम करने वाले चार सदस्यों और पाँच अतिरिक्त सी० एस० आई० आर० टी० दल के सदस्यों का एक मूल सी० एस० आई० आर० टी० दल होगा । उनमें से एक घूमने वाली पारी पर भी उपलब्ध होगा ।

कर्मचारी

सी० एस० आई० आर० टी० दल के नेता की सुरक्षा और 1$^{ले}$ और 2$^{रे}$ स्तर की सहायता की पृष्ठभूमि है और उसने प्रतिस्कंदन (रिसाइलियेंस) संकट प्रबंधन कार्यक्षेत्र में काम किया है । दल के अन्य तीन सदस्य सुरक्षा विशेषज्ञ हैं । सी० एस० आई० आर० टी० दल के अंशकालिक सदस्य सूचना प्रौद्योगिकी विभाग से हैं और उन्हें कंपनी की अवसंरचना के क्षेत्र में महारत हासिल है ।

6.4. *दफ़्तर का उपयोग और उपकरण*

उपकरण और दफ़्तर के स्थान व भौतिक सुरक्षा का उपयोग व्यापक विषय हैं इसलिए इस दस्तावेज़ में कोई भी पूर्ण विवरण नहीं दिया जा सकता । यह पाठ का उद्देश्य इस विषय का एक संक्षिप्त सिंहावलोकन देना है ।

भौतिक सुरक्षा के बारे में अधिक जानकारी निम्नलिखित पर मिल सकती है :
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"इमारत को कठोर बनाना"
चूंकि सी० एस० आई० आर० टी० आमतौर पर बहुत ही संवेदनशील जानकारी पर काम करते हैं इसलिए दल को दफ़्तर की भौतिक सुरक्षा का नियंत्रण लेने देना एक अच्छा अभ्यास है । यह काफ़ी हद तक मेज़बान कंपनी की मौजूदा सुविधाओं व अवसंरचना और मौजूदा जानकारी सुरक्षा नीति पर निर्भर करेगा ।

उदाहरण के लिये सरकारें वर्गीकरण योजनाओं के साथ काम करतीं हैं और गोपनीय जानकारी के उपयोग व रख-रखाव के बारे में बहुत सख्त हैं । स्थानीय नियमों और नीतियों के बारे में अपनी कंपनी या संस्थान से पता करें ।

आमतौर पर एक नई सी० एस० आई० आर० टी० को स्थानीय नियमों, नीतियों और अन्य कानूनी मुद्दों के बारे में जानने के लिए अपने मेज़बान संस्थान पर निर्भर रहना पड़ता है ।

जिन उपकरणों और सुरक्षा उपायों की ज़रूरत होगी उन सब का पूर्ण विवरण इस दस्तावेज़ के परास से बाहर है । तथापि नीचे आप अपने सी० एस० आई० आर० टी० के लिए मूल सुविधाओं की एक छोटी सूची देख सकते हैं :

इमारत के लिए सामान्य नियम

- पैठ नियंत्रणों का प्रयोग करें
- कम से कम सी० एस० आई० आर० टी० दफ़्तर केवल सी० एस० आई० आर० टी० कर्मचारियों के लिए सुलभ बनाएं ।
- दफ़्तर और प्रवेश-द्वारों पर कैमरे द्वारा नज़र रखें ।
- गोपनीय जानकारी लॉकरों या तिजोरी में सहेजें ।
- सुरक्षित सूचना प्रौद्योगिकी तंत्रों का उपयोग करें ।

सूचना प्रौद्योगिकी उपकरण के लिए सामान्य नियम

- उस उपकरण का उपयोग करें कर्मचारी जिसकी देखभाल कर सकें ।
- सभी तंत्रों को सशक्त बनाएं ।
- अपने तंत्रों को इंटरनेट से जोड़ने से पहले उन सब को पैच करें और उनका अद्यतन अद्यतन करें ।
- सुरक्षा प्रक्रिया सामग्री (फ़ॉयरवाल, एक से ज़्यादा एंटी-वॉयरस स्कैनर, एंटी-स्पाइवेयर, इत्यादि) का उपयोग करें ।

संचार-मार्ग बनाए रखना

- सार्वजनिक वेबसाइट
- वेबसाइट पर बंद सदस्य क्षेत्र
- घटनाओं की जानकारी देने के लिए वेब-प्रपत्र
- ई-मेल (पी० जी० पी०/ जी० पी० जी०/ एस०/माइम सहायता)
- मेलिंग सूची प्रक्रिया सामग्री
- चुनाव-क्षेत्र के लिए समर्पित फ़ोन नंबर उपलब्ध रखें :
    - फ़ोन
    - फ़ैक्स
    - एस० एम० एस०

अभिलेख (रिकॉर्ड) अन्वेषण तंत्र

- दल के सदस्यों, अन्य दलों, इत्यादि, के विवरण युक्त संपर्क आंकड़ा संचय
- ग्राहक संसाधन प्रबंधन (सी० आर० एम०) उपकरण
- घटना पर कार्रवाई के लिए टिकट तंत्र

शुरू से ही "सामूहिक शैली" का उपयोग करें

- मानक ई-मेल और परामर्श पत्र ले-आउट
- 'पुराने ढर्रे के' कागज़ पर लिखे गए पत्र

- मासिक या वार्षिक रिपोर्टें
- घटना रिपोर्ट प्रपत्र

अन्य मुद्दे

- आक्रमण होने पर आउट-ऑफ़-बैंड संचार का पूर्वानुमान लगाएं
- इंटरनेट संयोजन पर व्यतिरिक्ति का पूर्वानुमान लगाएं

एक विशिष्ट सी० एस० आई० आर० टी० के बारे में अधिक जानकारी प्राप्त के लिए पाठ *8.5 उपलब्ध सी० एस० आई० आर० टी० उपकरण* देखें ।

6.5. *जानकारी सुरक्षा नीति विकसित करना*

सी० एस० आई० आर० टी० के प्रकार के आधार पर आपके पास आपकी आवश्यकता के अनुरूप जानकारी सुरक्षा नीति होगी । प्रचालन और प्रशासनिक प्रक्रियाओं और कार्य-प्रणाली की अपेक्षित स्थिति के अलावा ऐसी नीति को, ख़ासकर सी० एस० आई० आर० टी० देयता के संबंध में, कानून और मानकों के अनुरूप होना चाहिए । आमतौर पर सी० एस० आई० आर० टी० राष्ट्रीय कानूनों और नियमों से बंधी है जो अक्सर युरोपीय कानून और अन्य अंतर्राष्ट्रीय अनुबधों के संदर्भ में कार्यान्वित किये जाते हैं । ज़रूरी नहीं कि मानक सीधे बाध्य करने वाले हों परंतु वे जनादेश द्वारा या नियमों और कानूनों द्वारा सुझाये गए हो सकते हैं ।

नीचे संभावित कानूनों और नीतियों की एक छोटी सूची दी गई है ।

राष्ट्रीय

- सूचना प्रौद्योगिकी, दूरसंचार प्रणाली, मीडिया
- आंकड़ों की सुरक्षा और गोपनीयता संबंधी कानून
- आंकड़े अवधारण करने संबंधी नियम और कानून
- वित्त, लेखाकरण और कंपनी के प्रबंधन संबंधी कानून
- निगम प्रशासन और सूचना प्रौद्योगिकी के प्रशासन संबंधी आचार संहिताएं

युरोपीय

- इलेक्ट्रॉनिक हस्ताक्षरों संबंधी निदेश (1993/93/EC)
- आंकड़ों की सुरक्षा (1995/46/EC) और इलेक्ट्रॉनिक संचार में गोपनीयता संबंधी निदेश (2002/58/EC)
- इलेक्ट्रॉनिक संचार संगठन-तंत्र और सेवाओं संबंधी निदेश (2002/19/EC - 2002/22/EC)
- कंपनी कानून संबंधी निदेश (उदाहरण के लिए कंपनी कानून निदेश)

अंतर्राष्ट्रीय

- बासेल II अनुबंध (ख़ासकर प्रचालन जोखिम के प्रबंधन के संबंध में)
- साइबर-अपराध संबंधी युरोप की परिषद का अनुबंध/ सम्मेलन
- मानव-अधिकारों के संबंध में युरोपीय परिषद का अनुबंध (गोपनीयता संबंधी नियम 8)
- अंतर्राष्ट्रीय लेखाकरण मानक (आई० ए० एस०; वे कुछ हद तक सूचना प्रौद्योगिकी नियंत्रणों को भी आदेश देते हैं)

मानक

- ब्रिटिश मानक BS 7799 (सूचना सुरक्षा)
- अंतर्राष्ट्रीय मानक ISO2700x (सूचना सुरक्षा प्रबंधन तंत्र)
- जर्मन आई०टी०-ग्रुंड्शुट्ज़बुख, फ़्राँसीसी ईबॉयोस और अन्य राष्ट्रीय भिन्नताएं

क्या आपकी सी० एस० आई० आर० टी० राष्ट्रीय और अंतर्राष्ट्रीय कानूनों के अनुसार काम कर रही है यह पता लगाने के लिए कृपया अपने कानूनी सलाहकार से परामर्श करें ।

आपकी सूचना पर कार्रवाई करने की नीतियों में जिन सबसे मूल प्रश्नों का उत्तर देना है वे निम्नलिखित हैं :

- आगत जानकारी को कैसे "लेबल लगाना" या "वर्गीकृत करना" है ?
- जानकारी पर कार्रवाई, ख़ासकर विशिष्टिकरण के संबंध में, कैसे की जाती है ?
- जानकारी के प्रकटीकरण, विशेषकर अगर घटना से संबंधित जानकारी अन्य दलों या स्थानों को आगे भेजी जाती है, के लिए कौन-से विचार अपनाये जाते हैं ?
- क्या ऐसे कोई कानूनी विचार हैं जिन्हे सूचना पर कार्रवाई के संबंध में ध्यान में रखने की ज़रूरत है ?
- क्या सहेजी गई जानकारी और/ या आंकड़ों के संचार, ख़ासकर ई-मेल द्वारा, की विशिष्टता व अखंडता को सुरक्षित रखने के लिए क्रिप्टोग्राफ़ी के उपयोग संबंधी आपकी कोई नीति है ?
- क्या कानूनी मुकदमों के मामले में इस नीति में 'की एस्क्रो' या 'डिक्रिप्शन की प्रवर्तनीयता' जैसी कानूनी सीमा शर्तें शामिल हैं ?

काल्पनिक सी० एस० आई० आर० टी० (चरण 5)
दफ़्तर के उपकरण और स्थान चूंकि मेज़बान कंपनी के पास पहले से ही कारगर भौतिक सुरक्षा है इसलिए नया सी० एस० आई० आर० टी० उस नज़रिये से अच्छी तरह सुरक्षित है । आपातकालीन स्थिति में समन्वयन संभव बनाने के लिए एक तथाकथित "युद्ध कक्ष" प्रदान किया जाता है । सामग्री और संवेदनशील दस्तावेज़ों के 'एन्क्रिप्शन' के लिए एक तिजोरी खरीदी जाती है । दफ़्तर के समय हॉटलाइन आसान बनाने के लिए स्विचबोर्ड युक्त एक अलग फ़ोन लाइन स्थापित की गई थी और दफ़्तर के समय के बाद 'ऑन-कॉल' ड्यूटी के लिए उसी फ़ोन नंबर वाला मोबाइल फ़ोन प्रदान किया गया था । सी० एस० आई० आर० टी० संबंधी जानकारी की घोषणा करने के लिए पहले से मौजूद उपकरण और निगम की वेबसाइट का भी उपयोग किया जा सकता है । दल के सदस्यों में आपस में और अन्य दलों के साथ संचार के एक सीमित भाग के साथ एक 'मेलिंग सूची' लगाई और अनुरक्षित

की जाती है । कर्मचारियों से संपर्क करने संबंधी सभी विवरण एक आंकड़ा संचय में सहेजे जाते हैं और इनकी एक छपी हुई प्रति तिजोरी में रखी जाती है ।

विनियम

चूंकि सी० एस० आई० आर० टी० कंपनी में उसकी पहले से मौजूद सूचना सुरक्षा नीतियों में जड़ा जाता है इसलिए सी० एस० आई० आर० टी० के लिए अनुरूपण नीतियां कंपनी के कानूनी सलाहकार की मदद से स्थापित की गईं हैं ।

6.6. *अन्य सी० एस० आई० आर० टी०ओं के बीच सहयोग और संभावित राष्ट्रीय पहलों की खोज*

अन्य सी० एस० आई० आर० टी० पहलों का पहले से मौजूद होना और उनमें सहयोग की अत्याधिक आवश्यकता के बारे में इस दस्तावेज़ में पहले ही चर्चा की जा चुकी है । सी० एस० आई० आर० टी० समुदायों के साथ ज़रूरी संपर्क स्थापित करने के लिए अन्य सी० एस० आई० आर० टी०ओं से यथाशीघ्र संपर्क करना एक अच्छा अभ्यास है । आमतौर पर अन्य सी० एस० आई० आर० टी० बहुत खुले होते हैं और हाल ही में बनाए गए दलों को काम शुरू करने में मदद करते हैं ।

एनीसा की युरोप में सी० ई० आर० टी० गतिविधियों की सूची[14] देश में अन्य सी० एस० आई० आर० टी०ओं या फिर राष्ट्रीय सी० एस० आई० आर० टी० सहयोग गतिविधियों की खोज की शुरूआत करने का एक अच्छा स्थान है ।

सी० एस० आई० आर० टी० जानकारी का उपयुक्त स्त्रोत खोजने में मदद प्राप्त करने के लिए एनीसा के सी० एस० आई० आर० टी० विशेषज्ञों से संपर्क करें :

cert-relations@enisa.europa.eu

[14] एनीसा की सूची : http://www.enisa.europa.eu/ENISA%20CERT

नीचे सी० एस० आई० आर० टी० की सामुदायिक गतिविधियों का सिंहावलोकन दिया गया है : कृपया अधिक व्यापक विवरण और जानकारी के लिए *सूची* देखें ।

युरोपीय सी० एस० आई० आर० टी० पहल

टी० एफ़० - सी० एस० आई० आर० टी०[15]

टी०एफ़०-सी० एस० आई० आर० टी० कार्यबल युरोप में मौजूद कंप्यूटर सुरक्षा घटना प्रत्युत्तर दलों (सी० एस० आई० आर० टी०) में सहयोग को बढ़ावा देता है । इस कार्य-बल के प्रमुख लक्ष्य हैं - अनुभव और ज्ञान के आदान-प्रदान के लिए मंच प्रदान करना, युरोपीय सी० एस० आई० आर० टी०ओं के समुदाय के लिए प्रायोगिक सेवायें स्थापित करना और नए सी० एस० आई० आर० टी० की स्थापना में मदद करना ।

कार्य-बल के मुख्य लक्ष्य हैं :

- अनुभव और ज्ञान के आदान-प्रदान के लिए मंच प्रदान करना
- युरोपीय सी० एस० आई० आर० टी०ओं के समुदाय के लिए प्रायोगिक सेवायें स्थापित करना
- सुरक्षा घटनाओं के प्रति प्रतिक्रिया के लिए सामान्य मानकों और प्रक्रियाओं को बढ़ावा देना
- नए सी० एस० आई० आर० टी०ओं की स्थापना और सी० एस० आई० आर० टी० के कर्मचारियों के प्रशिक्षण में मदद करना ।
- टेरेना की तकनीकी समिति द्वारा 15 सितंबर 2004 को स्वीकृत विचारार्थ विषय की सीमाओं के अनुसार टी० एफ़० - सी० एस० आई० आर० टी० की गतिविधियां युरोप और उसके पड़ोसी देशों पर केंद्रित हैं ।

वैश्विक सी० एस० आई० आर० टी० पहल

पहला[16]

पहला (फ़र्स्ट) एक प्रमुख संस्थान है जिसे घटना के प्रति प्रतिक्रिया के क्षेत्र में विश्व में अग्रणी के रूप में मान्यता-प्राप्त है । पहला घटना के प्रति प्रतिक्रिया करने वाले दलों को सुरक्षा-संबंधी घटनाओं के प्रति अधिक कारगर ढंग से प्रतिक्रिया - प्रतिक्रियात्मक और सक्रिय दोनों प्रकार की - करने में मदद करता है ।

पहला सरकार, व्यापारिक और शैक्षिक संस्थानों से विविध प्रकार के कंप्यूटर सुरक्षा घटना प्रतिक्रिया दलों को एक छत्रछाया में लाता है । पहला का लक्ष्य घटना को होने से रोकने में सहयोग और समन्वयन करने, घटनाओं के प्रति तेज़ प्रतिक्रिया करने के लिए प्रेरित करने और सदस्यों और मोटे तौर पर समुदायों के बीच जानकारी के आदान-प्रदान को बढ़ावा देना है ।

---

[15] टी०एफ़०-सी०एस०आई०आर०टी० : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_01_02.htm#06

[16] पहला : http://www.enisa.europa.eu/ENISA%20CERT/pages/05_02.htm

विश्वास नेटवर्क के अलावा पहला वैश्विक घटना प्रत्युत्तर समुदाय बनाता है, पहला विशेष उपयोगी सेवाएं भी प्रदान करता है ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 6)
सहयोग की खोज करना एनीसा की सूची का इस्तेमाल कर एक ही देश में मौजूद कुछ सी० एस० आई० आर० टी० खोजे गए और उनसे संपर्क किया गया । उनमें से एक के साथ हाल ही में काम पर रखे गए दल-नेता के लिए स्थान-यात्रा आयोजित की गई । उसने राष्ट्रीय सी० एस० आई० आर० टी० गतिविधियों के बारे में सीखा और एक बैठक में भाग लिया । यह बैठक काम करने के तरीकों के उदाहरण एकत्रित करने और कुछ अन्य दलों से सहयोग प्राप्त करने में बहुत ज़्यादा मददगार साबित हुई ।

7. व्यापार योजना को बढ़ावा देना

हमने अब तक निम्नलिखित कदम उठायें हैं:

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।
4. वातावरण और घटकों का विश्लेषण
5. उद्देश्य कथन परिभाषित करना
6. व्यापार योजना का विकास करना
    - क. वित्तीय नमूना परिभाषित करना
    - ख. संस्थानात्मक ढांचा परिभाषित करना
    - ग. कर्मचारियों को नौकरी पर रखना शुरू करना
    - घ. दफ़्तर का उपयोग करना और दफ़्तर को सुस्सजित करना
    - च. जानकारी सुरक्षा नीति विकसित करना
    - छ. सहयोग के लिए साझेदारों को खोजना

>> अगला चरण है - उपरोक्त को एक परियोजना योजना में लिखना और काम शुरू करना !

अपनी परियोजना को परिभाषित करने के लिए एक अच्छी शुरूआत है - एक व्यापारिक मामले के बारे में सोचना । इस व्यापार मामले का उपयोग परियोजना योजना के आधार के तौर पर और

प्रबंधन सहायता के लिए आवेदन करने व वित्त व अन्य संसाधन प्राप्त करने के लिए किया जाएगा ।

सूचना प्रौद्योगिकी सुरक्षा समस्याओं के बारे में जानकारी का स्तर उच्च बनाए रखने के लिए प्रबंधन को लगातार सूचित करना बहुत उपयोगी सिद्ध हुआ और ऐसा अपनी सी० एस० आई० आर० टी० की लगातार सहायता कर किया गया ।

एक व्यापार मामले की शुरूआत *पाठ 5.3 चुनाव-क्षेत्र का विश्लेषण* में जिस विश्लेषण नमूने के बारे में विस्तारपूर्वक बताया गया है उसका उपयोग कर समस्या और मौकों का विश्लेषण कर और संभावित चुनाव-क्षेत्र के साथ निकट संपर्क स्थापित कर होती है ।

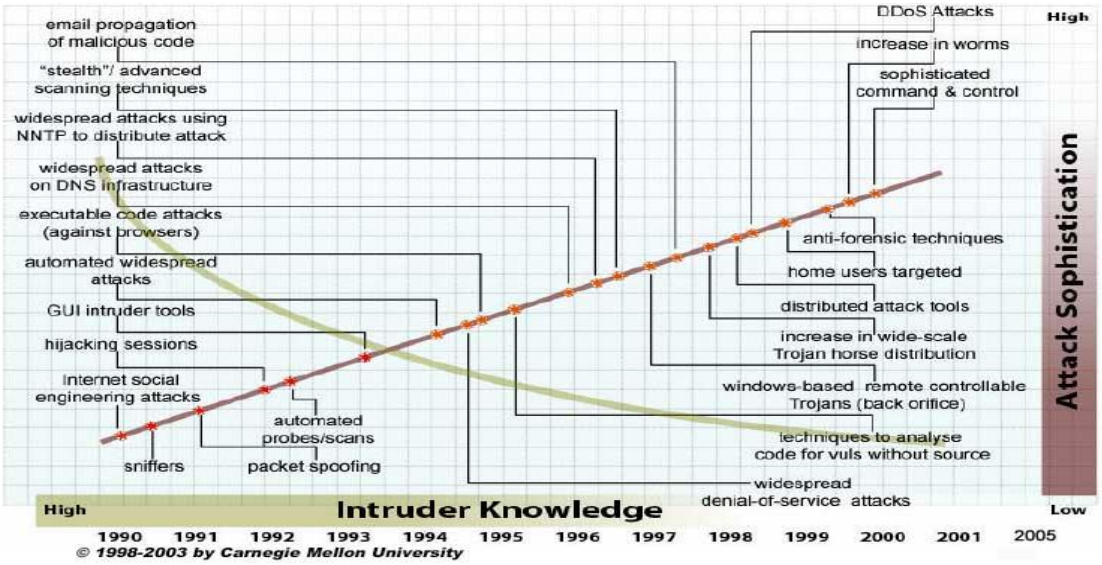
जैसा कि पहले विस्तारपूर्वक बताया गया है एक सी० एस० आई० आर० टी० शुरू करने से पहले बहुत-सी बातों पर विचार करना ज़रूरी है । जैसे-जैसे सी० एस० आई० आर० टी० विकसित होते हैं वैसे-वैसे उपरोक्त सामग्री को उनकी ज़रूरतों के अनुसार समायोजित करना सबसे बेहतर है ।

प्रबंधन को सूचित करते समय हाल में अख़बारों में या इंटरनेट पर छपे लेखों का प्रयोग कर अपने मामले को जितना अद्यतित कर सकें करना और सी० एस० आई० आर० टी० सेवा और घटनाओं का आंतरिक समन्वयन करना सुरक्षित व्यापार परिसंपत्तियों के लिए महत्त्वपूर्ण क्यों है यह विस्तारपूर्वक बताना एक अच्छा अभ्यास है । यह स्पष्ट करना भी ज़रूरी है कि सूचना प्रौद्योगिकी सुरक्षा के मामलों में केवल लगातार सहायता ही स्थिर व्यापार की ओर ले जाती है ख़ासकर एक ऐसी कंपनी या संस्थान को जो सूचना प्रौद्योगिकी पर निर्भर करता है ।

(ब्रूस श्नायॅर का एक प्रसिद्ध वाक्य इस मुद्दे को सामने लाता है : *"सुरक्षा एक उत्पाद नहीं अपितु एक प्रक्रिया है*[17] *!")*

सी०ई०आर०टी०/सी०सी० द्वारा प्रदान किया गया निम्नलिखित ग्राफ़ सुरक्षा-संबंधी समस्याओं को प्रदर्शित करने का एक प्रसिद्ध उपकरण है :

[17] ब्रूस श्नाएअर : http://www.schneier.com/



चित्र 8. *घुसपैठिये के बारे में जानकारी बनाम आक्रमण की जटिलता* (*स्त्रोत सी०ई०आर०टी०-सी०सी०*[18])

यह सूचना प्रौद्योगिकी सुरक्षा के क्षेत्र में रुझानों, विशेषकर बढ़ती हुई जटिलता वाले आक्रमणों को करने के लिए ज़रूरी कौशल में कमी, का मानसदर्शन करता है ।

एक और चर्चा करने योग्य मुद्दा है - असुरक्षाओं के लिए प्रक्रिया सामग्री के अद्यतनों की उपलब्धता और उनके ख़िलाव शुरू होते आक्रमणों के बीच लगातार छोटी होती समय-खिड़की ।

पैच ->आक्रमण		**फैलने की दर**	
निम्दा :	11 महीने	लाल कोड :	दिन
स्लैमर :	6 महीने	निम्दा:	घंटे
नाची :	5 महीने	स्लैमर:	मिनट
ब्लास्टर :	3 सप्ताह		
विट्टी :	1 दिन (!)		

घटनाओं के एकत्रित आंकड़े, संभावित सुधार और सीखी गईं सीखें भी एक अच्छी प्रस्तुति बनाते हैं ।

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1. व्यापार योजनाओं और प्रबंधन लिबलिबियों के विवरण

केवल सी० एस० आई० आर० टी० को बढ़ावा देने सहित प्रबंधन के लिए एक प्रस्तुति ही व्यापार मामला नहीं बनाती अपितु अगर इसे ठीक से लागू किया जाए तो अधिकतर मामलों में यह सी० एस० आई० आर० टी० के लिए प्रबंधन से समर्थन की ओर ले जाएगी । दूसरी ओर व्यापार मामले को केवल एक प्रबंधन अभ्यास के तौर पर ही नहीं देखना चाहिए अपितु इसका उपयोग दल और चुनाव-क्षेत्र के साथ विचारों के आदान-प्रदान के लिए भी किया जाना चाहिए । हो सकता है कि व्यापार मामला शब्द बहुत व्यापारिक और दैनिक सी० एस० आई० आर० टी० अभ्यास से दूर लगे परंतु यह सी० एस० आई० आर० टी० स्थापित करते समय ध्यान का अच्छा केंद्र और दिशा प्रदान करता है ।

निम्नलिखित प्रश्नों के उत्तरों का उपयोग एक अच्छा व्यापार मामला बनाने के लिए किया जा सकता है (दिये गए उदाहरण काल्पनिक हैं और केवल दर्शाने के लिए दिये गए हैं । "असली" उत्तर "असली" परिस्थितियों पर बहुत ज़्यादा निर्भर करते हैं) ।

- समस्या क्या है ?
- आप अपने घटकों के साथ क्या प्राप्त करना चाहेंगे ?
- अगर आप कुछ नहीं करते तो क्या होगा ?
- अगर आप कार्रवाई करते हैं तो क्या होगा ?
- इसकी लागत क्या आएगी ?
- क्या लाभ होगा ?
- आप कब शुरू करेंगे और यह कब ख़त्म होगा ?

समस्या क्या है ?

अधिकतर मामलों में सी० एस० आई० आर० टी० स्थापित करने का विचार तब उत्पन्न होता है जब सूचना प्रौद्योगिकी सुरक्षा कंपनी या संस्थान के मूल-व्यापार का महत्त्वपूर्ण हिस्सा बन चुकी होती है और जब सूचना प्रौद्योगिकी सुरक्षा एक व्यापारिक जोखिम बन सुरक्षा के शमन करने को एक सामान्य व्यापारिक कार्य बना देती है ।

अधिकतर कंपनियों और संस्थानों के पास नियमित सहायता विभाग या सहायता काउंटर है परंतु अधिकतर मामलों में सुरक्षा-संबंधी घटनाओं से अपर्याप्त ढंग से निपटा जाता है और यह उतने संगठित नहीं है जितना कि इनको होना चाहिए । अधिकतर मामलों में सुरक्षा घटना कार्य-क्षेत्र को विशेष कौशलों और ध्यान की ज़रूरत होती है । एक अधिक संगठित नज़रिया होना भी फ़ायदेमंद है और यह व्यापार जोख़िमों व कंपनी को होने वाले नुक्सान का शमन करेगा ।

अधिकतर मामलों में समस्या यह है कि समन्वयन की कमी होती है और घटनाओं का सामना करने के लिए मौजूदा ज्ञान का उपयोग नहीं किया जाता जो भविष्य में उन्हें होने से और संभावित वित्तीय हानियों और/ या एक संस्थान की ख्याति को क्षति को होने से रोक सकती है ।

चुनाव-क्षेत्र के साथ किन लक्ष्यों को प्राप्त करना है ?

जैसा कि आपको पहले विस्तारपूर्वक बताया गया है आपका सी० एस० आई० आर० टी० अपने घटकों की सेवा करेगा और सूचना प्रौद्योगिकी सुरक्षा घटनाओं व समस्याओं को सुल्झाने में उनकी मदद करेगा । सूचना प्रौद्योगिकी सुरक्षा संबंधी ज्ञान के स्तर को ऊँचा उठाना और एक सुरक्षा जानकार संस्कृति प्राप्त करना अतिरिक्त लक्ष्य हैं ।

यह लक्ष्य शुरू से ही सक्रिय और बचाव के उपाय लेने की कोशिश करता है और इसलिए प्रचालन लागतें घटाता है ।

अधिकतर मामलों में एक कंपनी या संस्थान के सहयोग या मदद के लिए इस संस्कृति को लागू करने से आमतौर पर दक्षता को बढ़ावा मिलता है ।

अगर कुछ न किया जाए तो क्या होगा ?

सूचना प्रौद्योगिकी सुरक्षा पर कार्रवाई करने के एक असंगठित तरीके से और हानि हो सकती है और इस हानि में संस्थान की ख्याति को होने वाली हानि सबसे कम नहीं है । वित्तीय हानियां और कानूनी अभिप्राय अन्य नतीजे हो सकते हैं ।

अगर कार्रवाई की जाए तो क्या होगा ?

सुरक्षा समस्याओं के होने से संबंधित ज्ञान बढ़ता है । इससे उन्हें अधिक कारगर ढंग से सुलझाने और भविष्य में नुक्सान होने से बचने में मदद मिलती है ।

इसकी लागत क्या आएगी ?

संगठनात्मक नमूने के आधार पर इस के कारण सी० एस० आई० आर० टी० दल के सदस्यों और संस्थानों के वेतन, उपकरण, औजार और प्रक्रिया सामग्री के लाइसेंस की लागत लगेगी ।

इससे क्या लाभ होगा ?

चूंकि व्यापार और भूतकाल में हुई हानियों के आधार पर यह प्रक्रियाओं व सुरक्षा अभ्यासों में अधिक पारदर्शिता प्राप्त करेगा अतः इससे ज़रूरी व्यापारिक परिसंपत्तियों की सुरक्षा करेगा ।

समय-रेखा क्या है ?

परियोजना योजना के विवरण के नमूने के लिए *पाठ 12. एक परियोजना योजना का विवरण* देखें ।

मौजूदा व्यापारिक मामलों और प्रस्तावों के उदाहरण

अध्ययन-योग्य सी० एस० आई० आर० टी० व्यापार मामलों के कुछ उदाहरण नीचे दिये गए हैं :

- http://www.cert.org/csirts/AFI_case-study.html
  एक सी० एस० आई० आर० टी० वित्तीय संस्थानों का निर्माण करना : एक मामले का अध्ययन

  इस दस्तावेज़ का उद्देश्य वित्तीय संस्थानों द्वारा सीखी गई सीखों का आपस में आदान-प्रदान (जिसे इस दस्तावेज़ में ए० एफ़० आई० का नाम दिया गया है) करना है चूंकि उन्होंने सुरक्षा-संबंधी चिंताओं व कंप्यूटर सुरक्षा घटना प्रत्युत्तर दल (सी० एस० आई० आर० टी०) पर चर्चा के लिए एक योजना विकसित व लागू की ।

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  सेर्ट पोल्स्का व्यापार मामले का सारांश (पी० डी० एफ़० फ़ॉर्मेट में स्लाइडशो) ।

- http://www.auscert.org.au/render.html?it=2252
  1990 के दशक में एक घटना प्रत्युत्तर दल (आई० आर० टी०) बनाना एक कठिन कार्य हो सकता है । आई० आर० टी० बनाने वाले कई लोगों के पास इसे करने का कोई अनुभव नहीं होता । यह दस्तावेज़ समुदाय में आई० आर० टी० द्वारा निभाई जाने वाली भूमिका और बनाते समय और प्रचालनों को शुरू करते समय जिन मुद्दों पर कार्रवाई की जानी चाहिए उन दोनों की जाँच करता है । इससे पहले से मौजूद आई०आर०टी०ओं को फ़ायदा हो सकता है क्योंकि इससे उन मुद्दों के बारे में ज्ञान बढ़ता है जिनके बारे में पहले चर्चा नहीं की गई ।

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  सूचना सुरक्षा, कंपनी को सुरक्षित करने संबंधी मामले का अध्ययन, रोजर बेन्टन द्वारा

  यह एक बीमा कंपनी की पूरी कंपनी के सुरक्षा-तंत्र की ओर जाने का एक व्यावहारिक मामला-अध्ययन है । यह व्यावहारिक कार्य करने का कारण एक सुरक्षा तंत्र बनाते या स्थानांतरित करते समय पालन करने के लिए एक पथ प्रदान करना है । शुरूआत में, एक मौलिक ऑनलाइन सुरक्षा तंत्र निगम के आंकड़ों तक पहुँच को नियंत्रित करने का एकमात्र तरीका था । अरक्षित छोड़ना गंभीर था - ऑनलाइन वातावरण के बाहर कोई भी अखंडता नियंत्रण नहीं थे । मौलिक प्रोग्रेमिंग कौशलों वाला कोई भी व्यक्ति उत्पादन आंकड़े जोड़, बदल और/ या मिटा सकता था ।

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  मैरियॅट की ई-सुरक्षा रणनीति : व्यापार-सूचना प्रौद्योगिकी सहयोग

  मैरियॅट इंटर्नेश्नल इन्क के क्रिस ज़ोलाद्ज़ का अनुभव यह है कि ई-व्यापार सुरक्षा एक परियोजना न हो कर एक प्रक्रिया है । ज़ोलाद्ज़ ने यह संदेश अभी हाल ही में इंटरमीडिया समूह द्वारा प्रायोजित बोस्टन में हुए ई-सुरक्षा सम्मेलन और एक्स्पो में दिया । हालांकि ज़ोलाद्ज़ वकील नहीं हैं तथापि मैरियट के सूचना सुरक्षा उपाध्यक्ष के रूप में वे कानूनी विभाग के माध्यम से सूचना देते हैं । उनका कार्य यह पता लगाना है कि मैरियट की सबसे ज़्यादा मूल्यवान व्यापारिक जानकारी कहाँ सहेजी गई है और यह कंपनी के अंदर और बाहर एक स्थान से दूसरे स्थान पर कैसे जाती है । मैरियट में तकनीकी अवसंरचना की सहायक सुरक्षा के लिए एक अलग ज़िम्मेदारी परिभाषित की गई है जो कि एक सूचना प्रौद्योगिकी सुरक्षा आर्किटेक्ट को दी जाती है ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 7)
व्यापार योजना को बढ़ावा देना कंपनी के इतिहास से तथ्य और अंक एकत्रित करने का निर्णय लिया जाता है । सूचना प्रौद्योगिकी सुरक्षा परिस्थिति के आंकड़ा सिंहावलोकन के लिए यह अत्याधिक उपयोगी है । जब सी० एस० आई० आर० टी० काम कर रहा हो तब यह संग्रह जारी रखा जाना चाहिए जिससे आंकड़ों अद्यतित रखा जा सके । अन्य राष्ट्रीय सी० एस० आई० आर० टी०ओं से भी संपर्क किया गया और उनके व्यापारिक मामलों के बारे में उनका साक्षात्कार लिया गया । उन्होंने सूचना प्रौद्योगिकी सुरक्षा घटनाओं के क्षेत्र में हाल में हुए विकासों और घटनाओं की लागतों के बारे में कुछ स्लाइडें बना कर सहायता की ।

उदाहरण के तौर पर दिये गए इस काल्पनिक सी० एस० आई० आर० टी० के मामले में प्रबंधन को सूचना प्रौद्योगिकी व्यापार के महत्त्व के बारे में विश्वास दिलाने की कोई ख़ास जल्दी नहीं थी और इसलिए पहले कदम के लिए आगे बढ़ने की अनुमति प्राप्त करना कठिन नहीं था । स्थापित करने और प्रचालन की लागत के अनुमान सहित एक व्यापार मामला और एक परियोजना योजना तैयार किये गए थे ।

8. प्रचालन संबंधी और तकनीकी कार्य-प्रणालियों के उदाहरण (कार्य-प्रवाह)

हमने अब तक निम्नलिखित कदम उठायें हैं:

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।
4. वातावरण और घटकों का विश्लेषण ।
5. उद्देश्य कथन परिभाषित करना ।
6. व्यापार योजना का विकास करना ।
   क. वित्तीय नमूना परिभाषित करना ।
   ख. संस्थानात्मक ढांचा परिभाषित करना ।
   ग. कर्मचारियों को नौकरी पर रखना शुरू करना ।
   घ. दफ़्तर का उपयोग करना और दफ़्तर को सुस्सजित करना
   च. जानकारी सुरक्षा नीति विकसित करना ।
   छ. सहयोग के लिए साझेदारों को खोजना ।
7. व्यापार योजना को बढ़ावा देना ।
   क. व्यापार मामले को स्वीकृत करवाना ।
   ख. सबकुछ परियोजना योजना में पूरी तरह लगाना ।

>> अगला कदम है : सी० एस० आई० आर० टी० को चालू करना

ठीक प्रकार से परिभाषित कार्य-प्रवाह होने से गुणवत्ता बेहतर होगी और प्रति घटना या संवेदनशीलता मामले के लिए ज़रूरी समय बेहतर बनेगा ।

जैसा कि प्रकोष्ठों में दिये गए उदाहरणों में विस्तारपूर्वक बताया गया है काल्पनिक सी० एस० आई० आर० टी० मौलिक मूल सी० एस० आई० आर० टी० सेवायें प्रदान करेगा :

- सतर्कादेश और चेतावनियां
- घटनाओं पर कार्रवाई
- घोषणाएं

यह पाठ उन कार्य-प्रवाहों के उदाहरण देता है जो एक सी० एस० आई० आर० टी० की मूल सेवाओं के बारे में विस्तारपूर्वक बताते हैं । इस पाठ में विभिन्न स्त्रोतों से जानकारी एकत्रित करने, इसकी प्रासंगिकता व सच्चाई की जाँच करने और पुनः चुनाव-क्षेत्र में वितरित करने के बारे में जानकारी दी गई है । और अंत में इस पाठ में सर्वाधिक प्राथमिक प्रक्रियाओं और विशिष्ट सी० एस० आई० आर० टी० उपकरणों के उदाहरण दिये गए हैं ।

8.1. चुनाव-क्षेत्र के संस्थापन आधार का मूल्यांकन करें

पहला कदम है आपके चुनाव-क्षेत्र में स्थापित सूचना प्रौद्योगिकी तंत्रों का सिंहावलोकन प्राप्त करना । इसके द्वारा सी० एस० आई० आर० टी० आने वाली जानकारी की प्रासंगिकता का मूल्यांकन कर सकता है और इसे पुनः वितरित करने से पहले इसकी जाँच कर सकता है जिससे कि संघटक ऐसी जानकारी में न डूब जाएं जो उनके लिए मूलतः बेकार है ।

साधारण से शुरू करना एक अच्छा अभ्यास है, उदाहरण के लिये निम्नलिखित एक्सेल शीट का प्रयोग कर :

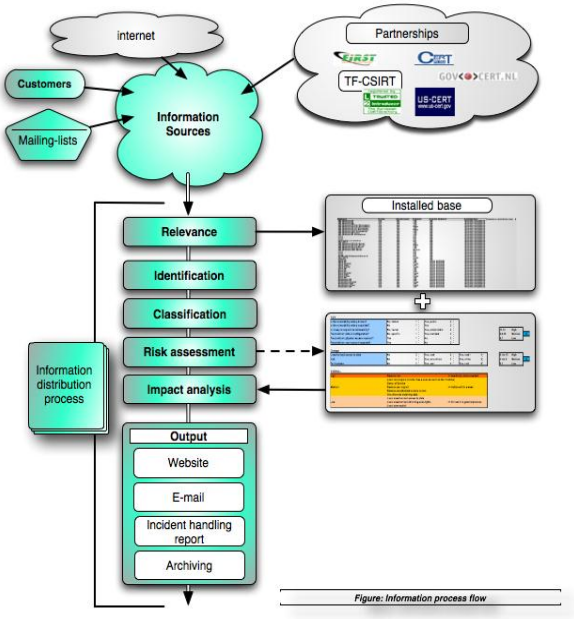
श्रेणी	अनुप्रयोग	प्रक्रिया सामग्री	संस्करण	ओ०एस०	ओ०एस० संस्करण	संघटक
डेस्कटॉप	ऑफ़िस	एक्सेल	x-x-x	माइक्रोसॉफ़्ट	एक्स०पी०-प्रो़फ़०	ए
डेस्कटॉप	ब्राउज़र	आई० ई०	x-x-	माइक्रोसॉफ़्ट	एक्स०पी०-प्रो़फ़०	ए
संगठन-तंत्र	राउटर	सिस्को	x-x-x	सिस्को	x-x-x-	बी
सर्वर	सर्वर	लिनक्स	x-x-x	एल-डिस्ट्रो	x-x-x	बी
सेवायें	वेब सर्वर	अपाचे		युनिक्स	x-x-x	बी

एक्सेल में फ़िल्टर फ़न्क्शन द्वारा उपयुक्त प्रक्रिया सामग्री चुनना और यह देखना कि कौन-सा संघटक किस प्रकार की प्रक्रिया सामग्री का उपयोग कर रहा है बहुत आसान है ।

8.2. *सतर्कादेश, चेतावनियां और घोषणाएं बनाना*

सतर्कादेश, चेतावनियां और घोषणाओं तीनों का उत्पादन एक ही कार्य-प्रवाह के अनुसार होता है :

- जानकारी-संग्रह करना
- प्रासंगिकता और स्त्रोत के आधार पर जानकारी का मूल्यांकन
- एकत्रित जानकारी के आधार पर जोखिम का मूल्यांकन
- जानकारी का वितरण



चित्र 9. : *जानकारी प्रक्रिया प्रवाह*

निम्नलिखित अनुच्छेदों में यह कार्यप्रवाह और अधिक विस्तारपूर्वक बताया जाएगा ।

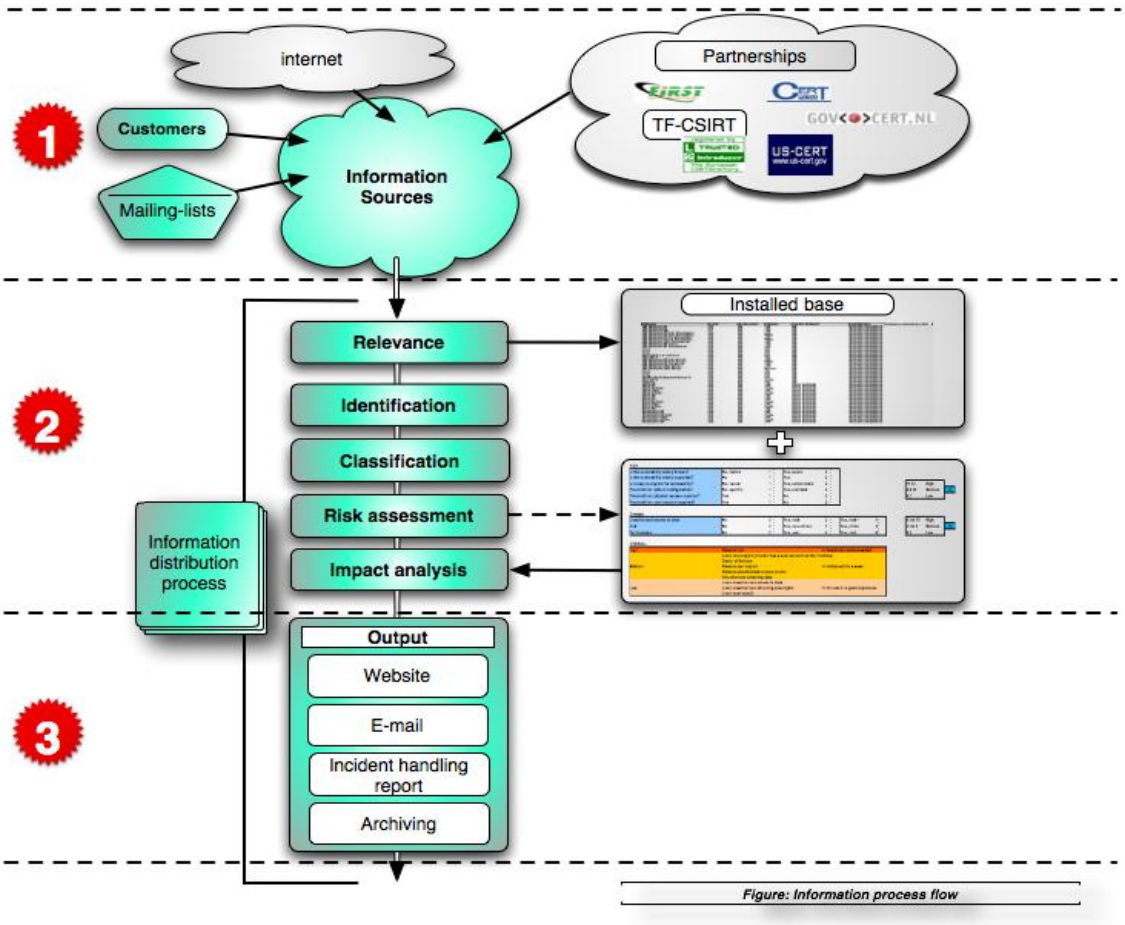


Figure: Information process flow

1 चरण 1 : संवेदनशीलता जानकारी एकत्रित करना ।

आमतौर पर दो मुख्य तरह के जानकारी के स्त्रोत सेवाओं के लिए आगत के तौर पर जानकारी प्रदान करते हैं :

- सूचना प्रौद्योगिकी तंत्रों (आपके) के बारे में संवेदनशीलता जानकारी
- घटना रिपोर्टें

व्यापार और सूचना प्रौद्योगिकी अवसंरचना के प्रकार के आधार पर संवेदनशीलता जानकारी के लिए कई सार्वजनिक व बंद स्त्रोत हैं :

- सार्वजनिक और बंद मेलिंग सूचियां
- विक्रेता संवेदनशीलता उत्पाद जानकारी
- वेबसाइटें

- इंटरनेट पर जानकारी (गूगल, इत्यादी...)
- सार्वजनिक और निजी साझेदारियां जो संवेदनशीलता संबंधी जानकारी प्रदान करतीं हैं (पहला, टी० एफ़०-सी० एस० आई० आर० टी०, सी०ई०आर०टी०-सी०सी०, यू०एस०-सी०ई०आर०टी०...)

यह सारी जानकारी सूचना प्रौद्योगिकी तंत्रों में विशिष्ट संवेदनशीलताओं के बारे में ज्ञान के स्तर को बढ़ाती है ।

जैसा कि पहले बताया गया है इंटरनेट पर बहुत से अच्छे और सुलभ सुरक्षा जानकारी के स्त्रोत उपलब्ध हैं । लिखने के समय एनीसा तदर्थ कार्य-समूह "सी०ई०आर०टी० *सेवायें*" 2006 के लिये एक अधिक व्यापक सूची बना रहा है जिसके 2006[19] के अंत तक पूरी होने की संभावना है ।

2 चरण 2 : जानकारी का मूल्यांकन और जोख़िम निर्धारण

इस चरण के नतीजतन चुनाव-क्षेत्र की सूचना प्रौद्योगिकी अवसंरचना के लिए एक विशिष्ट संवेदनशीलता के प्रभाव का विश्लेषण किया जाएगा ।

पहचान

आगत संवेदनशीलता जानकारी हमेशा अपने स्त्रोत द्वारा पहचानी जाती है और जानकारी को चुनाव-क्षेत्र को देने से पहले यह पता लगाना होगा कि क्या स्त्रोत विश्वसनीय है या नहीं । अन्यथा लोगों को गलत चेतावनियां मिल सकतीं हैं जिसके कारण व्यापार प्रक्रियाओं में बेकार की हलचल हो सकती है और अंत में सी० एस० आई० आर० टी०ओं की प्रतिष्ठा को हानि हो सकती है ।

[19] डब्लयू०जी० सी०ई०आर०टी० तदर्थ सेवायें :
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

निम्नलिखित प्रक्रिया एक संदेश की सच्चाई पहचानने का एक उदाहरण दिखाती है :

एक संदेश और उसके स्त्रोत की सच्चाई का पता लगाने की प्रक्रिया

सामान्य सूची

1. क्या स्त्रोत ज्ञात है और इस रूप में पंजीकृत है ?
2. क्या सूचना नियमित मार्ग से आ रही है ?
3. क्या इसमें कोई "अजीब" जानकारी है जो गलत "लग रही" है ?
4. अपनी भावनाओं का अनुसरण करें, अगर जानकारी के बारे में कोई शक हो तो कार्रवाई न कर एक बार फिर सत्यापित करें !

ई-मेल - स्त्रोत

1. क्या संस्थान और स्त्रोत सूची को स्त्रोत का पता ज्ञात है ?
2. क्या पी०जी०पी०-हस्ताक्षर सही हैं ?
3. जब भी शक हो तो संदेश के पूरे हेडर जाँचें ।
4. शक होने पर भेजने वाले का डोमेन[20] सत्यापित करने के लिए "nslookup" या "dig" का इस्तेमाल करें ।

WWW - स्त्रोत

1. सुरक्षित वेबसाइटों पर लॉग-इन करते समय ब्राउज़र प्रमाणपत्र जाँचें (https ://) ।
2. अंतर्वस्तु और वैधता के लिए स्त्रोत जाँचें (तकनीकी) ।
3. जब भी शक हो तो किसी भी लिंक पर क्लिक न करें और न ही कोई प्रक्रिया सामग्री डाउनलोड करें ।
4. जब भी शक हो तो डोमेन का "lookup" और "dig" करवायें और "traceroute" करें ।

फ़ोन

1. नाम ध्यानपूर्वक सुनें ।
2. क्या आप आवाज़ पहचानते हैं ?
3. शक होने पर फ़ोन नंबर पूछें और फ़ोन करने वाले लो फ़ोन करने का निवेदन करें ।

चित्र 10. *जानकारी पहचान प्रक्रिया का उदाहरण*

प्रासंगिकता

[20] सी०एच०आई०एच०टी० में पहचानों का सत्यापन करने के उपकरण : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

पहले दर्शाये गए लगाए गए यंत्र व प्रक्रिया सामग्री के सिंहावलोकन का उपयोग निम्नलिखित प्रश्नों के उत्तर जानने के लिए आगत संवेदनशीलता जानकारी को प्रासंगिकता के आधार पर छानने के लिए किया जा सकता है : "क्या चुनाव-क्षेत्र इस प्रक्रिया सामग्री का इस्तेमाल करता है ?", "क्या यह जानकारी उनके लिए प्रासंगिक है ?"

वर्गीकरण

कुछ जानकारी वर्गीकृत या सीमित के लेबल के साथ प्राप्त हो सकती है (उदाहरण के लिए अन्य दलों से मिलने वाली घटनाओं की रिपोर्टें) । सारी जानकारी प्रेषक के निवेदन के अनुसार और अपनी सूचना सुरक्षा नीति के अनुसार काम में लाई जानी चाहिए । एक अच्छा मूल नियम है - "अगर यह स्पष्ट न हो कि किसी जानकारी का वितरण करना है तो उसका वितरण न करें ; जब भी शक हो तो प्रेषक से ऐसा करने की अनुमति मांगें ।"

जोखिम-निर्धारण व प्रभाव-विश्लेषण

एक (संभावित) संवेदनशीलता के जोखिम और प्रभाव का निर्धारण करने के कई तरीके हैं ।

जोखिम की परिभाषा है कि एक संवेदनशीलता का लाभ उठाने का संभावित मौका । कई महत्त्वपूर्ण घटक हैं (अन्य में से) :

- क्या संवेदनशीलता के बारे में अच्छी तरह पता है ?
- क्या संवेदनशीलता फैली हुई है ?
- क्या संवेदनशीलता का फ़ायदा उठाना आसान है ?
- क्या इस संवेदनशीलता का फ़ायदा दूर से उठाया जा सकता है ?

यह सभी प्रश्न संवेदनशीलता की गंभीरता को एक अच्छा अर्थ देते हैं ।
निम्नलिखित फ़ॉर्मूला जोखिम की गणना करने का एक सरल तरीका है :

प्रभाव = जोखिम X संभावित क्षति

संभावित क्षति निम्नलिखित में से एक हो सकती है

- आंकड़ों तक अनधिकृत पैठ
- सेवा प्रदान करने से इन्कार (डॉस)
- अनुमतियां प्राप्त करना या आगे अन्य लोगों को प्रदान करना

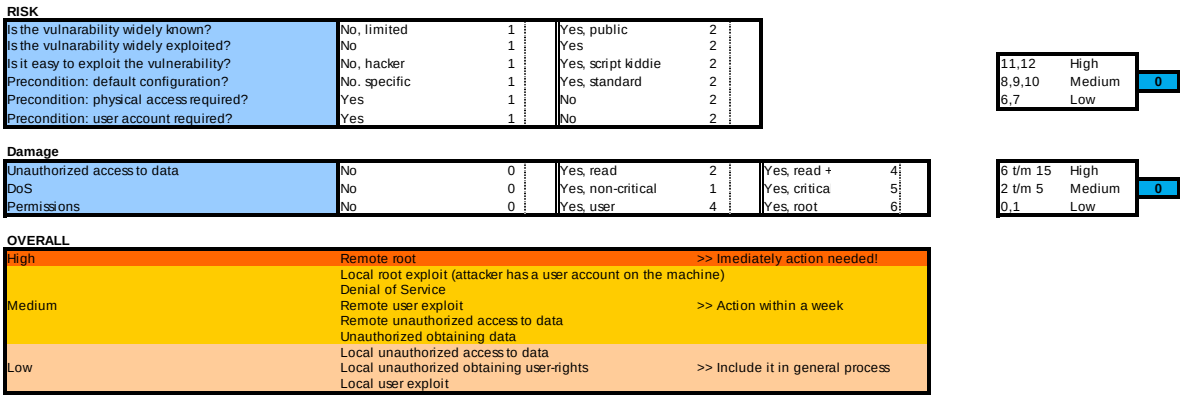
(अधिक विस्तृत वर्गीकरण योजनाओं के लिए कृपया इस पाठ का अंत देखें ।)

इन प्रश्नों का उत्तर देने के साथ संभावित जोखिम और क्षति के बारे में सूचित करते हुए परामर्श-पत्र में एक कुल मूल्यांकन जोड़ा जा सकता है । अक्सर निम्न, मध्यम और उच्च जैसे साधारण शब्दों का उपयोग किया जाता है ।

अन्य अधिक व्यापक जोखिम निर्धारण योजनाएं निम्नलिखित हैं :

GOVCERT.NL मूल्यांकन योजना[21]

डच सरकार के सी० एस० आई० आर० टी० GOVCERT.NL ने जोखिम के मूल्यांकन के लिए एक मैट्रिक्स विकसित की थी जिसे Govcert.nl के शुरूआती चरण में विकसित किया गया था और अब भी हाल के रुझानों के अनुसार जिसका अद्यतन किया जाता है ।



चित्र 11.GOVCERT.NL *मूल्यांकन योजना*

साधारण ई० आई० एस० पी० पी० परामर्श फ़ॉर्मेट विवरण[22]

जानकारी सुरक्षा को बढ़ावा देने का युरोपीय कार्यक्रम (ई० आई० एस० पी० पी०) एक ऐसी परियोजना है जिसे पाँचवे ढांचे के कार्यक्रम के अंतर्गत युरोपीय समुदाय द्वारा मिल कर वित्त प्रदान किया गया । ई० आई० एस० पी० पी० कार्यक्रम का उद्देश्य सुरक्षा-संबंधी ज्ञान के आदान-प्रदान के साथ-साथ छोटे व मध्यम आकार की औद्योगिक इकाइयों को सुरक्षा-संबंधी जानकारी का वितरण करने के लिए विषय-वस्तु व तरीके परिभाषित करने के लिए एक युरोपीय ढांचे को विकसित करना है । छोटे व मध्यम आकार की युरोपीय औद्योगिक इकाइयों को आवश्यक सूचना प्रौद्योगिकी सुरक्षा सेवायें देने से वे भी विश्वास और ई-कॉमर्स के उपयोग को विकसित करने के लिए प्रोत्साहित होंगी जिससे नए व्यापारों के लिए अधिक और बेहतर मौके सामने आएंगे । ई० आई० एस० पी० पी० युरोपीय कमीशन के युरोपीय संघ में दक्षता का युरोपीय संगठन-तंत्र बनाने के नज़रिये में प्रवर्तक है ।

डाफ़ जर्मन परामर्श फ़ॉर्मेट[23]

डाफ़ जर्मन सेर्ट-वेर्बुंद की पहल है और यह विभिन्न दलों द्वारा सुरक्षा परामर्श उत्पन्न करने और उनके आदा–प्रदान के लिए अवसंरचना का एक मूल भाग है । डाफ़ को विशेषकर जर्मन सेर्टों की ज़रूरतों के

[21] संवेदनशीलता मेट्रिक्स : http://www.govcert.nl/download.html?f=33
[22] ई०आई०एस०एस०पी० : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#03
[23] डी०ए०एफ़० : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#02

हिसाब से बनाया गया है ; मानक सेर्ट-बुंद, डी०एफ़०एन०-सेर्ट, प्रीसेक्योर और सीमन्स-सेर्ट द्वारा विकसित व अनुरक्षित किया गया है ।

चरण 3 : जानकारी का वितरण

एक सी० एस० आई० आर० टी० अपने घटकों की इच्छा और अपनी संचार रणनीति के अनुसार वितरण के कई तरीकों में से चुन सकता है ।

- वेबसाइट
- ई-मेल
- रिपोर्टें
- सहेजना व अनुसंधान करना

सुरक्षा परामर्श पत्र एक सी० एस० आई० आर० टी० द्वारा वितरित किये जाते हैं और इनका ढांचा हमेशा एक ही रहना चाहिए । इससे पठनीयता बढ़ेगी और पाठक तुरंत प्रासंगिक जानकारी खोज लेगा ।

एक परामर्श-पत्र में कम से कम निम्नलिखित जानकारी होनी चाहिए :

परामर्श-पत्र का शीर्षक .....
संदर्भ संख्या ..... **प्रभावित तंत्र** - ..... - ..... **संबंधित ओ०एस० व संस्करण** ..... **जोखिम** (उच्च-मध्यम-निम्न) ..... **प्रभाव/ संभावित क्षति** (उच्च-मध्यम-निम्न) ..... **बाह्य पहचानें :** (सी०वी०ई०, संवेदनशीलता बुलेटिन पहचानें) .....
संवेदनशीलता का सिंहावलोकन ..... **प्रभाव** ..... **समाधान** ..... **विवरण (विस्तृत जानकारी)** .....

परिशिष्ट

.....

चित्र 12. *परामर्श योजना का नमूना*

सुरक्षा परामर्श के एक पूर्ण उदाहरण के लिए पाठ *10. अभ्यास* देखें ।

8.3. घटनाओं पर कार्रवाई करना

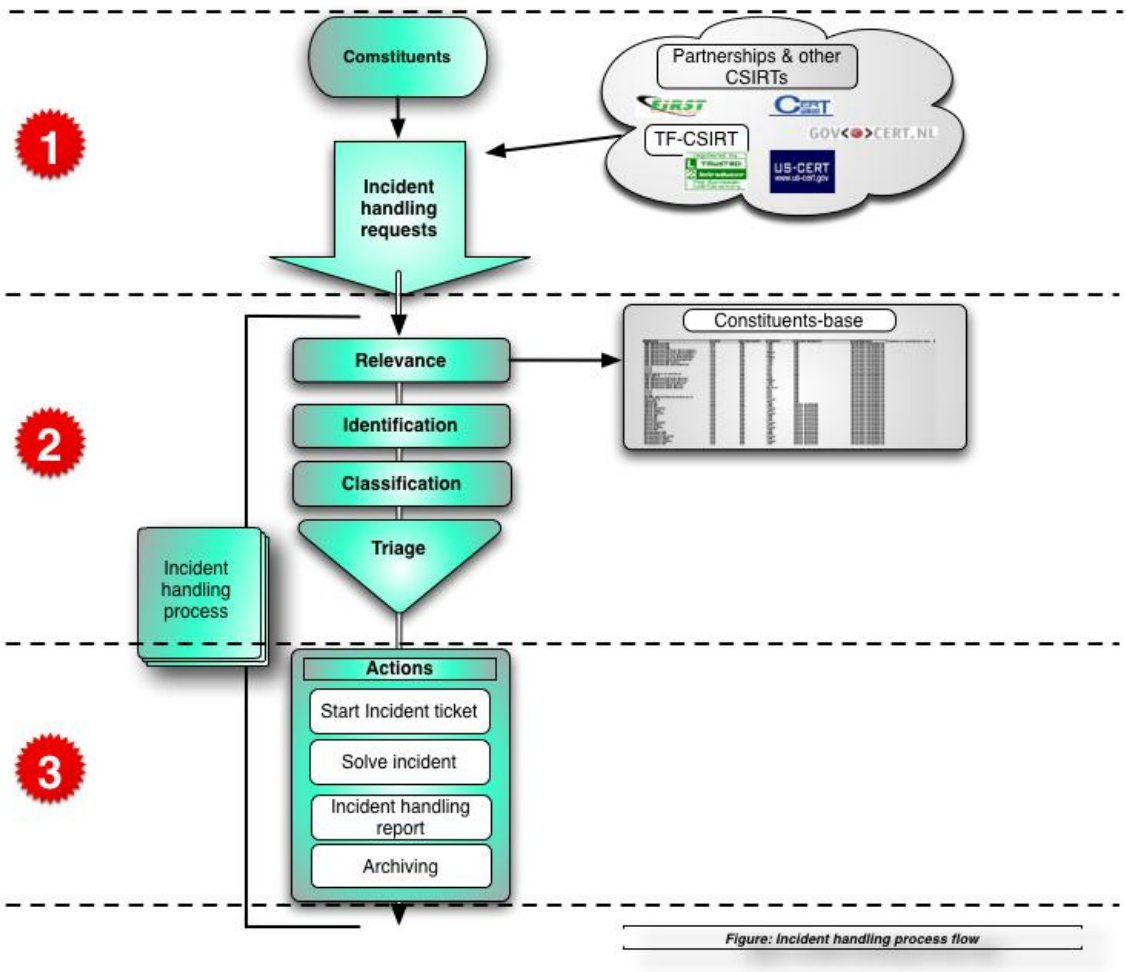
जैसा कि इस पाठ के उपसंहार में बताया गया है, एक घटना पर कार्रवाई करते समय जानकारी पर कार्रवाई करने की प्रक्रिया उस प्रक्रिया से काफ़ी मिलती-जुलती है जिसका उपयोग सतर्कादेश, चेतावनियां और घोषणाएं लिखने के लिए किया जाता है । परंतु जानकारी एकत्रित करने का भाग आमतौर पर अलग होता है क्योंकि घटना से संबंधित आंकड़े प्राप्त करने का साधारण तरीका चुनाव-क्षेत्र या अन्य दलों से घटना की रिपोर्टें प्राप्त करना या फिर घटना से सम्बद्ध पक्षों से प्रतिपुष्टि द्वारा प्राप्त करना है । आमतौर पर जानकारी (कूट-संकेतबद्ध) ई-मेल द्वारा प्रवाहित होती है ; कभी-कभी फ़ोन या फ़ैक्स ज़रूरी होता है ।

फ़ोन द्वारा जानकारी प्राप्त करते समय एक घटना पर कार्रवाई/ की सूचना देने वाले उपकरण या ज्ञापन बना कर प्रत्येक छोटे से छोटा विवरण तुरंत लिख लेना एक अच्छा अभ्यास है । तुरंत (कॉल खत्म होने से पहले) एक घटना संख्या उत्पन्न करना ज़रूरी है (अगर इस घटना के लिए अब तक कोई नहीं है) और फिर आगे के संचार के लिए संदर्भ के तौर पर फ़ोन पर सूचना देने वाले को जारी करना (या बाद में सारांश देती हुई ई-मेल द्वारा भेजना) आवश्यक है ।

इस पाठ के बाकी भाग में घटना पर कार्रवाई करने की मूल प्रक्रिया के बारे में विस्तारपूर्वक बताया गया है । घटना प्रबंधन की पूरी प्रक्रिया और उससे सम्बद्ध सभी कार्य-प्रवाहों और उप-कार्य-प्रवाहों का एक बहुत ही गहन विश्लेषण सी०ई०आर०टी०/सी०सी० दस्तावेज़ों *सी० एस० आई० आर० टी०ओं के लिए घटना प्रबंधन प्रक्रियाओं को परिभाषित करना*[24] में मौजूद है ।

[24] घटना प्रबंधन प्रक्रियाओं को परिभाषित करना : http://www.cert.org/archive/pdf/04tr015.pdf

मूलतः घटना पर कार्रवाई निम्नलिखित कार्य-प्रवाह के अनुसार काम करती है :



चित्र 13. *घटना प्रक्रिया प्रवाह*

चरण 1 : घटना की रिपोर्टें प्राप्त करना

जैसा कि पहले बताया गया है सी० एस० आई० आर० टी० को घटना की रिपोर्टें कई मार्गों, ज़्यादातर ई-मेल परंतु फ़ोन और फ़ैक्स द्वारा भी, पहुँचतीं हैं ।

जैसा कि पहले बताया गया है एक घटना की सूचना प्राप्त करते समय एक निश्चित फ़ॉर्मेट में सभी विवरण लिख लेना एक अच्छा अभ्यास है । ऐसा कर यह सुनिश्चित हो जाता है कि कोई भी महत्त्वपूर्ण जानकारी नहीं छूटी है । निम्नलिखित नमूना योजना देखी जा सकती है :

घटना रिपोर्ट प्रपत्र
कृपया यह प्रपत्र भर कर फ़ैक्स या ई-मेल द्वारा निम्नलिखित को भेजें : …….. ** द्वारा अंकित पंक्तियां अनिवार्य हैं ।* *नाम और संस्थान* 1. नाम* : 2. संस्थान का नाम* : 3. क्षेत्र प्रकार : 4. देश* : 5. शहर : 6. ई-मेल पता* : 7. फ़ोन नंबर* : 8. अन्य : *प्रभावित मेज़बान* 9. मेज़बानों की संख्या : 10. मेज़बान का नाम व आई०पी०* : 11. मेज़बान का कार्य* : 12. समय-क्षेत्र : 13. यंत्रसामग्री : 14. प्रचालन तंत्र : 15. प्रभावित प्रक्रिया सामग्री : 16. प्रभावित फ़ाइलें : 17. सुरक्षा : 18. मेज़बान का नाम व आई०पी०:

19. प्रोटोकॉल / पोर्ट :

घटना

20. संदर्भ संख्या ref # :
21. घटना-प्रकार :
22. घटना शुरू हुई :
23. क्या यह एक चालू घटना है : हाँ नहीं
24. पता लगने का समय और तरीका :
25. ज्ञात संवेदनशीलताएं :
26. संदिग्ध फ़ाइलें :
27. प्रत्युपाय :
28. विस्तृत विवरण* :

चित्र 14. *घटना रिपोर्ट की विषय-वस्तु*

चरण 2 : घटना का मूल्यांकन

इस चरण के दौरान जिस घटना की सूचना मिली है उसकी सच्चाई और प्रासंगिकता की जाँच की जाती है और घटना को वर्गीकृत किया जाता है ।

पहचान

कोई भी बेकार की कार्रवाई करने से बचने के लिए यह जाँचना एक अच्छी आदत है कि सूचना देने वाला विश्वसनीय है और क्या सूचना देने वाला आप में से कोई है या सहयोगी सी० एस० आई० आर० टी० के घटकों में से कोई है । जैसे नियमों के बारे में पाठ *8.2 सतर्कादेश उत्पन्न करना* में विस्तारपूर्वक बताया गया है वैसे ही नियम लागू होते हैं ।

प्रासंगिकता

इस चरण के साथ आप यह जाँचते हैं कि क्या घटना पर कार्रवाई करने का निवेदन सी० एस० आई० आर० टी०ओं के चुनाव-क्षेत्र से प्राप्त हुआ है और क्या घटना चुनाव-क्षेत्र के सूचना प्रौद्योगिकी तंत्रों से संबंधित है । अगर उपरोक्त में से कोई भी लागू नहीं होता तो आमतौर पर रिपोर्ट पुनः ठीक सी०आई०एस०आर०टी०[25] को भेजी जाती है ।

वर्गीकरण

इस चरण के साथ घटना की गंभीरता का वर्गीकरण कर छंटाई तैयार होती है । घटना के वर्गीकरण के बारे में अधिक चर्चा करना इस दस्तावेज़ के परास से बाहर है । सी० एस० आई० आर० टी० मामला वर्गीकरण योजना का उपयोग करना एक अच्छी शुरूआत है (कंपनी सी० एस० आई० आर० टी० के लिए उदाहरण) :

[25] सी०एच०आई०एच०टी० में पहचानों का सत्यापन करने के उपकरण :
http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

चित्र 15. *घटना वर्गीकरण योजना* (*स्त्रोत* : *पहला*)[26]

छंटाई

छंटाई वह तंत्र है जिसका उपयोग चैकित्सिक या आपातकालीन कर्मचारी सीमित चैकित्सिक संसाधनों के वितरण के लिए तब करते हैं जब जिन घायलों को देखभाल की ज़रूरत है उनकी संख्या देखभाल करने के लिए उपलब्ध संसाधनों से अधिक होती है ताकि अधिकतम मरीज़ों का इलाज किया जा सके[27] ।

सी०ई०आर०टी०/ सी०सी० निम्नलिखित विवरण देती है :

छंटनी किसी भी घटना के प्रबंधन क्षमता, विशेषकर किसी स्थापित सी० एस० आई० आर० टी०, के लिए महत्त्वपूर्ण घटक है । छटनी उस महत्त्वपूर्ण पथ का भाग है जिससे यह समझा जा सकता है कि संस्थान-भर में किस बात की सूचना दी जा रही है । यह उस वाहन के तौर पर काम करती है जिसके द्वारा सारी जानकारी एक एकमात्र संपर्क-स्थल में जाती है जिससे कंपनी को चालू गतिविधि और जिन आंकड़ों की सूचना दी गई है उन सब के व्यापक पारस्परिक संबंध का पता लगता है । छंटनी से एक प्राप्त सूचना का शुरूआती निर्धारण होता है और यह आगे कार्रवाई के लिए पंक्तिबद्ध हो जाती है । यह एक रिपोर्ट या निवेदन की शुरूआती दस्तावेज़ीकरण और डाटा एंट्री, अगर पता लगाने की प्रक्रिया के दौरान ऐसा पहले नहीं किया गया है, के लिए भी स्थान प्रदान करती है ।

[26] सी०एस०आई०आर०टी० मामला वर्गीकरण http://www.first.org/resources/guides/csirt_case_classification.html

[27] विकिपीडिया में छंटाई : http://en.wikipedia.org/wiki/Triage

छंटनी का कार्य उस सारी जानकारी की वर्तमान स्थिति का तुरंत चित्र दर्शाता है जिसके बारे में सूचना दी गई है - कौन-सी रिपोर्टों को खोला या बंद किया गया, कौन-से कार्य बाकी हैं और प्रत्येक प्रकार की कितनी रिपोर्टें मिलीं । इस प्रक्रिया से संभावित सुरक्षा समस्याओं का पता लगाने और कार्यभार को प्राथमिकता के आधार पर पंक्तिबद्ध करने में मदद मिल सकती है । छंटनी के दौरान एकत्रित जानकारी का उपयोग ऊपरी प्रबंधन के लिए संवेदनशीलता और घटना रुझान और आंकड़े बनाने के लिए भी किया जा सकता है[28] *।*

छंटनी केवल दल के सर्वाधिक अनुभवी सदस्यों द्वारा ही की जानी चाहिए क्योंकि इसके लिए चुनाव-क्षेत्र के विशिष्ट भागों पर घटनाओं के प्रभाव की अच्छी समझ और यह निर्णय लेने की क्षमता की ज़रूरत होती है कि उस घटना पर कार्रवाई करने के लिए दल का कौन-सा सदस्य उपयुक्त होगा ।

[28] घटना प्रबंधन प्रक्रियाओं को परिभाषित करना : http://www.cert.org/archive/pdf/04tr015.pdf

चरण 3 : कार्य

आमतौर पर जिन घटनाओं की छंटनी की गई है वे एक घटना पर कार्रवाई करने के उस उपकरण में एक निवेदन पंक्ति में जाते हैं जिसका एक या एक से ज़्यादा घटना पर कार्रवाई करने वाले कर्मचारी उपयोग करते हैं और जो मूलतः निम्नलिखित चरणों पर चलते हैं ।

घटना की शुरूआत की टिकट

हो सकता है कि घटना की टिकट संख्या पहले ही पिछले चरण में जारी कर दी गई हो (उदाहरण के लिए जब फ़ोन द्वारा घटना की सूचना दी गई थी) । अगर ऐसा नहीं किया गया तो पहला चरण ऐसी संख्या बनाना है जिसका उपयोग भविष्य में इस घटना के बारे में किए जाने वाले आदान-प्रदान में किया जाएगा ।

घटना का जीवनचक्र

एक घटना पर कार्रवाई करना उन चरणों पर नहीं चलता जो अंत में समाधान की ओर ले जाते हैं अपितु यह चरणों के एक चक्र पर चलता है जो तब तक बारंबार किये जाते हैं जब तक कि घटना को अंत में सुलझा नहीं लिया जाता और सभी संबंधित पक्षों के पास पूरी आवश्यक जानकारी न हो । इस चक्र, जिसे अक्सर "घटना का जीवनचक्र" के नाम से भी जाना जाता है, में निम्नलिखित प्रक्रियाएं होतीं हैं :

विश्लेषण :	जिस घटना की सूचना दी गई है उससे संबद्ध सभी विवरणों का विश्लेषण किया जाता है ।
संपर्क जानकारी प्राप्त करना :	सभी संबंधित पक्षों जैसे अन्य सी० एस० आई० आर० टी०ओं, शिकारों और शायद उन तंत्रों के मालिकों आक्रमण के लिए जिनका दुरुपयोग किया गया है, को आगे घटना से संबंधित जानकारी पहुँचा पाना ।
तकनीकी मदद प्रदान करना :	घटना के नतीजों से शीघ्र उबरने में शिकारों की मदद करना और आक्रमण के बारे में अधिक जानकारी एकत्रित करना ।
समन्वयन :	आक्रमण के लिए जिस सूचना प्रौद्योगिकी तंत्र का प्रयोग किया गया है उसकी सी० एस० आई० आर० टी० और अन्य शिकारों जैसे सभी संबंधित पक्षों को सूचित करना ।

इस ढांचे को "जीवनचक्र" कहते हैं क्योंकि इसका एक चरण अगले की ओर ले जाता है और अंतिम चरण, समन्वयन-भाग, फिर नए विश्लेषण की ओर ले जा सकता है और चक्र पुनः चालू हो जाता है । जब सभी संबंधित पक्ष पूरी आवश्यक जानकारी प्राप्त कर लेते हैं और इसकी सूचना दे देते हैं तब इस प्रक्रिया का अंत होता है ।

जीवन-चक्र के अधिक विस्तृत विवरण के लिए कृपया सी० ई० आर० टी०/ सी० सी० सी० एस० आई० आर० टी० निर्देश-पुस्तिका देखें[29] ।

घटनाओं पर कार्रवाई की रिपोर्ट

एक रिपोर्ट तैयार कर प्रबंधन द्वारा घटनाओं के बारे में पूछे जाने वाले प्रश्नों के लिए तैयार रहें । कर्मचारियों को प्रशिक्षित करने और भविष्य में घटना पर कार्रवाई करने की प्रक्रिया में गल्तियों से बचने के लिए "सीखी गई सीखों" के बारे में एक दस्तावेज़ लिखना एक अच्छा अभ्यास है ।

सहेजना

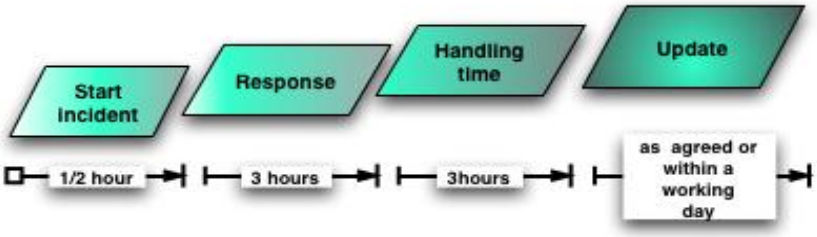
पहले पाठ *6.6 एक सूचना सुरक्षा नीति विकसित करना* में पहले सहेजने के लिए जिन नियमों के बारे में विस्तारपूर्वक बताया गया है उन्हें देखें ।

घटना प्रबंधन और घटना जीवन-चक्र के बारे में व्यापक निर्देशों के लिए कृपया परिशिष्ट खंड *क.1 अतिरिक्त पठन-सामग्री देखें ।*

8.4. एक प्रत्युत्तर समयसारणी का उदाहरण

प्रत्युत्तर अवधियों की परिभाषा को अक्सर नज़रंदाज़ किया जाता है परंतु इसे सी० एस० आई० आर० टी० और इसके चुनाव-क्षेत्र के बीच होने वाले हर सही ढंग से बनाए गए सेवा स्तर के अनुबंध (एस० एल० ए०) का भाग होना चाहिए । घटना पर कार्रवाई करते समय घटकों को समय पर प्रतिपुष्टि देना घटकों की अपनी देयताओं और दल की ख्याति दोनों के लिए महत्त्वपूर्ण है ।
गलत अपेक्षाओं से बचने के लिए चुनाव क्षेत्र को प्रत्युत्तर समय स्पष्ट तौर पर बताया जाना चाहिए । निम्नलिखित बहुत ही मूल समयसारणी का उपयोग सी० एस० आई० आर० टी० के चुनाव-क्षेत्र के साथ एक अधिक विस्तृत एस० एल० ए० के शुरूआत बिंदु के तौर पर किया जा सकता है ।

मदद के लिए एक आगत निवेदन के स्थान से एक व्यावहारिक प्रत्युत्तर समयसारणी का एक उदाहरण नीचे दिया गया है :



चित्र 16. *प्रत्युत्तर समयसारणी का उदाहरण*

[29] सी०एस०आई०आर०टी० पुस्तिका: http://www.cert.org/archive/pdf/csirt-handbook.pdf

चुनाव-क्षेत्र को उनके अपने प्रत्युत्तर समय, ख़ासकर आपातकालीन स्थिति में सी० एस० आई० आर० टी० से कब संपर्क करना है, के बारे में निर्देश देना भी एक अच्छा अभ्यास है । अधिकतर मामलों में शुरूआती चरण पर उनकी सी० एस० आई० आर० टी० से संपर्क करना बेहतर है और शक होने पर चुनाव-क्षेत्र को ऐसा करने के लिए प्रोत्साहित करना एक अच्छा अभ्यास है ।

8.5. *उपलब्ध सी० एस० आई० आर० टी० उपकरण*

यह पाठ सी० एस० आई० आर० टी० द्वारा काम में लाए जाने वाले कुछ आम उपकरणों के बारे में जानकारी देता है । यह केवल उदाहरण देता है, अधिक जानकारी *घटना पर कार्रवाई करने के उपकरणों का शोधन-गृह*[30] *(सी० एच० आई० एच० टी०)* में देखी जा सकती है ।

ई-मेल और संदेश एन्क्रिप्शन प्रक्रिया सामग्री

- जी० एन० यू० पी० जी० http://www.gnupg.org/
  जी०एन०यू०पी०जी० जी०एन०यू० परियोजना के अंतर्गत आर०एफ़०सी०2440 द्वारा दी गई परिभाषा के अनुसार ओपन पी०जी०पी० मानक का पूर्ण और मुफ़्त कार्यान्वयन है । जी०एन०यू०पी०जी की मदद से आप अपने आंकड़े और संचार कूट-संकेतबद्ध (एन्क्रिप्ट) कर और उन पर हस्ताक्षर कर सकते हैं ।

- पी०जी०पी० http://www.pgp.com/
  व्यापारिक रूपांतर

घटनाओं पर कार्रवाई करने वाला उपकरण

घटनाओं और उनके अनुवर्तन को प्रशासित करें, कार्रवाइयों पर नज़र रखें ।

- आर०टी०आई०आर० http://www.bestpractical.com/rtir/
  आर०टी०आई०आर० मुफ़्त मुक्त-स्त्रोत घटना पर कार्रवाई करने वाला तंत्र है जिसे सी०ई०आर०टी० और घटना पर कार्रवाई करने वाले अन्य दलों की ज़रूरतों को ध्यान में रखते हुए बनाया गया है ।

ग्राहक संसाधन प्रबंधन (सी० आर० एम०) उपकरण

जब आपके कई अलग-अलग संघटक हों और आपको सभी नियुक्तियों व विवरणों पर नज़र रखने की ज़रूरत हो तो एक सी०आर०एम० आंकड़ा संचय उपयोगी सिद्ध होता है । कई अलग-अलग भिन्नताएं हैं जिनके उदाहरण नीचे दिये गए हैं :

- शूगर सी०आर०एम० http://www.sugarcrm.com/crm/

- शूगरफ़ोर्स (मुफ़्त मुक्त-स्त्रोत संस्करण) http://www.sugarforge.org/

सूचना की जाँच करना

- वेबसाइट वॉचर (वेबसाइट पर नज़र रखने वाला) http://www.aignes.com/index.htm
  यह अनुप्रयोग अद्यतनों और बदलावों के लिए वेबसाइटों पर नज़र रखता है ।

[30] सी०एच०आई०एच०टी० : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

- वॉच दैट पेज (वह पृष्ठ देखें)
  http://www.watchthatpage.com/
  यह सेवा वेबसाइट में किये गए बदलावों के बारे में जानकारी ई-मेल द्वारा भेजती है (मुफ़्त और व्यापारिक) ।

संपर्क जानकारी का पता लगाना

घटनाओं की सूचना देने के लिए सही संपर्कों का पता लगाना कोई आसान काम नहीं है । जानकारी के कुछ स्त्रोतों का उपयोग किया जा सकता है :

- राइप[31]
- आई०आर०टी०-ऑबजेक्ट[32]
- टी०आई०[33]

इसके अतिरिक्त सी०एच०आई०एच०टी० के पास संपर्क जानकारी ढूंढने वाले कुछ उपकरणों की भी सूची है[34] ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 8)

प्रक्रिया प्रवाह और प्रचालक व तकनीकी कार्य-प्रणालिया स्थापित करना

काल्पनिक सी० एस० आई० आर० टी० मूल सी० एस० आई० आर० टी० सेवायें देने पर अपना ध्यान केंद्रित करता है ।

- सतर्कादेश और चेतावनियां
- घोषणाएं
- घटनाओं पर कार्रवाई

दल ने वे कार्य-प्रणालियां विकसित कीं हैं जो सही ढंग से काम करती है और जिसे दल का हर सदस्य आसानी से समझ सकता है । काल्पनिक सी० एस० आई० आर० टी० ने देयताओं और सूचना सुरक्षा नीति पर कार्रवाई करने के लिए एक कानूनी विशेषज्ञ को भी नौकरी पर रखा । दल ने कुछ महत्त्वपूर्ण उपकरण अपनाये और अन्य सी० एस० आई० आर० टी०ओं से चर्चा कर प्रचालन संबंधी मुद्दों के बारे में उपयोगी जानकारी प्राप्त की ।

[31] राइप हूइज़ : http://www.ripe.net/whois
[32] राइप आंकड़ा-संचय में आई०आर०टी०-वस्तु :
http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_01.htm#08
[33] विश्वस्त प्रस्तुतकर्ता : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_01_03.htm#07
[34] सी०एच०आई०एच०टी० में पहचानों के सत्यापन हेतु उपकरण :
http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm#04

सुरक्षा परामर्शों और घटनाओं की रिपोर्टों के लिए एक निश्चित टेम्प्लेट भी तैयार किया गया । घटना पर कार्रवाई करने के लिए दल आर०टी०आई०आर० का उपयोग करता है ।

9. सी० एस० आई० आर० टी० प्रशिक्षण

हमने अब तक निम्नलिखित कदम उठायें हैं:

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।
4. वातावरण और घटकों का विश्लेषण ।
5. उद्देश्य कथन परिभाषित करना ।
6. व्यापार योजना का विकास करना ।
   क. वित्तीय नमूना परिभाषित करना ।
   ख. संस्थानात्मक ढांचा परिभाषित करना ।
   ग. कर्मचारियों को नौकरी पर रखना शुरू करना ।
   घ. दफ़्तर का उपयोग करना और दफ़्तर को सुस्सजित करना
   च. जानकारी सुरक्षा नीति विकसित करना ।
   छ. सहयोग के लिए साझेदारों को खोजना ।
7. व्यापार योजना को बढ़ावा देना ।
   क. व्यापार मामले को स्वीकृत करवाना ।
   ख. सब कुछ परियोजना योजना में पूरी तरह लगाना ।
8. सी० एस० आई० आर० टी० को चालू करना ।
   क. कार्य-प्रवाह बनाना
   ख. सी० एस० आई० आर० टी० उपकरणों को कार्यान्वित करना ।

>> अगला कदम है : कर्मचारियों को प्रशिक्षित करना ।

इस पाठ में समर्पित सी० एस० आई० आर० टी० प्रशिक्षण के लिए दो मुख्य स्त्रोतों की सूची दी गई है : ट्रान्सिट्स और सी०ई०आर०टी०/सी०सी० पाठ्यक्रम ।

9.1. ट्रान्सिट्स

ट्रान्सिट्स कंप्यूटर सुरक्षा घटना प्रत्युत्तर दलों (सी० एस० आई० आर० टी०) की स्थापना को बढ़ावा देने और कुशल सी० एस० आई० आर० टी० कर्मचारियों की कमी की समस्या पर काम कर मौजूदा सी० एस० आई० आर० टी०ओं को बेहतर बनाने की युरोपीय परियोजना रही है । (नए) सी० एस० आई० आर० टी०ओं के कर्मचारियों को सी० एस० आई० आर० टी० सेवायें प्रदान करने से जुड़े संगठनात्मक, प्रचालक, तकनीकी, बाज़ार और कानूनी मुद्दों के लिए प्रशिक्षित करने के लिए विशेषज्ञ प्रशिक्षण पाठ्यक्रम प्रदान कर इस लक्ष्य की दिशा में काम किया गया है ।

विशेषकर, ट्रान्सिट ने

- मोड्यूलॅर प्रशिक्षण पाठ्यक्रम सामग्री विकसित, अद्यतित और नियमित तौर पर परिशोधित की है
- जहाँ पाठ्यक्रम सामग्री भेजी गई वहाँ प्रशिक्षण कार्यशालाएं आयोजित कीं ।
- युरोपीय संघ के सदस्य राष्ट्रों की भागीदारी पर विशेष ज़ोर देते हुए इन प्रशिक्षण कार्यशालाओं में (नए) सी० एस० आई० आर० टी०ओं के कर्मचारियों की भागीदारी को संभव बनाया ।
- प्रशिक्षण पाठ्यक्रम सामग्री वितरित की और नतीजों का प्रयोग सुनिश्चित किया[35] ।

एनीसा ट्रान्सिट पाठ्यक्रमों को संभव बनाती है और उनके साथ सहयोग करती है । अगर आप पाठ्यक्रमों के लिए आवेदन कैसे करें, उनकी ज़रूरते और कीमत जानना चाहते हैं तो कृपया एनीसा के सी० एस० आई० आर० टी० विशेषज्ञों से संपर्क करें :

cert-relation@enisa.europa.eu

कृपया इस दस्तावेज़ के परिशिष्ट में दी गई नमूना पाठ्यक्रम सामग्री देखें !

9.2. सी०ई०आर०टी०/ सी०सी०

कंप्यूटर और नेटवर्क अवसंरचनाओं की जटिलता और प्रशासन की चुनौती नेटवर्क सुरक्षा के सही तरह से प्रशासन को कठिन बनाते हैं । नेटवर्क और तंत्र प्रशासकों के पास आक्रमणों से रक्षा करने के लिए और नुक्सान को कम से कम करने के लिए काफ़ी लोग और सुरक्षा अभ्यास लागू नहीं होते । नतीजतन कंप्यूटर सुरक्षा घटनाओं की संख्या बढ़ती जा रही है ।
जब कंप्यूटर सुरक्षा घटनाएं होती हैं तब संस्थानों को शीघ्र और कारगर ढंग से कार्रवाई करनी चाहिए । जितनी तेज़ी से एक संस्थान एक घटना को पहचानता, उसका विश्लेषण करता और प्रत्युत्तर देता है उतनी ही अच्छी तरह से वह नुक्सान को सीमित एवं संभलने की लागत को कम कर सकता है । एक कंप्यूटर सुरक्षा घटना प्रत्युत्तर दल (सी० एस० आई० आर० टी०) स्थापित करना तेज़ी से प्रत्युत्तर देने की यह क्षमता प्रदान करने और साथ ही भविष्य में घटनाओं को होने से रोकने का एक उत्तम तरीका है ।

सी०ई०आर०टी०-सी०सी० प्रबंधकों व तकनीकी कर्मचारियों के लिए कंप्यूटर सुरक्षा घटना प्रत्युत्तर दल (सी० एस० आई० आर० टी०) बनाने और उनका प्रबंधन करने, सुरक्षा घटनाओं का प्रत्युत्तर देने व विश्लेषण करने एवं नेटवर्क सुरक्षा बेहतर बनाने जैसे क्षेत्रों में पाठ्यक्रम प्रदान करता है । अगर अन्यथा नहीं लिखा गया तो सभी पाठ्यक्रम पिट्सबर्ग, पी०ए० में आयोजित किये जाते हैं । हमारे कर्मचारी कार्नेजी मेल्लॅन विश्वविद्यालय में भी सुरक्षा पर पाठ्यक्रम पढ़ाते हैं ।

सी० एस० आई० आर० टी० को समर्पित उपलब्ध सी०ई०आर०टी०/ सी०सी० पाठ्यक्रम[36]

[35] ट्रान्ज़िट्स : http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02_02.htm#11

एक कंप्यूटर सुरक्षा प्रत्युत्तर दल (सी०एस०आई०आर०टी०) बनाना
कंप्यूटर सुरक्षा-संबंधी घटना प्रत्युत्तर दलों (सी०एस०आई०आर०टी०) का प्रबंधन
घटना पर कार्रवाई करने संबंधी मूल सिद्धांत
तकनीकी कर्मचारियों के लिए घटना पर कार्रवाई करने के बारे में उच्च श्रेणी की जानकारी

कृपया इस दस्तावेज़ के परिशिष्ट में दी गई नमूना पाठ्यक्रम सामग्री देखें!

काल्पनिक सी० एस० आई० आर० टी० (चरण 9)
कर्मचारियों को प्रशिक्षित करना । काल्पनिक सी० एस० आई० आर० टी० अपने सभी कर्मचारियों को अगले उपलब्ध ट्रान्सिट पाठ्यक्रमों में भेजने का निर्णय लेता है । इसके साथ-साथ दल का नेता सी०ई०आर०टी०/सी०सी० द्वारा आयोजित *एक सी० एस० आई० आर० टी० का प्रबंधन करना में भी भाग लेता है ।*

[36] सी०ई०आर०टी०/सी०सी० पाठ्यक्रम : http://www.sei.cmu.edu/products/courses

10. अभ्यास : एक परामर्श विज्ञप्ति बनाना

हमने अब तक निम्नलिखित कदम उठायें हैं:

1. यह समझना कि सी० एस० आई० आर० टी० क्या है और यह इसके क्या लाभ हो सकते हैं ।
2. एक नया दल अपनी सेवायें किस क्षेत्र को प्रदान करेगा ?
3. एक सी० एस० आई० आर० टी० अपने चुनाव-क्षेत्र को किस तरह की सेवायें प्रदान कर सकता है ।
4. वातावरण और संघटकों का विश्लेषण ।
5. उद्देश्य कथन परिभाषित करना ।
6. व्यापार योजना का विकास करना ।
   क. वित्तीय नमूना परिभाषित करना ।
   ख. संस्थानात्मक ढांचा परिभाषित करना ।
   ग. कर्मचारियों को नौकरी पर रखना शुरू करना ।
   घ. दफ़्तर का उपयोग करना और दफ़्तर को सुस्सजित करना
   च. जानकारी सुरक्षा नीति विकसित करना ।
   छ. सहयोग के लिए साझेदारों को खोजना ।
7. व्यापार योजना को बढ़ावा देना ।
   क. व्यापार मामले को स्वीकृत करवाना ।
   ख. सब कुछ परियोजना योजना में पूरी तरह लगाना ।
8. सी० एस० आई० आर० टी० को चालू करना ।
   क. कार्य-प्रवाह बनाना
   ख. सी० एस० आई० आर० टी० उपकरणों को कार्यान्वित करना
9. अपने कर्मचारियों को प्रशिक्षित करना ।

>> अगला कदम है अभ्यास करना और असली काम के लिए तैयार रहना !

समझाने के लिए यह पाठ एक दैनिक सी० एस० आई० आर० टी० कार्य के नमूने के तौर पर किये गए अभ्यास के बारे में विस्तारपूर्वक बताता है : एक सुरक्षा परामर्श तैयार करना ।

माइक्रोसॉफ़्ट द्वारा भेजी गई निम्नलिखित असली सुरक्षा सलाह इसकी लिबलिबी (ट्रिगर) थी ।

विज्ञप्ति पहचानकर्ता	**माइक्रोसॉफ़्ट सुरक्षा विज्ञप्ति MS06-042**
विज्ञप्ति का शीर्षक	**इंटरनेट एक्स्प्लोरर के लिए एकीकृत सुरक्षा अद्यतन (918899)**
कार्यकारी सारांश	यह अद्यतन इंटरनेट एक्सप्लोरर में मौजूद ऐसी कई संवेदनशीलताओं का समाधान करता है जो दूर से कोड को कार्यान्वित करने दे सकतीं थीं ।
अधिकतम गंभीरता मूल्यांकन	गंभीर
संवेदनशीलता का प्रभाव	दूर से कोड का कार्यान्वयन
प्रभावित प्रक्रिया सामग्री	**विंडोज़, इंटरनेट एक्सप्लोरर ।** अधिक जानकारी के लिए प्रभावित प्रक्रिया सामग्री और डाउनलोड स्थल खंड देखें ।

यह विक्रेता विज्ञप्ति इंटरनेट एक्सप्लोरर में हाल ही में पाई गई एक संवेदनशीलता पर कार्रवाई करती है । विक्रेता माइक्रोसॉफ़्ट विंडोज़ के कई संस्करणों के लिए इस के कई तोड़ प्रकाशित करता है ।

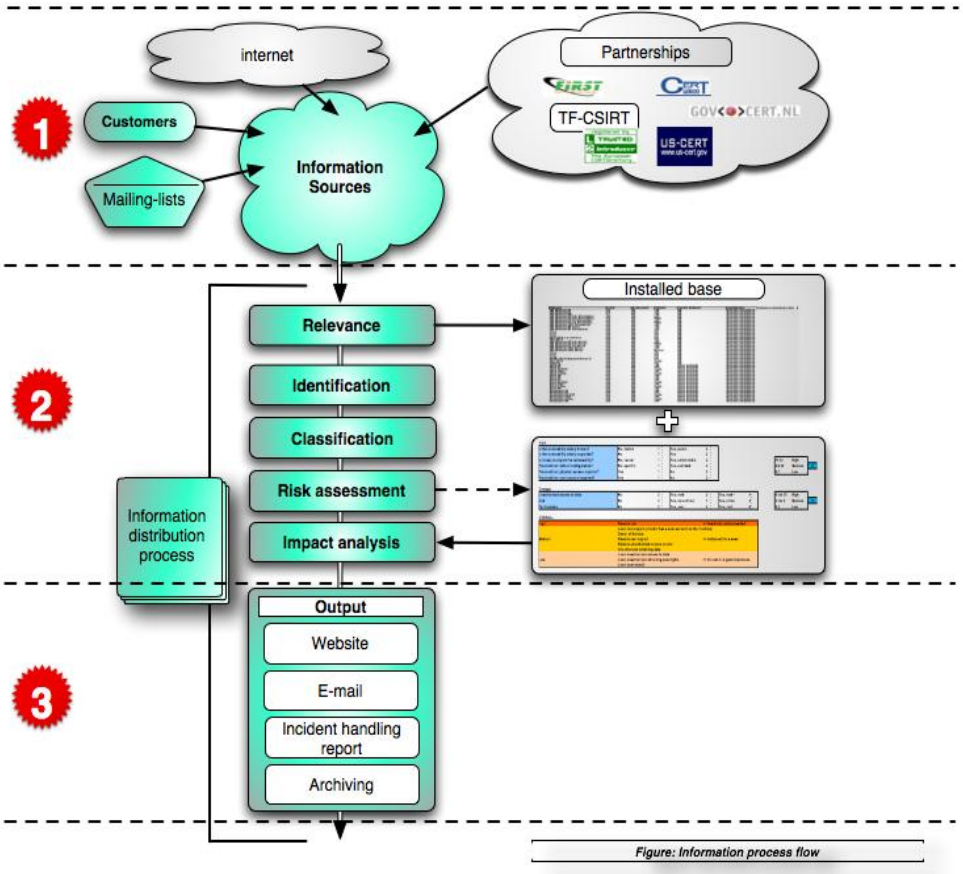


Figure: Information process flow

मेलिंग-सूची द्वारा यह संवेदनशीलता जानकारी प्राप्त करने के बाद काल्पनिक सी० एस० आई० आर० टी० पाठ *8.2*

सतर्कादेश, चेतावनियां और घोषणाएं बनाना में जिस कार्यप्रवाह के बारे में विस्तारपूर्वक बताया गया है उसके साथ काम शुरू करता है ।

चरण 1 : संवेदनशीलता जानकारी एकत्रित करना ।

पहला चरण विक्रेता की वेबसाइट देखना है । काल्पनिक सी० एस० आई० आर० टी० जानकारी का सत्यापन करता है और संवेदनशीलता व प्रभावित सूचना प्रौद्योगिकी तंत्रों के बारे में अधिक जानकारी एकत्रित करता है ।

चरण 2 : जानकारी का मूल्यांकन और जोख़िम निर्धारण

पहचान

ई-मेल द्वारा प्राप्त संवेदनशीलता संबंधी जानकारी को विक्रेता की वेबसाइट पर दिये गए पाठ्य के साथ मिला कर जानकारी पहले से सत्यापित कर ली गई है ।

प्रासंगिकता

काल्पनिक सी० एस० आई० आर० टी० वेबसाइट पर पाये गए प्रभावित तंत्रों की सूची को चुनाव-क्षेत्र में प्रयुक्त तंत्रों की सूची के साथ जाँचता है । यह पता लगाता है कि उनका कम से कम एक संघटक इंटरनेट एक्सप्लोरर का उपयोग कर रहा है इसलिए यह संवेदनशीलता जानकारी असल में प्रासंगिक है ।

श्रेणी	अनुप्रयोग	प्रक्रिया सामग्री उत्पाद	संस्करण	ओ०एस०	ओ०एस० संस्करण	संघटक
डेस्कटॉप	ब्राउज़र	आई० ई०	x-x-	माइक्रोसॉफ़्ट	एक्स०पी०-प्रोफ़०	ए

वर्गीकरण

यह जानकारी सार्वजनिक है इसलिए इसका उपयोग और पुनः वितरण किया जा सकता है ।

जोखिम-निर्धारण व प्रभाव-विश्लेषण

प्रश्नों का उत्तर देने से यह पता लगता है कि जोखिम और प्रभाव *उच्च* हैं (माइक्रोसॉफ़्ट द्वारा *गंभीर* मूल्यांकित किये गए) ।

जोखिम

क्या संवेदनशीलता के बारे में अच्छी तरह पता है ?	हाँ
क्या संवेदनशीलता बहुत ज़्यादा फैली हुई है ?	हाँ
क्या संवेदनशीलता का फ़ायदा उठाना आसान है ?	हाँ
क्या इस संवेदनशीलता का फ़ायदा दूर से उठाया जा सकता है ?	हाँ

क्षति

संभावित प्रभाव दूर से पैठ कर पाना और दूरी से कोड का संभावित प्रचालन हैं । इस संवेदनशीलता में कई मुद्दे हैं जो क्षति के जोखिम को *उच्च* बनाते हैं ।

चरण 3 : वितरण

काल्पनिक सी० एस० आई० आर० टी० एक आंतरिक सी० एस० आई० आर० टी० है । संचार के मार्गों के रूप में इसके पास ई-मेल, फ़ोन और आंतरिक वेबसाइट उपलब्ध हैं । *पाठ 8.2 सतर्कादेश, चेतावनियां और घोषणाएं उत्पन्न करना* में दिये गए टेम्पलेट से प्राप्त कर सी०एस०आई०आर०टी० यह विज्ञप्ति बनाता है ।

परामर्श का शीर्षक
इंटरनेट एक्सप्लोरर में कई संवेदनशीलताएं पाई गईं ।

संदर्भ संख्या
082006-1
प्रभावित तंत्र

- माइक्रोसॉफ़्ट का उपयोग करने वाले सभी डेस्कटॉप तंत्र ।

संबंधित ओ०एस० व संस्करण

- माइक्रोसॉफ़्ट विंडोज़ 2000 सर्विस पैक 4
- माइक्रोसॉफ़्ट विंडोज़ एक्स पी सर्विस पैक 1 और माइक्रोसॉफ़्ट विंडोज़ एक्स पी सर्विस पैक 2
- माइक्रोसॉफ़्ट विंडोज़ एक्स पी प्रोफ़ेशनल x64 संस्करण
- माइक्रोसॉफ़्ट विंडोज़ सर्वर 2003 और माइक्रोसॉफ़्ट विंडोज़ सर्वर 2003 सर्विस पैक 1
- आईटेनियम पर आधारित तंत्रों के लिए माइक्रोसॉफ़्ट विंडोज़ सर्वर 2003 और आईटेनियम पर आधारित तंत्रों के लिए एसपी1 के साथ माइक्रोसॉफ़्ट विंडोज़ सर्वर 2003
- माइक्रोसॉफ़्ट विंडोज़ सर्वर 2003 x64 संस्करण

जोखिम (उच्च-मध्यम-निम्न)
उच्च
प्रभाव /संभावित क्षति (उच्च-मध्यम-निम्न)
उच्च
बाह्य पहचानें : (सी०वी०ई०, संवेदनशीलता बुलेटिन पहचानें)
एम एस -06-42

संवेदनशीलता का सिंहावलोकन
माइक्रोसॉफ़्ट ने इंटरनेट एक्सप्लोरर में कई बहुत गंभीर संवेदनशीलताएं पाईं हैं जिनसे दूरी से कोड के प्रचालन किया जा सकता है ।

प्रभाव

कोई आक्रमणकर्ता तंत्र को पूरी तरह से अपने नियंत्रण में ले अनुप्रयोग स्थापित कर, प्रयोक्ता और वी जोड़, आंकड़े बदल या मिटा सकता है । शमन करने वाला घटक यह है कि उपरोक्त तभी संभव है जब प्रयोक्ता ने प्रशासक अधिकारों के साथ लॉग-इन किया हुआ हो । जो प्रयोक्ता कम अधिकारों के साथ लॉग-इन करते हैं उन पर कम प्रभाव पड़ सकता है ।

समाधान

अपने इंटरनेट एक्सप्लोरर को तुरंत पैच करें ।

विवरण (विस्तृत जानकारी)

अधिक जानकारी के लिए ms06-042.mspx देखें

परिशिष्ट

अधिक जानकारी के लिए ms06-042.mspx देखें

अब यह नतीजा वितरण के लिए तैयार है । चूंकि यह एक महत्त्वपूर्ण विज्ञप्ति है इसलिए जब संभव हो घटकों को फ़ोन करने की सलाह दी जाती है ।

काल्पनिक सी० एस० आई० आर० टी० (चरण 10)

अभ्यास करना

प्रचालन के शुरूआती सप्ताहों के दौरान काल्पनिक सी० एस० आई० आर० टी० ने ऐसे कई काल्पनिक मामलों का उपयोग किया (जो उन्हें अन्य सी० एस० आई० आर० टी०ओं से उदाहरण के तौर पर मिले थे) अभ्यास के दौरान जिनका प्रयोग किया गया था । इसके अलावा उन्होंने अन्य यंत्र और प्रक्रिया सामग्री विक्रेताओं द्वारा वितरित असली संवेदनशीलता जानकारी के आधार पर कुछ सुरक्षा परामर्श जारी किये जिन्हें उन्होंने अपने चुनाव-क्षेत्र की ज़रूरतों के अनुसार ठीक व समायोजित किया ।

11. निष्कर्ष

निदेशिका यहाँ खत्म होती है । इस दस्तावेज़ का उद्देश्य एक सी० एस० आई० आर० टी० स्थापित करने के लिए ज़रूरी विभिन्न प्रक्रियाओं का एक बहुत ही संक्षिप्त सिंहावलोकन प्रदान करना है । यह पूर्ण होने का दावा नहीं करता और न ही यह बहुत ज़्यादा विशिष्ट विवरण देता है । इस विषय पर पठनीय साहित्य के लिए कृपया परिशिष्ट में खंड *क. अतिरिक्त पठन-सामग्री* देखें ।

अब काल्पनिक सी० एस० आई० आर० टी० के लिए अगले महत्त्वपूर्ण चरण निम्नलिखित होंगे :

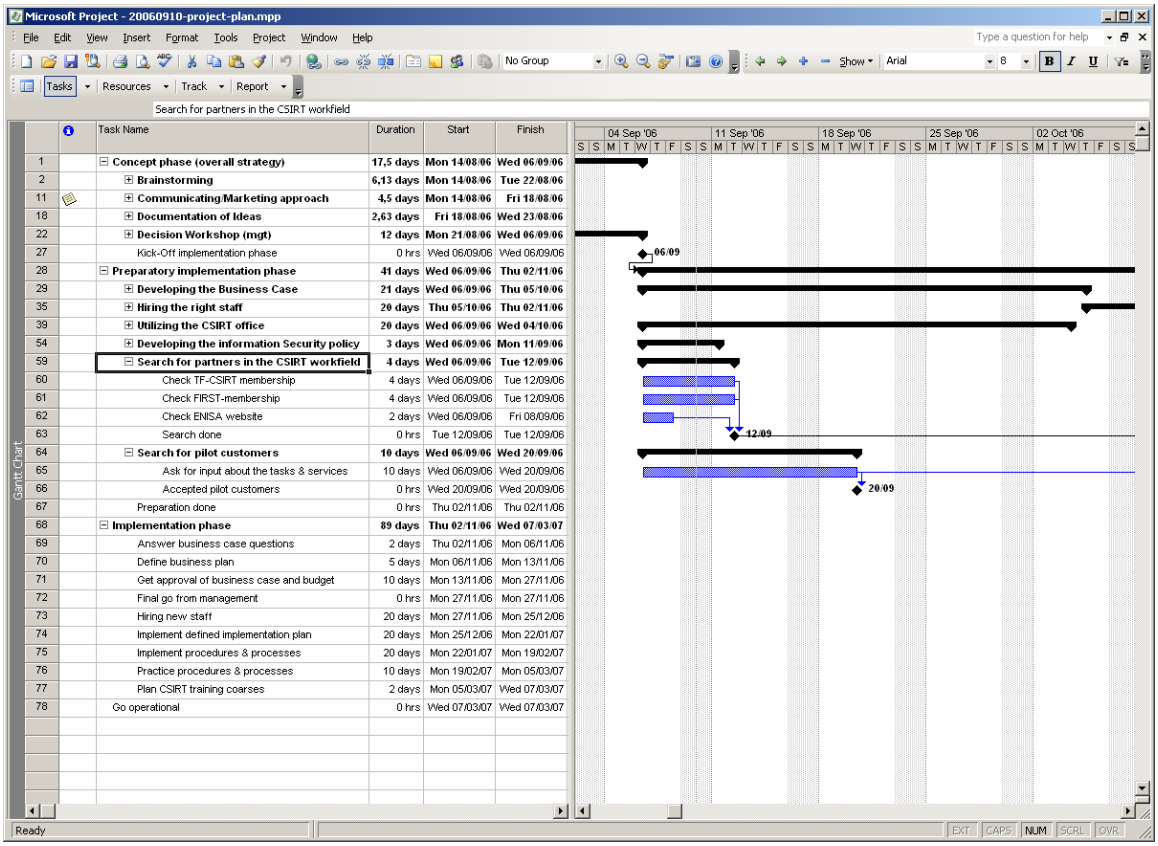
- प्रदान की जाने वाली सेवाओं को बेहतर बनाने के लिए चुनाव-क्षेत्र से प्रतिपुष्टि प्राप्त करना
- दैनिक कार्य को नियमित बनाना
- आकस्मिक परिस्थितियों का अभ्यास करना
- विभिन्न सी० एस० आई० आर० टी० समुदायों के स्वैच्छिक कार्य में एक दिन सहयोग करने के उद्देश्य से उनके साथ निकट संपर्क में रहना

12. परियोजना योजना का विवरण

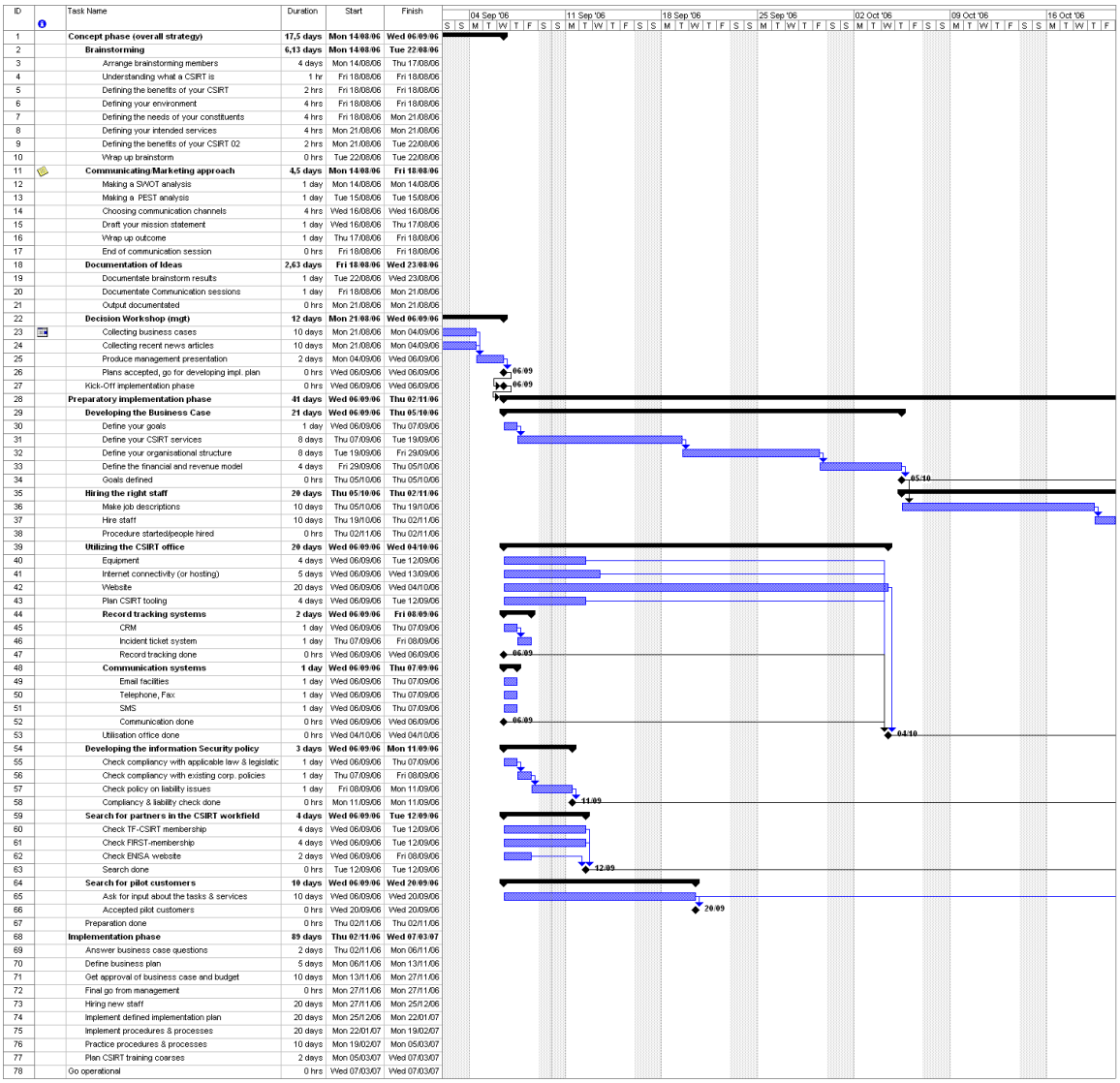
टिप्पणी : परियोजना योजना ज़रूरी समय का पहला अनुमान है । उपलब्ध संसाधनों के आधार पर परियोजना की असली अवधि अलग हो सकती है ।

परियोजना योजना सी० डी० और एनीसा की वेबसाइट पर अलग-अलग फ़ॉर्मेटों में उपलब्ध है । इस दस्तावेज़ में जिन प्रक्रियाओं का विवरण दिया गया है यह उन सब के बारे में पूरा विवरण देती है ।

मुख्य फ़ॉर्मेट माइक्रोसॉफ़्ट प्रोजेक्ट होगा जिससे यह इस परियोजना प्रबंधन उपकरण में सीधे काम में लाया जा सके ।



चित्र 17. *परियोजना योजना*



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

चित्र 18. *सभी कार्यों और गैंट चार्ट के एक भाग के साथ परियोजना योजना*

परियोजना योजना सी०वी०एस०- और एक्स०एम०एल०- फ़ॉर्मेटों में भी उपलब्ध है । एनीसा के सी० एस० आई० आर० टी० विशेषज्ञों को अधिक उपयोग का निवेदन किया जा सकता है : cert-relations@enisa.europa.eu!

परिशिष्ट

क.1 अतिरिक्त पठन-सामग्री

सी० एस० आई० आर० टी० के लिए निर्देश-पुस्तिका (सी०ई०आर०टी०/सी०सी०)

सी० एस० आई० आर० टी० के काम के लिए प्रासंगिक सभी विषयों के लिए एक व्यापक संदर्भ-कार्य

स्त्रोत : http://www.cert.org/archive/pdf/csirt-handbook.pdf

सी० एस० आई० आर० टी० के लिए घटना प्रबंधन प्रक्रियाओं को परिभाषित करना : चालू काम

घटना प्रबंधन का एक गहन विश्लेषण

स्त्रोत: http://www.cert.org/archive/pdf/04tr015.pdf

कंप्यूटर सुरक्षा घटना प्रत्युत्तर दलों (सी० एस० आई० आर० टी०) के अभ्यास की स्थिति

इतिहास, आंकड़ों और बहुत-सी अन्य जानकारी सहित दुनिया भर में सी० एस० आई० आर० टी० दृश्य से संबंधित वर्तमान स्थिति का व्यापक विश्लेषण

स्त्रोत: http://www.cert.org/archive/pdf/03tr001.pdf

एक बक्से में सी०ई०आर०टी०

GOVCERT.NL और 'De Waarschuwingsdienst', डच राष्ट्रीय चेतावनी सेवा स्थापित करने से सीखी गईं सीखों का व्यापक विवरण ।

स्त्रोत: http://www.govcert.nl/render.html?it=69

आर०एफ़०सी० 2350 : कंप्यूटर सुरक्षा घटना प्रत्युत्तर से अपेक्षाएं

स्त्रोत: http://www.ietf.org/rfc/rfc2350.txt

एन०आई०एस०टी०[37] द्वारा प्रकाशित कंप्यूटर सुरक्षा घटनाओं पर कार्रवाई करने की मार्गदर्शिका

स्त्रोत: http://www.securityunit.com/publications/sp800-61.pdf

एनीसा द्वारा तैयार की गई युरोप में सी०ई०आर०टी० गतिविधियों की सूची

एक संदर्भ-कार्य जिसमें युरोप में सी० एस० आई० आर० टी०ओं के बारे में जानकारी और उनकी विभिन्न गतिविधियों की सूची दी गई है

स्त्रोत: http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] एन०आई०एस०टी० : राष्ट्रीय मानक और तकनीक संस्थान

क.2 सी० एस० आई० आर० टी० सेवायें

उन सी०ई०आर०टी०/सी०सी० को विशेष धन्यवाद जिन्होंने यह सूची प्रदान की

प्रतिक्रियात्मक सेवायें	**सक्रिय सेवायें**	**शिल्पकृति पर कार्रवाई**
• **सतर्कादेश और चेतावनियां** • **घटना पर कार्रवाई करना** • **घटना का विश्लेषण** • **घटना प्रत्युत्तर सहायता** • **घटना प्रत्युत्तर समन्वयन** • घटना-स्थल पर घटना-प्रत्युत्तर • सुभेद्यता पर कार्रवाई • सुभेद्यता विश्लेषण • सुभेद्यता प्रत्युत्तर • सुभेद्यता प्रत्युत्तर समन्वयन	• **घोषणाएं** • तकनीक पर नजर रखना • सुरक्षा लेखा-परीक्षा या मूल्यांकन • सुरक्षा का विन्यास व देखभाल • सुरक्षा उपकरणों का विकास • घुसपैठ का पता लगाने की सेवायें • सुरक्षा-संबंधी जानकारी का वितरण	• *शिल्पकृति विश्लेषण* • *शिल्पकृति प्रत्युत्तर* • *शिल्पकृति प्रत्युत्तर समन्वयन* ***सुरक्षा गुणवत्ता प्रबंधन*** • *जोखिम विश्लेषण* • *व्यापार निरंतरता और विपदा से उबरना* • *सुरक्षा परामर्श* • *ज्ञान-वर्धन* • *शिक्षा/ प्रशिक्षण* • *उत्पाद का मूल्यांकन या प्रमाणीकरण*

चित्र 1. *सी०ई०आर०टी०/सी०सी० से प्राप्त सी०एस०आई०आर०टी सेवाओं की सूची*

सेवा विवरण

प्रतिक्रियात्मक सेवाएं

प्रतिक्रियात्मक सेवाओं को सहायता के निवेदनों, सी० एस० आई० आर० टी० चुनाव-क्षेत्र से प्राप्त घटनाओं की सूचनाओं और सी० एस० आई० आर० टी० तंत्रों के खिलाफ़ किसी भी धमकी या आक्रमण का प्रत्युत्तर देने के लिए बनाया गया है । कुछ सेवायें तृतीय-पक्षों द्वारा दी गई सूचना या नज़र रखने की प्रक्रिया या आई०डी०एस० लॉग्स और चेतावनियों को देख कर शुरू की जा सकतीं हैं ।

सतर्कादेश और चेतावनियां

यह सेवा उस जानकारी के वितरण से संबद्ध है जो एक घुसपैठिये के आक्रमण, सुरक्षा संवेदनशीलता, घुसपैठ सतर्कादेश, कंप्यूटर वॉयरस या छल (होएक्स) का विस्तृत विवरण देती है । इसके साथ-साथ यह सेवा इनसे उत्पन्न होने वाली समस्या का सामना करने के लिए सुझाई गई कम अवधि की कार्रवाई प्रदान करने से भी संबद्ध है । सतर्कादेश, चेतावनी या परामर्श विज्ञप्ति वर्तमान समस्याओं के बारे में घटकों को गतिविधियों की जानकारी देने की प्रतिक्रिया के तौर पर और घटकों को अपने तंत्रों की रक्षा करने या किसी

भी प्रभावित तंत्र को पुनः ठीक करने ने लिए भेजी जाती है । जानकारी सी० एस० आई० आर० टी० द्वारा तैयार की जा सकती है या फिर विक्रेताओं, अन्य सी० एस० आई० आर० टी०ओं या सुरक्षा विशेषज्ञों या चुनाव-क्षेत्र के अन्य भागों से प्राप्त कर पुनः वितरित की जा सकती है ।

घटनाओं पर कार्रवाई

घटना पर कार्रवाई करने में निवेदन व रिपोर्टें प्राक्त करना, उनकी छंटनी करना और उनका प्रत्युत्तर देना एवं घटनाओं व कार्यक्रमों का विश्लेषण करना शामिल है । विशिष्ट प्रत्युत्तर कार्रवाइयों में निम्नलिखित शामिल हो सकतीं हैं :

- घुसपैठिये की गतिविधि से प्रभावित या प्रभाव के डर वाले तंत्रों और नेटवर्कों की रक्षा के लिए कार्रवाई करना
- प्रासंगिक परामर्श विज्ञप्तियों या सतर्कादेशों से समाधान और शमन रणनितियां प्रदान करना
- नेटवर्क के अन्य भागों पर घुसपैठ की कार्रवाई ढूंढना
- नेटवर्क ट्रेफ़िक छानना
- तंत्रों का पुनर्निर्माण
- तंत्रों में पैच लगाना या उनकी मरम्मत करना
- अन्य प्रत्युत्तर या वर्कअराउंड रणनीतियां विकसित करना

चूंकि विभिन्न तरह के सी० एस० आई० आर० टी० घटना पर कार्रवाई करने की गतिविधियों को अलग-अलग तरह से कार्यान्वित करते हैं इसलिए किस प्रकार की कार्रवाई की गई और मदद दी गई इस आधार पर यह सेवा निम्नलिखित ढंग से आगे पुनः श्रेणीबद्ध की जाती है :

घटना का विश्लेषण

घटना के विश्लेषण के कई स्तर और कई उप-सेवायें हैं । घटना का विश्लेषण मुख्यतः एक घटना या कार्यक्रम से संबंधित सभी उपलब्ध जानकारियों और समर्थन करने वाले सबूतों या शिल्पकृतियों की जाँच है । इस विश्लेषण का उद्देश्य घटना के परास को, घटना से कितनी क्षति हुई, घटना का प्रकार और उपलब्ध रणनीतियां या वर्कअराउंड पहचानना है । सी० एस० आई० आर० टी० संवेदनशीलता और शिल्पकृति विश्लेषण (जिसका विस्तृत विवरण नीचे दिया गया है) के नतीजों का उपयोग एक विशिष्ट तंत्र पर क्या हुआ है यह समझने और इसके सबसे पूर्ण और अद्यतित विश्लेषण प्रदान करने के लिए कर सकता है । सी० एस० आई० आर० टी० अलग-अलग घटनाओं की गतिविधियों को जोड़ कर यह पता लगाता है कि क्या उनमें कोई परस्पर संबंध, रुझान, प्रतिरूप (पैटर्न) या घुसपैठिये के हस्ताक्षर हैं । निम्नलिखित दो उप-सेवाओं का उपयोग सी० एस० आई० आर० टी० के उद्देश्य, लक्ष्य और प्रक्रियाओं के आधार पर घटना के विश्लेषण के भाग के रूप में किया जा सकता है :

फ़ोरेन्सिक प्रमाण एकत्रित करना

तंत्र में बदलावों का पता लगाने और अंतर्ग्रस्त होने तक की घटनाओं के पुनर्निर्माण में मदद करने के लिए एक अंतर्ग्रस्त कंप्यूटर तंत्र से दस्तावेज़ों को एकत्रित करना और सहेजना एवं प्रमाण का विश्लेषण करना । जानकारी और प्रमाण एकत्रित करने की यह प्रक्रिया इस तरह की जानी चाहिए कि सभी दस्तावेज़ एक

ऐसी कड़ी बनाएं जिसे साबित किया जा सके और जो प्रमाणों के नियमों के अंतर्गत न्यायालय में स्वीकार की जा सके । फ़ोरेन्सिक प्रमाण एकत्रित करने में निम्नलिखित शामिल हैं : प्रभावित तंत्र की हार्ड-ड्राइव की बिट-छवि की प्रतिकृति बनाना; तंत्र में बदलावों जैसे नए अनुप्रयोगों (प्रोग्रेम), फ़ाइलों, सेवाओं व प्रयोक्ताओं की जाँच करना ; चालू प्रक्रियाओं व खुले पोर्ट खोजना एवं ट्रोजन होर्स कार्यक्रमों और उपकरण-समूहों के लिए जाँच करना । यह कार्य करने वाले सी० एस० आई० आर० टी० कर्मचारी को न्यायालय की कार्रवाइयों के दौरान विशेषज्ञ साक्षी के रूप में काम करने के लिए भी तैयार करना पड़ सकता है ।

अन्वेषण करना या खोजना

एक घुसपैठिये के उद्गम का पता लगाना या जिन तंत्रों तक घुसपैठिये की पहुँच है उन्हें पहचानना । इस गतिविधि में यह अन्वेषण करना या खोजना शामिल हो सकता है कि घुसपैठिया प्रभावित तंत्र या संबंधित नेटवर्कों में कैसे घुसा, घुसपैठ करने के लिए किन तंत्रों का उपयोग किया गया था, आक्रमाण कहाँ शुरू हुआ और आक्रमण के भाग के रूप में कौन-से अन्य तंत्रों व नेटवर्कों का उपयोग किया गया था । इसमें घुसपैठिये की पहचान सुनिश्चित करना भी शामिल हो सकता है । यह काम अकेले किया जा सकता है परंतु आमतौर पर इसमे कानून लागू करने वाले कर्मचारियों, इंटरनेट सेवा प्रदाताओं या अन्य संबंधित संस्थानों के साथ काम करना शामिल होता है ।

घटना के स्थान पर प्रत्युत्तर

घटकों की एक घटना से उबरने में मदद करने के लिए सी० एस० आई० आर० टी० सीधी, घटना-स्थल पर सहायता प्रदान करता है । केवल फ़ोन या ई-मेल द्वारा घटना प्रत्युत्तर देने की बजाय सी० एस० आई० आर० टी० स्वयं प्रभावित तंत्रों का भौतिक विश्लेषण करता है और उनकी मरम्मत व उन्हें ठीक करता है (नीचे देखें) । इस सेवा में अगर किसी घटना के होने का शक है या वह घटित होती है तो स्थानीय स्तर पर ज़रूरी सभी कार्य करना शामिल है । अगर प्रभावित स्थल पर सी० एस० आई० आर० टी० का पता नहीं लगता तो दल के सदस्य घटना-स्थल पर जा कर प्रत्युत्तर प्रदान करते हैं । अन्य मामलों में हो सकता है कि एक स्थानीय दल अपने दैनिक कार्य के भाग के रूप में घटना प्रत्युत्तर देते हुए पहले से ही घटना स्थल पर मौजूद हो । यह ख़ासतौर पर तब सच होता है जब घटना पर कार्रवाई एक स्थापित सी० एस० आई० आर० टी० की बजाय तंत्र, नेटवर्क या सुरक्षा प्रशासकों द्वारा एक सामान्य कार्य के भाग के रूप में की जाए ।

घटना प्रत्युत्तर सहायता

सी० एस० आई० आर० टी० एक आक्रमण के शिकारों को फ़ोन, ई-मेल, फ़ैक्स या दस्तावेज़ों द्वारा घटना से उबरने में मदद करता है । इसमें एकत्रित आंकड़ों की व्याख्या, संपर्क जानकारी प्रदान करने या शमन करने या उबरने की रणनीतियों से संबंधित मार्गदर्शन प्रदान करने के लिए तकनीकी सहायता देना शामिल हो सकता है । इसमें जैसा कि ऊपर बताया गया है वैसे सीधे, घटना-स्थल पर प्रत्युत्तर कार्रवाई शामिल नहीं होती । इसकी बजाय सी० एस० आई० आर० टी० दूर से मार्गदर्शन प्रदान करता है जिससे घटना-स्थल पर मौजूद कर्मचारी स्वयं उबरने का काम कर सकें ।

घटना प्रत्युत्तर समन्वयन

सी० एस० आई० आर० टी० एक घटना से संबद्ध पक्षों के बीच प्रत्युत्तर कोशिशों का समन्वयन करता है । आमतौर पर इसमें घटना के शिकार, घटना से संबद्ध अन्य स्थल और घटना का विश्लेषण करने में मदद मांगने वाले अन्य स्थल शामिल होते हैं । इसमें वे पक्ष भी शामिल हो सकते हैं जो शिकार को सूचना प्रौद्योगिकी सहायता प्रदान करते हैं जैसे इंटरनेट सेवा प्रदाता, अन्य सी० एस० आई० आर० टी० और स्थल के तंत्र व नेटवर्क प्रशासक । समन्वयन कार्य में संपर्क जानकारी एकत्रित करना, स्थलों को उनके संभावित संबंध (एक आक्रमण के शिकार या स्त्रोत के रूप में) के बारे में जानकारी देना, संबद्ध स्थलों की संख्याओं के बारे में आंकड़े एकत्रित करना और जानकारी का आदान-प्रदान व विश्लेषण आसान बनाना शामिल हो सकते हैं । समन्वयन कार्य का एक भाग एक संस्थान के कानूनी सलाहकार, मानव संसाधन या जन-संपर्क विभागों को सूचित करना और उनके साथ मिल कर काम करना हो सकता है । इसमें कानून प्रवर्त्तन के साथ समन्वयन भी शामिल होगा । इस सेवा में सीधे घटना-स्थल पर प्रत्युत्तर शामिल नहीं होता ।

संवेदनशीलता पर कार्रवाई

संवेदनशीलता पर कार्रवाई करने में यंत्रसामग्री व प्रक्रिया सामग्री संवेदनशीलताओं के बारे में जानकारी और रिपोर्टें प्राप्त करना ; संवेदनशीलताओं की प्रकृतियों, प्रक्रियाओं व प्रभावों का विश्लेषण करना एवं उन्हें पहचानने के लिए प्रत्युत्तर रणनीतियां विकसित करना व संवेदनशीलताओं की मरम्मत करना शामिल हैं । चूंकि विभिन्न तरह के सी० एस० आई० आर० टी० संवेदनशीलताओं पर कार्रवाई करने की गतिविधियों को अलग-अलग तरह से कार्यान्वित करते हैं इसलिए किस प्रकार की कार्रवाई की गई और मदद दी गई इस आधार पर यह सेवा निम्नलिखित ढंग से आगे पुनः श्रेणीबद्ध की जाती है :

संवेदनशीलता विश्लेषण

सी० एस० आई० आर० टी० यंत्रसामग्री या प्रक्रिया सामग्री में संवेदनशीलताओं का तकनीकी विश्लेषण व जाँच करता है । इसमें संवेदनशीलताएं कहाँ मौजूद हैं और इनका फ़ायदा कैसे उठाया जा सकता है यह पता लगाने के लिए संदिग्ध संवेदनशीलताओं और यंत्रसामग्री या प्रक्रिया सामग्री की संवेदनशीलताओं की तकनीकी जाँच की जाती है । विश्लेषण में संवेदनशीलता कहाँ उत्पन्न होती है यह पता लगाने के लिए डिबग्गर का उपयोग कर स्त्रोत कोड का पुनरावलोकन या समस्या को एक परीक्षण तंत्र पर पुनः उत्पन्न करने की कोशिश शामिल हो सकती है ।

संवेदनशीलता का प्रत्युत्तर

इस सेवा में संवेदनशीलता का शमन करने या उसकी मरम्मत करने के लिए उपयुक्त प्रत्युत्तर निश्चित करना शामिल होता है । इसमें पैच, फ़िक्स और वर्कअराउंड विकसित करना या उन पर अनुसंधान करना शामिल हो सकता है । इसमें संभवतः परामर्श विज्ञप्तियां या सतर्कादेश बना व वितरित कर अन्य लोगों को शमन रणनीति के बारे में सूचित करना भी शामिल होता है । इस सेवा में पैच, फ़िक्स या वर्कअराउंड लगा कर प्रत्युत्तर देना शामिल हो सकता है ।

संवेदनशीलता प्रत्युत्तर समन्वयन

सी० एस० आई० आर० टी० कंपनी या चुनाव-क्षेत्र के विभिन्न भागों को संवेदनशीलता के बारे में सूचित करता है और संवेदनशीलता को कैसे ठीक करना है या फिर उसका शमन कैसे करना है इस बारे में जानकारी बांटता है । सी० एस० आई० आर० टी० यह सत्यापित करता है कि संवेदनशीलता प्रत्युत्तर रणनीति को सफलतापूर्वक कार्यान्वित किया गया है । इस सेवा में विक्रेताओं, अन्य सी० एस० आई० आर० टी०ओं, तकनीकी विशेषज्ञों, संघटक सदस्यों और उन व्यक्तियों या समूहों के साथ जानकारी का आदान-प्रदान करना शामिल हो सकता है जिन्होंने पहले संवेदनशीलता का पता लगाया या इसकी जानकारी दी । गतिविधियों में संवेदनशीलता या संवेदनशीलता रिपोर्ट का विश्लेषण ; संबंधित दस्तावेज़ों, पैचों या वर्कअराउंड की रिलीज़ योजनाओं का समन्वयन एवं विभिन्न पक्षों द्वारा किये गए तकनीकी विश्लेषण का संयोजन करने में मदद करना शामिल होता है । इस सेवा में संवेदनशीलता संबंधी जानकारी का सार्वजनिक या निजी सहेजी हुई जानकारी-संग्रह या ज्ञानसंग्रह और उनसे संबंधित प्रत्युत्तर रणनीतियां भी शामिल हो सकतीं हैं ।

शिल्पकृति पर कार्रवाई

एक शिल्पकृति ऐसी कोई भी फ़ाइल या दस्तावेज़ है जो तंत्रों व नेटवर्कों की छान-बीन करने या उन पर आक्रमण करने से संबद्ध हो सकता है या फिर जिसका इस्तेमाल सुरक्षा उपायों को बेकार करने के लिए किया जा रहा है । शिल्पकृतियों में वॉयरस, ट्रोजन होर्सेज़ अनुप्रयोग, वॉर्म, एक्सप्लॉयट स्क्रिप्ट और उपकरणों की किट शामिल हो सकती हैं परंतु यह इन तक सीमित नहीं हैं ।

शिल्पकृतियों पर कार्रवाई करने में शिल्पकृतियों के बारे में जानकारी व उनकी वे प्रतिकृतियां प्राप्त करना शामिल होता है जिनका उपयोग घुसपैठियों के आक्रमणों, पहचान और अन्य अनधिकृत या गड़बड़ी उत्पन्न करने वाली गतिविधियों के लिए किया जाता है । एक बार प्राप्त होने पर शिल्पकृतियों का पुनरावलोकन किया जाता है । इसमें शिल्पकृतियों की प्रकृति, प्रक्रियाओं, संस्करण और उपयोग एवं इन शिल्पकृतियों को पहचानने, इन्हें हटाने और इनसे सुरक्षा के लिए प्रतिक्रिया रणनीतियां विकसित करना (या उनकी सलाह देना) । चूंकि विभिन्न तरह की सी० एस० आई० आर० टी० शिल्पकृतियों पर कार्रवाई करने की गतिविधियों को अलग-अलग तरह से कार्यान्वित करते हैं इसलिए किस प्रकार की कार्रवाई की गई और मदद दी गई इस आधार पर यह सेवा निम्नलिखित ढंग से आगे पुनः श्रेणीबद्ध की जाती है:

शिल्पकृति विश्लेषण

सी० एस० आई० आर० टी० एक तंत्र पर पाई गई हर शिल्पकृति की एक तकनीकी जाँच व विश्लेषण करता है । हो सकता है कि किये गए विश्लेषण में शिल्पकृति की फ़ाइल के प्रकार व ढांचे की पहचान करना, समानतायें व अंतर देखने के लिए नई शिल्पकृति की पहले से मौजूद शिल्पकृतियों या उसी शिल्पकृति के अन्य संस्करणों के साथ तुलना करना या शिल्पकृति के उद्देश्य व कार्य का पता लगाने के लिए उलट अभियांत्रिकी (रिवर्स इंजीनियरिंग) या डिसैसेंब्लिंग कोड करना शामिल हो सकता है ।

शिल्पकृति प्रत्युत्तर

इस सेवा में शिल्पकृति को किसी तंत्र से हटाने के लिए उपयुक्त कार्य एवं शिल्पकृतियों को स्थापित करने से बचने के लिए कार्य शामिल होते हैं । इसमें वे हस्ताक्षर बनाना शामिल हो सकता है जो एंटीवॉयरस प्रक्रिया सामग्री या आई० डी० एस० में जोड़े जा सकते हैं ।

शिल्पकृति प्रत्युत्तर समन्वयन

इस सेवा में अन्य अनुसंधानकर्ताओं, सी० एस० आई० आर० टी०ओं, विक्रेतां व अन्य सुरक्षा विशेषज्ञों के साथ एक शिल्पकृति से संबंधित विश्लेषण के नतीजों व प्रत्युत्तर रणनीतियों का आदान-प्रदान और उनका संयोजन शामिल होता है । गतिविधियों में अन्य लोगों को सूचित करना और विविध स्त्रोतों से प्राप्त तकनीकी विश्लेषणों का संयोजन करना शामिल है । गतिविधियों में ज्ञात शिल्पकृतियों और उनके प्रभाव व संबंधित प्रतिक्रिया रणनीतियों का एक सार्वजनिक या संघटक ज्ञानसंग्रह बनाए रखना शामिल हो सकता है ।

सक्रिय सेवाएं

सक्रिय सेवाओं को किसी भी घटना या कार्यक्रम के होने या पता लगने से पहले चुनाव-क्षेत्र की अवसंरचना व सुरक्षा प्रक्रियाओं को बेहतर बनाने के लिए बनाया जाता है । मुख्य लक्ष्य घटनाओं से बचना और उनके होने पर उनके प्रभाव व प्रसार को कम करना होता है ।

घोषणाएं

इसमें घुसपैठ सतर्कादेश, संवेदनशीलता की चेतावनियां व सुरक्षा परामर्श विज्ञप्तियां शामिल हैं परंतु यह इन तक सीमित नहीं है । इस तरह की घोषणाएं घटकों को मध्यम- से दीर्घकालीन प्रभावे से संबंधित नये विकासों के, जैसे जिन असुरक्षाओं या घुसपैठ के उपकरणों का हाल ही में पता चला है उनके, बारे में सूचित करतीं हैं । घोषणाओं से संघटक हाल ही में खोजी गई समस्याओं का उपयोग हो उससे पहले ही अपने तंत्रों व नेटवर्कों की उनसे रक्षा कर सकते हैं ।

तकनीक की चौकीदारी

सी० एस० आई० आर० टी० भविष्य में आने वाले खतरों को पहचानने के लिए नए तकनीकी विकासों, घुसपैठिये की गतिविधियों व संबंधित रुझानों पर नज़र रखता है । जिन विषयों का पुनरावलोकन किया गया है कानूनी व वैधानिक निर्णयों, सामाजिक या राजनीतिक खतरों और नयी तकनीकों को शामिल करने के लिए उनके परास को बढ़ाया जा सकता है । इस सेवा में संघटक तंत्रों व नेटवर्कों की सुरक्षा से संबंधित जानकारी एकत्रित करने के लिए विज्ञान, तकनीक, राजनीति व सरकार के क्षेत्रों की सुरक्षा मेलिंग सूचियों, सुरक्षा वेब-साइटों और हाल की खबरों व अख़बार के लेखों को पढ़ना शामिल होता है । इसमें यह सुनिश्चित करने के लिए इन क्षेत्रों में विशेषज्ञ ऐसे अन्य पक्षों से जानकारी का आदान-प्रदान करना शामिल हो सकता है कि बेहतरीन और सबसे सही जानकारी या अर्थ प्राप्त किया गया है । कुछ प्रकार की ऐसी घोषणाएं, निर्देश या सुझाव जिनका ध्यान अधिक मध्यम- से दीर्घ-कालीन सुरक्षा-संबंधी मुद्दों पर केंद्रित हो इस सेवा का नतीजा हो सकते हैं ।

सुरक्षा लेखा-परीक्षण या निर्धारण

यह सेवा संस्थान या लागू होने वाले अन्य उद्योग मानकों द्वारा परिभाषित ज़रूरतों के आधार पर किसी संस्थान की सुरक्षा अवसंरचना का एक विस्तृत पुअरावलोकन और विश्लेषण प्रदान करती है । इसमें संस्थान के सुरक्षा अभ्यासों का एक पुनरावलोकन भी शामिल हो सकता है । कई अलग-अलग प्रकार के लेखा-परीक्षण या मूल्यांकन प्रदान किये जा सकते हैं जिनमें निम्नलिखित शामिल हैं :

अवसंरचना पुनरावलोकन

यंत्रसामग्री और प्रक्रिया सामग्री के विन्यास, राउटर्ज़, फ़ायरवॉल्ज़, सर्वर व डेस्कटॉप उपकरणों का यह सुनिश्चित करने के लिए हस्तचालित पुनरावलोकन करना कि वे संस्थान या उद्योग की सुरक्षा नीतियों और मानक विन्यासों से संबंधित बेहतरीन अभ्यासों से मेल खाते हैं ।

बेहतरीन अभ्यास पुनरावलोकन

कर्मचारियो और तंत्र व नेटवर्क प्रशासकों का यह सुनिश्चित करने के लिए साक्षात्कार करना कि क्या उनके सुरक्षा-अभ्यास संस्थान की परिभाषित सुरक्षा नीति या किसी विशिष्ट उद्योग मानक से मेल खाते हैं या नहीं ।

स्कैन करना

संवेदनशीलता या वॉयरस स्कैनरों का यह सुनिश्चित करने के लिए प्रयोग करना कि कौन-से तंत्र और नेटवर्क संवेदनशील हैं ।

प्रवेश परीक्षण करना

किसी स्थान के तंत्रों और नेटवर्कों पर जान-बूझ कर आक्रमण कर उसकी सुरक्षा का परीक्षण करना
इस तरह के लेखा-परीक्षण या मूल्यांकन करने से पहले उच्च प्रबंधन की स्वीकृति प्राप्त करना आवश्यक है । हो सकता है कि संस्थान की नीति द्वारा इनमें से कुछ प्रस्तावों पर प्रतिबंध लगा हो । इस तरह की सेवा प्रदान करने में परीक्षण, मूल्यांकन, लेखा-परीक्षण या पुनरावलोकन करने वाले कर्मचारियों के लिए आवश्यक कौशल समूह या प्रमाणीकरण आवश्यकताएं विकसित करने के साथ-साथ एक ऐसे सामान्य अभ्यासों का समूह विकसित करना शामिल हो सकता है जिनके आधार पर परीक्षण या मूल्यांकन किया जाते हैं । किसी तृतीय पक्ष के ठेकेदार को भी यह सेवा करने को कहा जा सकता है या फिर लेखा-परीक्षण और मूल्यांकन करने में उपयुक्त विशेषज्ञताप्राप्त सुरक्षा सेवा प्रदाता द्वारा भी इसका प्रबंध किया जा सकता है ।

सुरक्षा उपकरणों, अनुप्रयोगों, अवसंरचनाओं और सेवाओं का विन्यास और मरम्मत

यह सेवा यह पता लगाती है या फिर इस दिशा में उपयुक्त मार्गदर्शन करती है कि सी० एस० आई० आर० टी० चुनाव-क्षेत्र या सी० एस० आई० आर० टी० द्वारा खुद जिन उपकरणों, अनुप्रयोगों और सामान्य कंप्यूटिंग अवसंरचनाओं का उपयोग किया जा रहा है उन्हें किस तरह सुरक्षित ढंग से संरूपित करना है और उनकी देखभाल करनी है । मार्गदर्शन करने के अलावा सी० एस० आई० आर० टी० आई०डी०एस०, नेटवर्क स्कैनिंग या निरीक्षण तंत्रों, फ़िल्टरों, रैपरों, फ़ायरवॉल, वर्चुअल निजी नेटवर्कों (वी०पी०एन) या सत्यापन उपकरणों जैसे सुरक्षा उपकरणों और सेवाओं का अद्यतन और मरम्मत भी कर सकता है । सी० एस० आई० आर० टी० अपने मुख्य कार्यों के भाग के तौर पर भी यह सेवायें प्रदान कर सकता है । सी० एस० आई० आर० टी० सुरक्षा निर्देशों के अनुसार सर्वरों, डेस्कटॉप, लैपटॉप, व्यक्तिगत अंकीय सहायकों (पी०डी०ए०) और अन्य बेतार उपकरणों का संरूपण और उनकी देखभाल भी कर सकता है । इस सेवा में प्रबंधन को उपकरणों और अनुप्रयोगों के विन्यास या प्रयोग से संबंधित ऐसे किसी भी मुद्दे या समस्या के बारे में सूचित करना शामिल है सी० एस० आई० आर० टी० के अनुसार जो एक आक्रमण के प्रति असुरक्षित तंत्र छोड़ सकता है ।

सुरक्षा उपकरणों का विकास

इस सेवा में किसी भी ऐसे विशिष्ट संघटक वाले नए उपकरण का विकास करना शामिल है चुनाव-क्षेत्र या सी० एस० आई० आर० टी० को खुद को जिनकी ज़रूरत या अपेक्षा हो । उदाहरण के लिए इसमें

निम्नलिखित शामिल हो सकते हैं : चुनाव-क्षेत्र द्वारा इस्तेमाल की जा रही आवश्यकता के अनुरूप विकसित विशिष्ट प्रक्रिया सामग्री के लिए सुरक्षा पैच विकसित करना या फिर ऐसे सुरक्षित प्रक्रिया सामग्री वितरण विकसित करना जिनका उपयोग अंतर्ग्रस्त मेज़बान के पुनर्निर्माण के लिए किया जा सके । इसमें ऐसे उपकरण या स्क्रिप्टें विकसित करना भी शामिल हो सकता है जो मौजूदा सुरक्षा उपकरणों के कार्य के प्रसार को बढ़ाते हैं जैसे संवेदनशीलता, या नेटवर्क स्कैनर, स्क्रिप्टों के लिए एक ऐसा नया प्लग-इन बनाना जो एन्क्रिप्शन तकनीक या स्वचालित पैच वितरण तरीकों के उपयोग को आसान बनाता हो ।

घुसपैठ अभिज्ञान सेवायें

जो सी० एस० आई० आर० टी० यह सेवा प्रदान करते हैं वे मौजूदा आई०डी०एस० लॉगों का पुनरावलोकन करते हैं और किसी भी ऐसी घटना का विश्लेषण कर उसका प्रत्युत्तर देना शुरू करते हैं जो उनके द्वारा परिभाषित सीमा या फिर पूर्व-निर्धारित सेवा स्तर अनुबंध या सूचना देने की रणनीति के अनुरूप हो । संबंधित सुरक्षा लॉगों की घुसपैठ पहचान व उसका विश्लेषण एक कठिन काम हो सकता है - केवल यह पता लगाने के लिए ही नहीं कि वातावरण में सेन्सर कहाँ स्थित हैं परंतु उसके बाद बड़ी मात्रा में एकत्रित करने और उसका विश्लेषण करने के लिए भी । कई मामलों में ख़तरे की झूठी घंटियों, आक्रमणों या नेटवर्क घटनाओं को पहचानने और इन घटनाओं को ख़त्म करने या कम से कम करने की रणनीतियों को लागू करने की जानकारी का संयोजन करने और समझने के लिए विशेष उपकरणों या दक्षता की ज़रूरत होती है । कुछ संस्थान इस गतिविधि को प्रबंधित सुरक्षा सेवा प्रदाताओं जैसे ऐसे अन्य लोगों या संस्थानों से करवाने का निर्णय लेते हैं जो यह सेवाएं प्रदान करने में ज़्यादा दक्ष हों ।

सुरक्षा-संबंधी जानकारी का वितरण करना

यह सेवा घटकों को ऐसी उपयोगी जानकारी का व्यापक और आसानी से खोजा जा सकने वाला संग्रह प्रदान करती है जिससे सुरक्षा को बेहतर बनाने में मदद मिलती है । ऐसी जानकारी में निम्नलिखित शामिल हो सकते हैं :

- सी० एस० आई० आर० टी० के लिए सूचना देने संबंधी निर्देश और संपर्क जानकारी
- सतर्कादेश, चेतावनी और अन्य घोषणाओं के ज्ञानसंग्रह
- वर्तमान बेहतरीन अभ्यासों के बारे में दस्तावेज़
- सामान्य कंप्यूटर सुरक्षा मार्गदर्शन
- नीतियां, कार्य प्रणालियां और सूचियां
- पैच विकसित और वितरण करने संबंधी जानकारी
- विक्रेता लिंक
- घटनाओं की सूचना देने के संबंध में वर्तमान आंकड़े और रुझान
- ऐसी अन्य जानकारी जो समग्र सुरक्षा अभ्यासों को बेहतर बना सकती है

यह जानकारी सी० एस० आई० आर० टी० या संस्थान के किसी और भाग (सूचना प्रौद्योगिकी, मानव संसाधन या मीडिया संबंध) द्वारा विकसित और प्रकाशित की जा सकती है और इसमें बाह्य संसाधनों जैसे अन्य सी० एस० आई० आर० टी०ओं, विक्रेताओं और सुरक्षा विशेषज्ञों से प्राप्त जानकारी शामिल हो सकती

है ।

सुरक्षा गुणवत्ता प्रबंधन सेवायें

जो सेवायें इस श्रेणी में आती हैं ऐसा नहीं है कि वे केवल विशेषकर घटना पर कार्रवाई करने या सी० एस० आई० आर० टी० के लिए हों । वे ऐसी सुप्रख्यात और प्रतिष्ठित सेवायें हैं जिन्हें एक संस्थान की समग्र सुरक्षा को बेहतर बनाने के लिए बनाया गया है । उपरोक्त प्रतिक्रियात्मक व सक्रिय सेवायें प्रदान करते हुए प्राप्त अनुभव का उत्तोलन कर एक सी० एस० आई० आर० टी० इन गुणवत्ता सेवाओं में ऐसे अनुपम नज़रिये ला सकता है जो हो सकता है कि अन्यथा उपलब्ध न हों । इन सेवाओं को घटनाओं, संवेदनशीलताओं और आक्रमणों का प्रत्युत्तर देते हुए प्राप्त ज्ञान के आधार पर प्राप्त प्रतिपुष्टि और सीखी गईं सीखों को शामिल करने के लिए बनाया गया है । एक सुरक्षा गुणवत्ता प्रबंधन प्रक्रिया के भाग के रूप में इस तरह के अनुभवों को प्रतिष्ठित पारंपरिक सेवाओं (जिनके बारे में नीचे विस्तारपूर्वक बताया गया है) से जोड़ने से एक संस्थान की दीर्घकालीन सुरक्षा की दिशा में की जा रही कोशिशें बेहतर बनतीं हैं । एक संस्थान के ढांचे और ज़िम्मेदारियों के अनुसार एक सी० एस० आई० आर० टी० यह सेवायें प्रदान कर सकता है या फिर एक ज़्यादा बढ़ी संस्थानात्मक दल की कोशिश के हिस्से के रूप में भाग ले सकता है । निम्नलिखित विवरण यह विस्तारपूर्वक बताते हैं कि सी० एस० आई० आर० टी० की दक्षता इन में से प्रत्येक सुरक्षा गुणवत्ता प्रबंधन सेवा को कैसे लाभ पहुँचा सकती है ।

जोखिम विश्लेषण

सी० एस० आई० आर० टी० जोख़िम विश्लेषण और मूल्यांकन में मूल्यवृद्धि कर सकते हैं । इससे संस्थान की असली ख़तरों का मूल्यांकन करने, सूचना परिसंपत्तियों के लिए ख़तरों संबंधी यथार्थवादी गुणवत्तात्मक और परिमाणवाचक मूल्यांकन प्रदान करने एवं सुरक्षा व प्रत्युत्तर रणनीतियों का मूल्यांकन करने क्षमता बेहतर बनती है । यह सेवा प्रदान करने वाले सी० एस० आई० आर० टी० नए तंत्रों और व्यापार प्रक्रियाओं के लिए सूचना सुरक्षा ख़तरे के विश्लेषण गतिविधियां करेंगे या इनमें मदद करेंगे या फिर संघटक परिसंपत्तियों व तंत्रों के ख़िलाफ़ दी जाने वाली धमकियों व किये जाने वाले आक्रमणों का मूल्यांकन करेंगे ।

व्यापार निरंतरता और विपदा से उबरने की योजना बनाना

पिछली घटनाओं और नई घटनाओं या सुरक्षा रुझानों संबंधी भविष्यवाणियों के आधार पर बढ़ती संख्या में घटनाओं के कारण व्यापारिक प्रचालनों की गंभीर अवनति होने की संभावना होती है । अतः योजना बनाने की कोशिशों को व्यापारिक प्रचालनों की निरंतरता सुनिश्चित करने के लिए ऐसी घटनाओं के साथ बेहतरी ढंग से निबटने का निर्णय लेने के लिए सी० एस० आई० आर० टी० अनुभव और सुझावों के बारे में विचार करना चाहिए । यह सेवा प्रदान करने वाले सी० एस० आई० आर० टी० कंप्यूटर सुरक्षा धमकियों व आक्रमणों से संबंधित घटनाओं के लिए व्यापार की निरंतरता और विपदाओं से उबरने की योजना बनाने से जुड़े होते हैं ।

सुरक्षा परामर्श

सी० एस० आई० आर० टी०ओं का उपयोग घटके के व्यापारिक प्रचालनों को लागू करने के लिए बेहतरीन सुरक्षा अभ्यासों को लागू करने से संबंधित सलाह और मार्गदर्शन देने के लिए किया जा सकता है । यह

सेवा प्रदान करने वाला एक सी० एस० आई० आर० टी० नए तंत्रों, नेटवर्क उपकरणों, प्रक्रिया सामग्री अनुप्रयोगों या पूरी कंपनी की व्यापारिक प्रक्रियाओं की खरीद, स्थापना या उन्हें सुरक्षित करने संबंधी सुझाव तैयार करने या ज़रूरतों को पहचानने में लीन होता है । इस सेवा में संस्थानात्मक या चुनाव-क्षेत्र की सुरक्षा नीतियों का विकास करने के लिए मार्गदर्शन और मदद प्रदान करना शामिल है । इसमें वैधानिक या अन्य सरकारी संगठनों को साक्ष्य या सलाह प्रदान करना भी शामिल हो सकता है ।

ज्ञानवर्धन

सी० एस० आई० आर० टी० यह पता लगाने में भी सक्षम हो सकते हैं कि घटकों को स्वीकृत सुरक्षा अभ्यासों और संस्थानात्मक सुरक्षा नीतियों का बेहतर ढंग से पालन करने के लिए कहाँ अधिक जानकारी और मार्गदर्शन की ज़रूरत है । संघटक जनसंख्या का बढ़ता हुआ सामान्य सुरक्षा ज्ञान न केवल सुरक्षा संबंधी मुद्दों के बारे में उनकी समझ को बेहतर बनाता है अपितु यह उनके दैनिक कार्यों को भी अधिक सुरक्षित ढंग से करने में उनकी मदद करता है । इससे सफल आक्रमणों की घटनाओं में कमी आ सकती है और इस बात की संभावना बढ़ सकती है कि संघटक आक्रमणों को पहचान कर उनके बारे में सूचना दे कर उनसे उबरने में लगने वाला समय घटायेंगे और नुक्सान ख़त्म या कम से कम करेंगे ।

यह सेवा प्रदान करने वाले सी० एस० आई० आर० टी० लेख, पोस्टर, सूचना-पत्र, वेब साइटें या जानकारी के अन्य ऐसे स्त्रोत विकसित कर सुरक्षा संबंधी ज्ञान बढ़ाने के मौके खोजते हैं जो बेहतरीन सुरक्षा अभ्यासों के बारे में विस्तारपूर्वक बताते हैं और जो सावधानियां अपनानी हैं उनके बारे में सलाह देते हैं । गतिविधियों में घटकों को चालू सुरक्षा कार्य-प्रणालियों और संस्थानात्मक तंत्रों के लिए संभावित ख़तरों के बारे में नवीनतम जानकारी देने के लिए बैठकें व गोष्ठियां आयोजित करना शामिल हो सकता है ।

शिक्षा/ प्रशिक्षण

इस सेवा में घटकों को गोष्ठियों, कार्यशालाओं, पाठ्यक्रमों और प्रशिक्षण कार्यक्रमों के माध्यम से कंप्यूटर सुरक्षा संबंधी मुद्दों के बारे में जानकारी देना शामिल होता है । शीर्षकों में घटना के बारे में सूचना देने संबंधी निर्देश, उपयुक्त प्रत्युत्तर देने के तरीके, घटना का प्रत्युत्तर देने के काम आने वाले उपकरण, घटना को होने से रोकने वाले तरीके और कंप्यूटर सुरक्षा घटनाओं से सुरक्षा, उनका पता लगाने, उनकी सूचना व प्रत्युत्तर देने के लिए आवश्यक अन्य आवश्यक जानकारी शामिल हो सकती है ।

उत्पाद मूल्यांकन या प्रमाणीकरण

इस सेवा के लिए सी० एस० आई० आर० टी० उपकरणों, अनुप्रयोगों या अन्य सेवाओं पर यह सुनिश्चित करने के लिए उत्पाद मूल्यांकन कर सकता है कि उत्पाद सुरक्षित हैं और वे स्वीकारनीय सी० एस० आई० आर० टी० या संस्थानात्मक सुरक्षा अभ्यासों के अनुरूप हैं । जिन उपकरणों व अनुप्रयोगों का पुनरावलोकन किया जाता है वे मुक्त-स्त्रोत (ओपन-सोर्स) या व्यापारिक उत्पाद दोनों ही हो सकते हैं । यह सेवा संस्थान या सी० एस० आई० आर० टी० द्वारा लागू मानकों के आधार पर एक मूल्यांकन के तौर पर या फिर प्रमाणीकरण कार्यक्रम के माध्यम से प्रदान की जा सकती है ।

क.3 उदाहरण

काल्पनिक सी॰ एस॰ आई॰ आर॰ टी॰

चरण 0 - यह समझना कि एक सी॰ एस॰ आई॰ आर॰ टी॰ क्या है :

नमूने के तौर पर प्रस्तुत सी॰ एस॰ आई॰ आर॰ टी॰ को कम से कम 200 कर्मचारियों वाले मध्यम-आकार के संस्थान की सेवा करनी होगी। संस्थान का अपना अलग सूचना प्रौद्योगिकी विभाग है और उसी देश में दो अन्य शाखाएं हैं। कंपनी में सूचना प्रौद्योगिकी एक प्रमुख भूमिका निभाती है क्योंकि इसका उपयोग आंतरिक संचार, आंकड़ा संगठन-तंत्र और 24x7 ई-व्यापार के लिए किया जाता है। संस्थान का अपना अलग संगठन-तंत्र (नेटवर्क) है और इसके पास दो अलग-अलग इंटरनेट सेवा प्रदाताओं के माध्यम से इंटरनेट के साथ एक अतिरिक्त संयोजन (कॅनैक्शन) है।

- -

चरण 1 : शुरुआती चरण

शुरुआती चरण में नये सी॰ एस॰ आई॰ आर॰ टी॰ की योजना एक ऐसे आंतरिक सी॰ एस॰ आई॰ आर॰ टी॰ के तौर पर बनाई जाती है जो मेज़बान कंपनी, स्थानीय सूचना प्रौद्योगिकी विभाग और कर्मचारियों को अपनी सेवाएं प्रदान करता है। यह दफ़्तर की विभिन्न शाखाओं के बीच सूचना प्रौद्योगिकी सुरक्षा संबंधी घटनाओं पर कार्रवाई का समर्थन व समन्वयन भी करता है।

- -

चरण 2 : सही सेवायें चुनना

शुरुआती चरण में यह निर्णय लिया जाता है कि नया सी॰ एस॰ आई॰ आर॰ टी॰ मुख्यतः कर्मचारियों को कुछ महत्वपूर्ण सेवाएं देने पर अपना ध्यान केंद्रित करेगा।

यह निर्णय लिया जाता है कि शुरुआती चरण के बाद सेवा पोर्टफ़ोलियो के विस्तार पर विचार किया जा सकता है और कुछ 'सुरक्षा प्रबंधन सेवायें' जोड़ी जा सकतीं हैं। यह निर्णय शुरुआती घटकों से प्राप्त प्रतिपुष्टि के आधार पर और गुणवत्ता आश्वासन विभाग के साथ निकट सहयोग द्वारा लिया जाएगा।

- -

चरण 3 : चुनाव-क्षेत्र और उपयुक्त संचार माध्यमों का विश्लेषण करना

प्रबंधन और चुनाव-क्षेत्र के कुछ प्रमुख व्यक्तियों के साथ एक विचार-विमर्श सत्र से स्वॉट विश्लेषण के लिए पर्याप्त आगत उत्पन्न हुई। इससे इस निष्कर्श पर पहुँचे कि महत्वपूर्ण सेवाओं की ज़रूरत है :

- सतर्कादेश और चेतावनियां
- घटना पर कार्रवाई करना (विश्लेषण, प्रत्युत्तर सहायता और प्रत्युत्तर समन्वयन)
- घोषणाएं

यह सुनिश्चित किया जाना चाहिए कि जानकारी सही तरह से संगठित ढंग से वितरित की जाती है जिससे यह चुनाव-क्षेत्र के जितने बड़े भाग तक पहुँच सके पहुँचे।इस लिए निर्णय लिया जाता है कि सतर्कादेश,

चेतावनियां और घोषणाएं सुरक्षा प्रस्तावों के रूप में इस कार्य हेतु ख़ासतौर पर बनाई गई एक वेबसाइट पर प्रकाशित की जाएंगी और मेलिंग सूची द्वारा वितरित की जाएंगी । सी० एस० आई० आर० टी० घटना की रिपोर्टें ई-मेल, फोन और-फ़ैक्स द्वारा प्राप्त करने को आसान बनाता है । अगले चरण के लिए एक एकीकृत वेब-प्रपत्र बनाने की योजना है ।

चरण 4 : उद्देश्य कथन

काल्पनिक सी० एस० आई० आर० टी० के प्रबंधन ने निम्नलिखित उद्देश्य कथन बनाया है:
"*काल्पनिक सी० एस० आई० आर० टी० कंप्यूटर सुरक्षा घटनाओं के जोख़िम को कम करने और साथ-साथ जब इस तरह की घटनाएं हों तो उनका प्रत्युत्तर देने के लिए अपनी मेज़बान कंपनी के कर्मचारियों को जानकारी और मदद प्रदान करता है ।*"

इसके द्वारा काल्पनिक सी० एस० आई० आर० टी० यह स्पष्ट करता है कि यह एक आंतरिक सी० एस० आई० आर० टी० है और इसका प्रमुख कार्य सूचना प्रौद्योगिकी की सुरक्षा से संबंधित मुद्दों का सामना करना है ।

- -

चरण 5 : व्यापार योजना परिभाषित करना

वित्तीय नमूना

चूंकि कंपनी का एक 24x7 ई-व्यापार है और साथ ही एक 24x7 काम करने वाला सूचना प्रौद्योगिकी विभाग है अतः दफ़्तर के समय के दौरान पूर्ण सेवा और दफ़्तर के समय के अलावा बाकी समय पर कॉल-ड्यूटी प्रदान करने का निर्णय लिया जाता है । चुनाव-क्षेत्र के लिए सेवायें मुफ़्त प्रदान की जाएंगी परंतु शुरूआती और मूल्यांकन चरण के दौरान बाहय ग्राहकों को सेवायें प्रदान करने की संभावना का मूल्यांकन किया जाएगा ।

आय का नमूना

शुरूआती- और प्रायोगिक- चरण के दौरान सी० एस० आई० आर० टी० को एक मेज़बान कंपनी के माध्यम से वित्त प्रदान किया जाएगा । प्रायोगिक- और मूल्यांकन चरण के दौरान बाहय ग्राहकों को सेवायें बेचने की संभावना सहित अतिरिक्त वित्त सुलभ कराने के बारे में चर्चा की जाएगी ।

संस्थानात्मक नमूना

मेज़बान संस्थान एक छोटी कंपनी है इसलिए एक जड़ा हुआ नमूना चुना गया है ।
दफ़्तर के समय के दौरान तीन कर्मचारी मूलभूत-सेवायें (सुरक्षा परामर्श का वितरण और घटना पर कार्रवाई /उसका समन्वयन) प्रदान करेंगे ।

कंपनी के सूचना प्रौद्योगिकी विभाग में पहले से ही उपयुक्त कौशलों वाले लोग काम कर रहे हैं । उस विभाग के साथ एक अनुबंध किया जाता है जिससे नये सी० एस० आई० आर० टी० जब भी ज़रूरत पड़े तब तदर्थ आधार पर सहायता का निवेदन कर सके । साथ ही उनके ऑन-काल-तकनीकज्ञों की दूसरी पंक्ति का इस्तेमाल किया जा सकता है ।
पूरा समय काम करने वाले चार सदस्यों और पाँच अतिरिक्त सी० एस० आई० आर० टी० दल के सदस्यों का एक मूल सी० एस० आई० आर० टी० दल होगा । उनमें से एक घूमने वाली पारी पर भी उपलब्ध होगा ।

कर्मचारी

सी० एस० आई० आर० टी० दल के नेता की सुरक्षा और 1ले और 2रे स्तर की सहायता की पृष्ठभूमि है और उसने प्रतिस्कंदन (रिसाइलियेंस) संकट प्रबंधन कार्यक्षेत्र में काम किया है । दल के अन्य तीन सदस्य सुरक्षा विशेषज्ञ हैं । सी० एस० आई० आर० टी० दल के अंशकालिक सदस्य सूचना प्रौद्योगिकी विभाग से हैं और उन्हें कंपनी की अवसंरचना के क्षेत्र में महारत हासिल है ।

चरण 5 : दफ़्तर और जानकारी सुरक्षा नीति का उपयोग करना

दफ़्तर के उपकरण और स्थान

चूंकि मेज़बान कंपनी के पास पहले से ही कारगर भौतिक सुरक्षा है इसलिए नया सी० एस० आई० आर० टी० उस नज़रिये से अच्छी तरह सुरक्षित है । आपातकालीन स्थिति में समन्वयन संभव बनाने के लिए एक तथाकथित "युद्ध कक्ष" प्रदान किया जाता है । सामग्री और संवेदनशील दस्तावेज़ों के 'एन्क्रिप्शन' के लिए एक तिजोरी खरीदी जाती है । दफ़्तर के समय हॉटलाइन आसान बनाने के लिए स्विचबोर्ड युक्त एक अलग फ़ोन लाइन स्थापित की गई थी और दफ़्तर के समय के बाद 'ऑन-कॉल' ड्यूटी के लिए उसी फ़ोन नंबर वाला मोबाइल फ़ोन प्रदान किया गया था ।

सी० एस० आई० आर० टी० संबंधी जानकारी की घोषणा करने के लिए पहले से मौजूद उपकरण और निगम की वेबसाइट का भी उपयोग किया जा सकता है । दल के सदस्यों में आपस में और अन्य दलों के साथ संचार के एक सीमित भाग के साथ एक 'मेलिंग सूची' लगाई और अनुरक्षित की जाती है । कर्मचारियों से संपर्क करने संबंधी सभी विवरण एक आंकड़ा संचय में सहेजे जाते हैं और इनकी एक छपी हुई प्रति तिजोरी में रखी जाती है ।

विनियम

चूंकि सी० एस० आई० आर० टी० कंपनी में उसकी पहले से मौजूद सूचना सुरक्षा नीतियों में जड़ा जाता है इसलिए सी० एस० आई० आर० टी० के लिए अनुरूपण नीतियां कंपनी के कानूनी सलाहकार की मदद से स्थापित की गईं हैं ।

- -

चरण 7 : सहयोग की खोज करना

एनीसा की सूची का इस्तेमाल कर एक ही देश में मौजूद कुछ सी० एस० आई० आर० टी० खोजे गए और उनसे संपर्क किया गया । उनमें से एक के साथ हाल ही में काम पर रखे गए दल-नेता के लिए स्थान-यात्रा आयोजित की गई । उसने राष्ट्रीय सी० एस० आई० आर० टी० गतिविधियों के बारे में सीखा और एक बैठक में भाग लिया ।

यह बैठक काम करने के तरीकों के उदाहरण एकत्रित करने और कुछ अन्य दलों से सहयोग प्राप्त करने में बहुत ज़्यादा मददगार साबित हुई ।

- -

चरण 8 : व्यापार योजना को बढ़ावा देना

कंपनी के इतिहास से तथ्य और अंक एकत्रित करने का निर्णय लिया जाता है । सूचना प्रौद्योगिकी सुरक्षा परिस्थिति के आंकड़ा सिंहावलोकन के लिए यह अत्याधिक उपयोगी है । जब सी० एस० आई० आर० टी० काम कर रहा हो तब यह संग्रह जारी रखा जाना चाहिए जिससे आंकड़ों अद्यतित रखा जा सके ।

अन्य राष्ट्रीय सी० एस० आई० आर० टी०ओं से भी संपर्क किया गया और उनके व्यापारिक मामलों के बारे में उनका साक्षात्कार लिया गया । उन्होंने सूचना प्रौद्योगिकी सुरक्षा घटनाओं के क्षेत्र में हाल में हुए विकासों और घटनाओं की लागतों के बारे में कुछ स्लाइडें बना कर सहायता की ।

उदाहरण के तौर पर दिये गए इस काल्पनिक सी० एस० आई० आर० टी० के मामले में प्रबंधन को सूचना प्रौद्योगिकी व्यापार के महत्त्व के बारे में विश्वास दिलाने की कोई ख़ास जल्दी नहीं थी और इसलिए पहले कदम के लिए आगे बढ़ने की अनुमति प्राप्त करना कठिन नहीं था । स्थापित करने और प्रचालन की लागत के अनुमान सहित एक व्यापार मामला और एक परियोजना योजना तैयार किये गए थे ।

- -

चरण 9 : प्रक्रिया प्रवाह और प्रचालक व तकनीकी कार्य-प्रणालिया स्थापित करना

काल्पनिक सी॰ एस॰ आईः॰ आर॰ टी॰ मूल सी॰ एस॰ आईः॰ आर॰ टी॰ सेवायें देने पर अपना ध्यान केंद्रित करता है ।

- सतर्कादेश और चेतावनियां
- घोषणाएं
- घटनाओं पर कार्रवाई

दल ने वे कार्य-प्रणालियां विकसित कीं हैं जो सही ढंग से काम करती है और जिसे दल का हर सदस्य आसानी से समझ सकता है । काल्पनिक सी॰ एस॰ आईः॰ आर॰ टी॰ ने देयताओं और सूचना सुरक्षा नीति पर कार्रवाई करने के लिए एक कानूनी विशेषज्ञ को भी नौकरी पर रखा । दल ने कुछ महत्त्वपूर्ण उपकरण अपनाये और अन्य सी॰ एस॰ आईः॰ आर॰ टी॰ओं से चर्चा कर प्रचालन संबंधी मुद्दों के बारे में उपयोगी जानकारी प्राप्त की ।

सुरक्षा परामर्शों और घटनाओं की रिपोर्टों के लिए एक निश्चित टेम्प्लेट भी तैयार किया गया । घटना पर कार्रवाई करने के लिए दल आर॰टी॰आईः॰आर॰ का उपयोग करता है ।

- -

चरण 10 : कर्मचारियों को प्रशिक्षित करना

काल्पनिक सी॰ एस॰ आईः॰ आर॰ टी॰ अपने सभी कर्मचारियों को अगले उपलब्ध ट्रान्सिट पाठ्यक्रमों में भेजने का निर्णय लेता है । इसके साथ-साथ दल का नेता सी॰ई॰आर॰टी॰/सी॰सी॰ द्वारा आयोजित एक सी॰ एस॰ आईः॰ आर॰ टी॰ का प्रबंधन करना में भी भाग लेता है ।

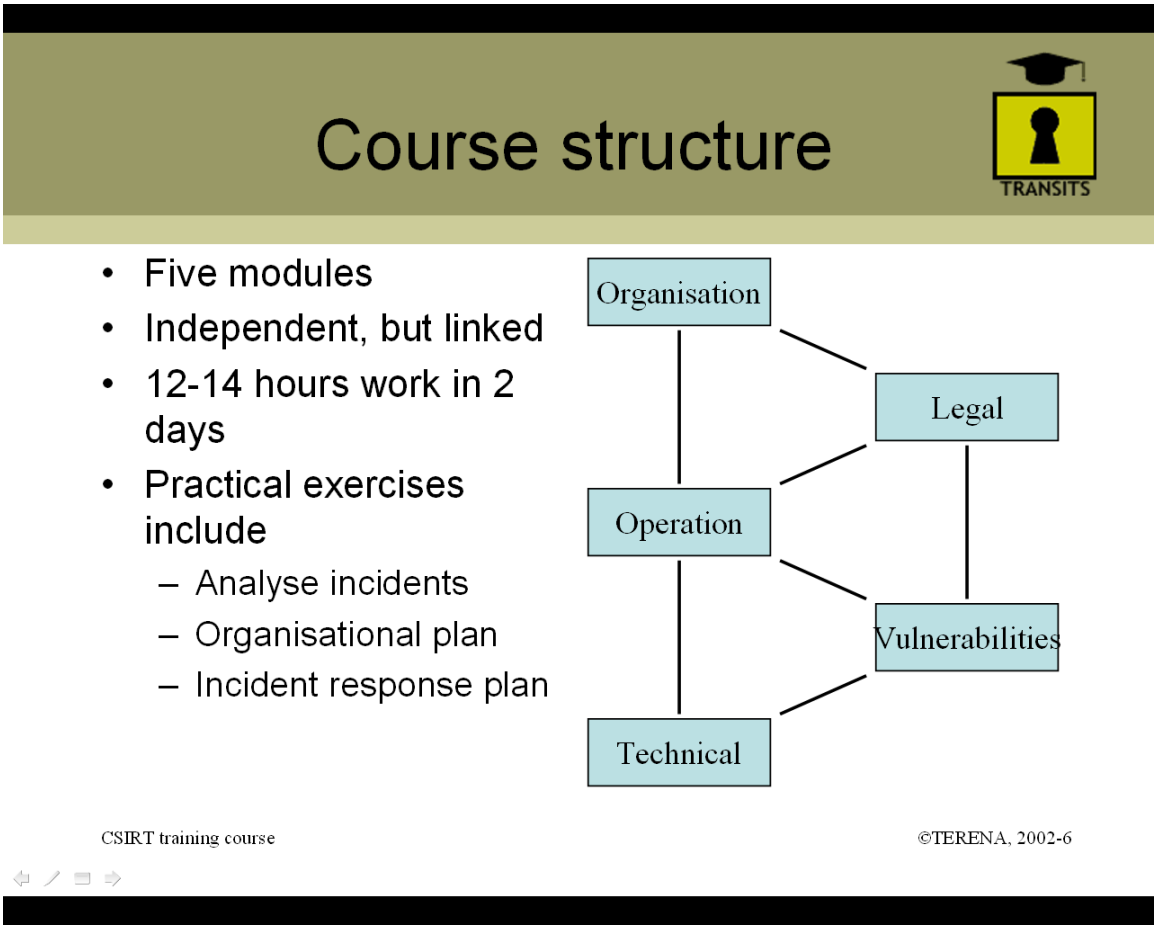
- -

चरण 11 : अभ्यास करना

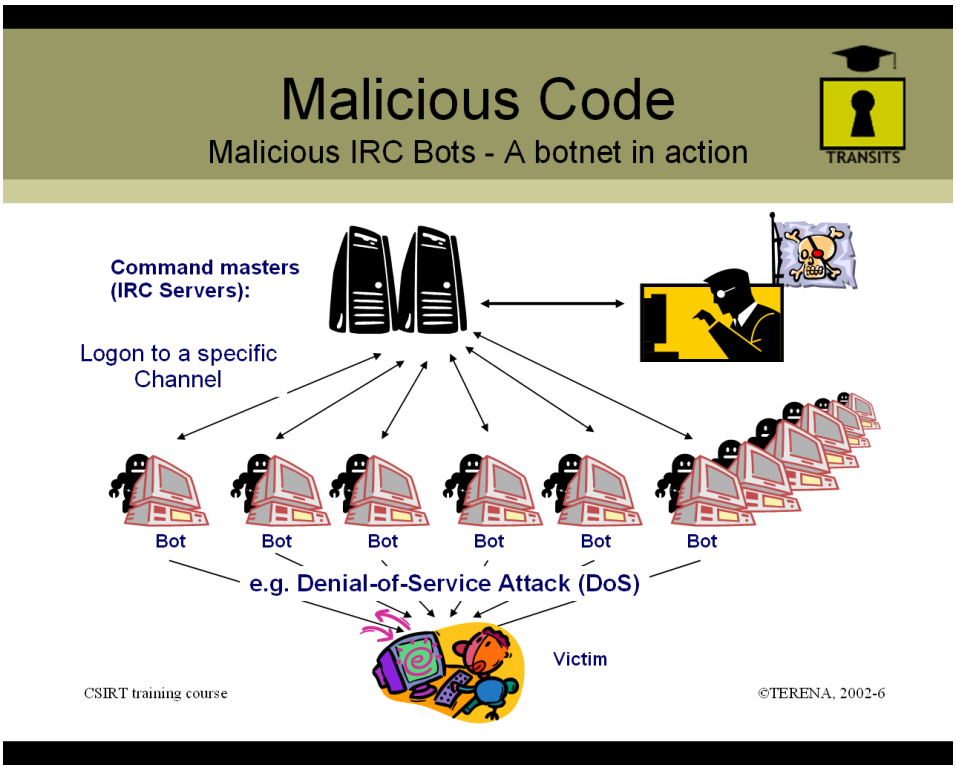
प्रचालन के शुरूआती सप्ताहों के दौरान काल्पनिक सी॰ एस॰ आईः॰ आर॰ टी॰ ने ऐसे कई काल्पनिक मामलों का उपयोग किया (जो उन्हें अन्य सी॰ एस॰ आईः॰ आर॰ टी॰ओं से उदाहरण के तौर पर मिले थे) अभ्यास के दौरान जिनका प्रयोग किया गया था । इसके अलावा उन्होंने अन्य यंत्र और प्रक्रिया सामग्री विक्रेताओं द्वारा वितरित असली संवेदनशीलता जानकारी के आधार पर कुछ सुरक्षा परामर्श जारी किये जिन्हें उन्होंने अपने चुनाव-क्षेत्र की ज़रूरतों के अनुसार ठीक व समायोजित किया ।

क.4 सी० एस० आई० आर० टी० पाठ्यक्रमों से प्राप्त नमूना सामग्री

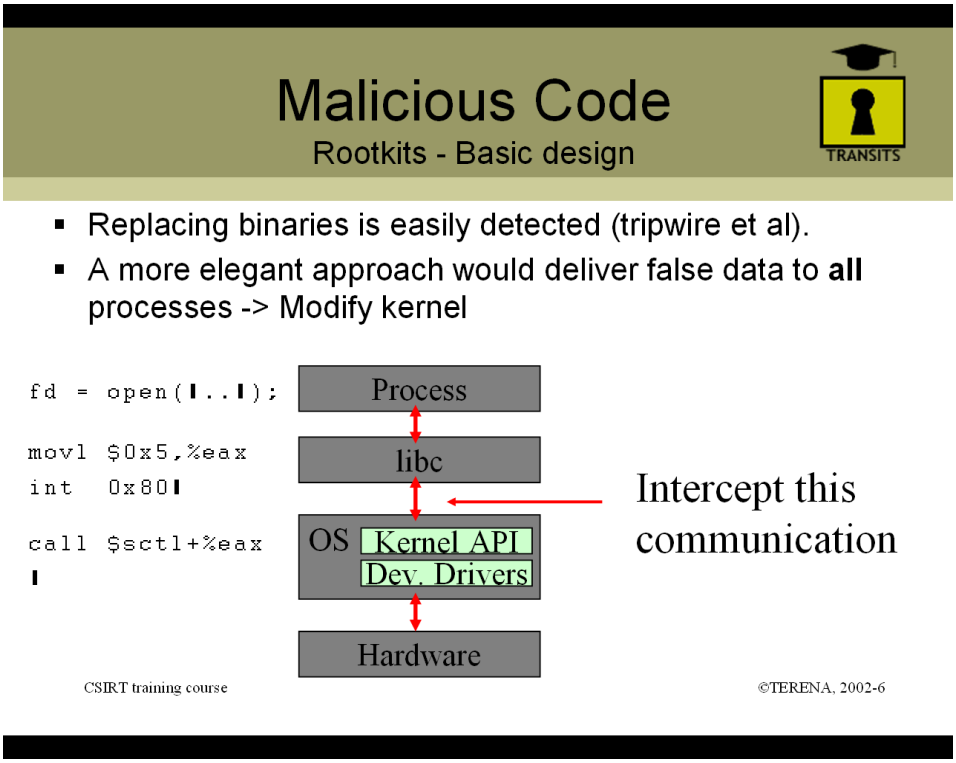
ट्रान्ज़िट्स (टेरेना की अनुमति से, http://www.terena.nl)



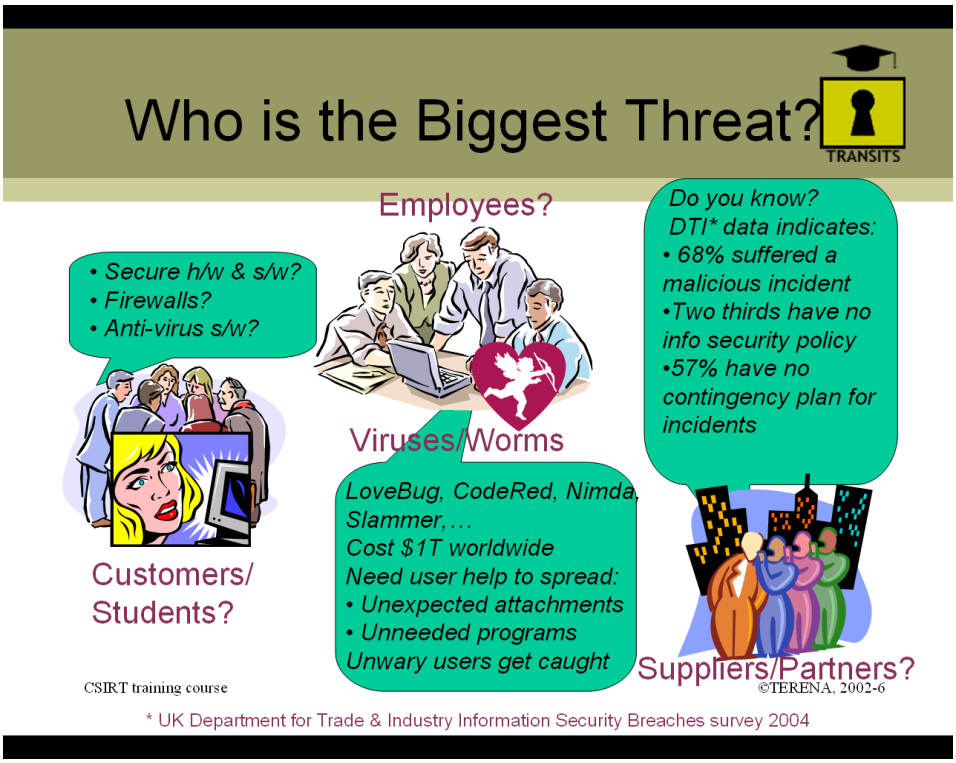
सिंहावलोकन : पाठ्यक्रम का ढांचा



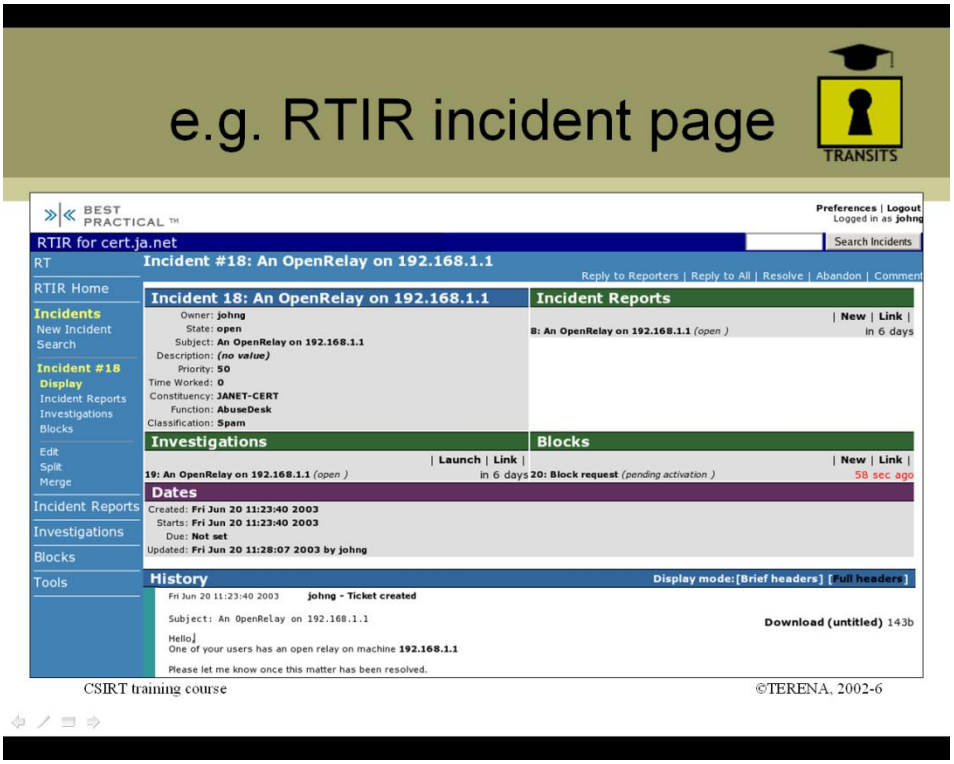
तकनीकी मॉड्यूल : एक बॉटनेट के विवरण से



तकनीकी मॉड्यूल : एक रूटकिट का मूल डिज़ाइन से



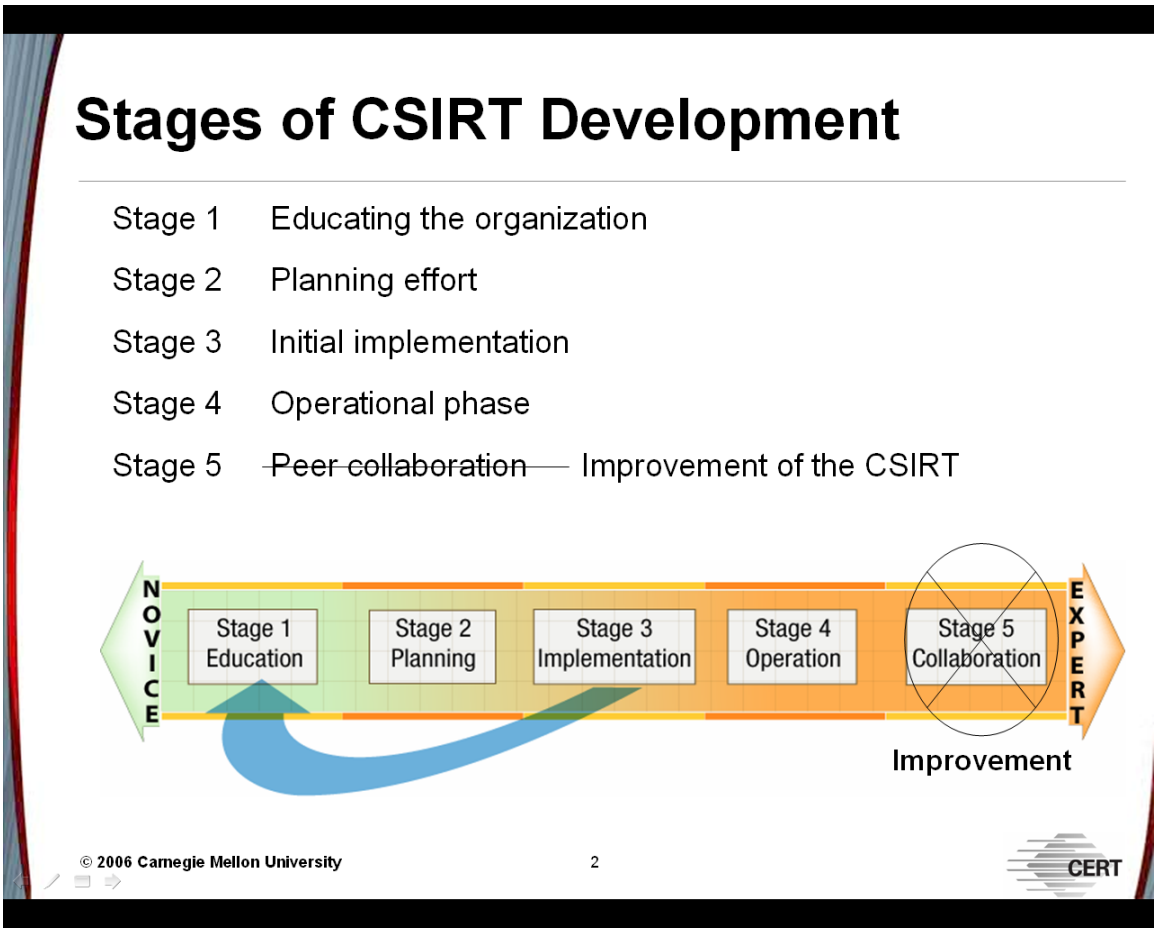
संस्थानात्मक मॉड्यूल : आंतरिक या बाह्य - बड़ा ख़तरा कहाँ से है ?



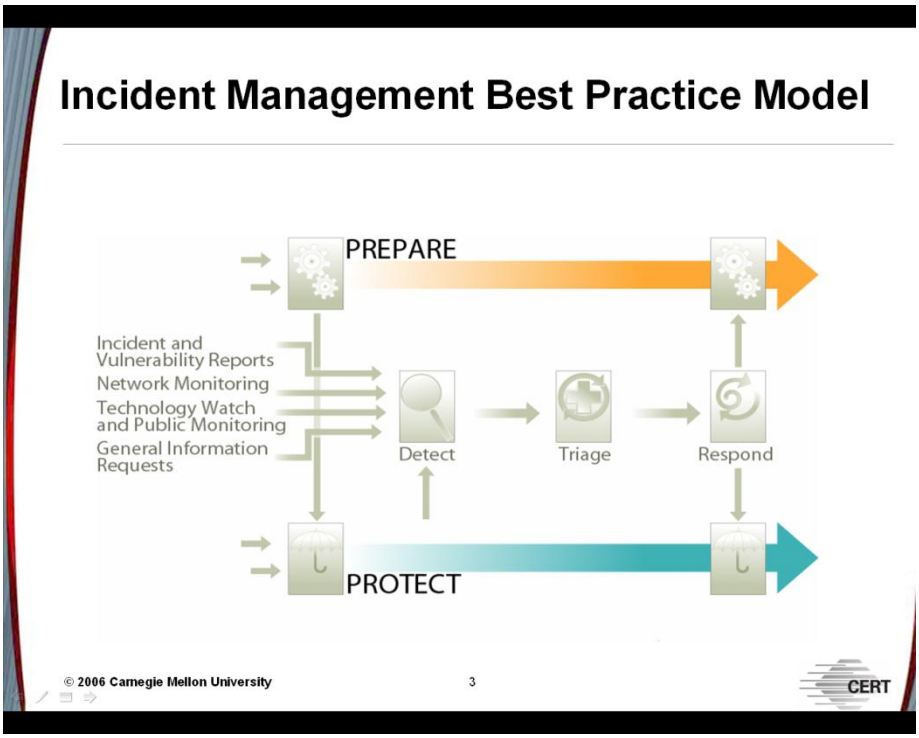
प्रचालन ट्रैक : ट्रैकर को घटना का प्रत्युत्तर देने का निवेदन करें (आर०टी०आई०आर) से

"सी० एस० आई० आर० टी० स्थापित करना" (सी०ई०आर०टी०/सी०सी० की अनुमति से, http://www.cert.org)

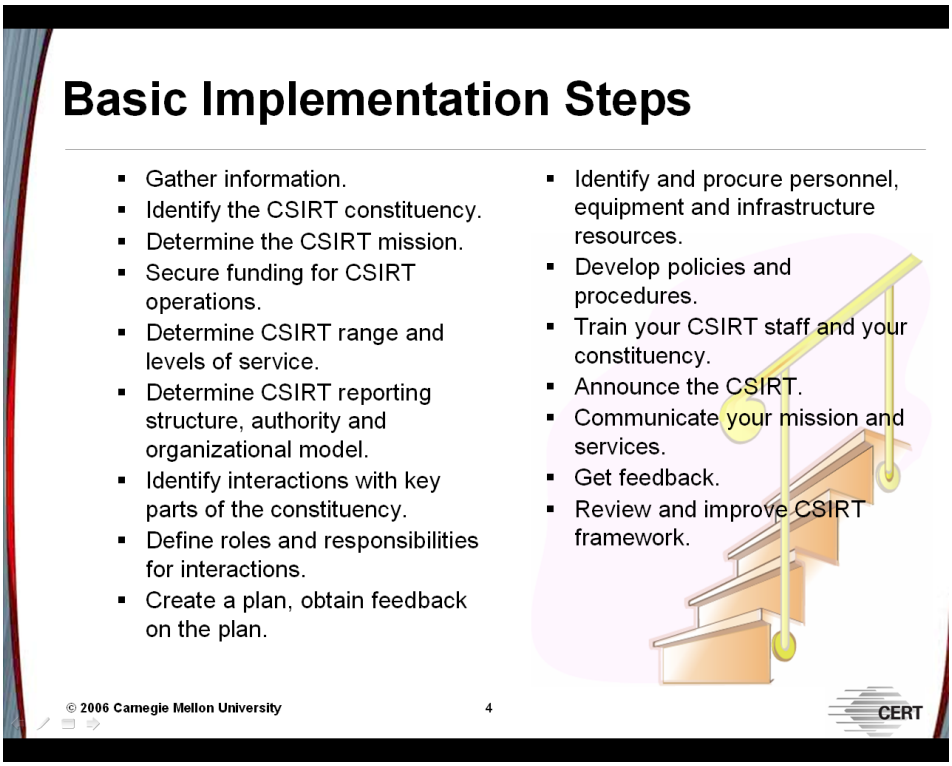
एनीसा सी०ई०आर०टी० कार्यक्रम में सी० एस० आई० आर० टी० विकास दल का आभार प्रकट करती है कि उन्होंने हमें अपने प्रशिक्षण कार्यक्रमों की अंतर्वस्तु का प्रयोग करने की अनुमति दी!



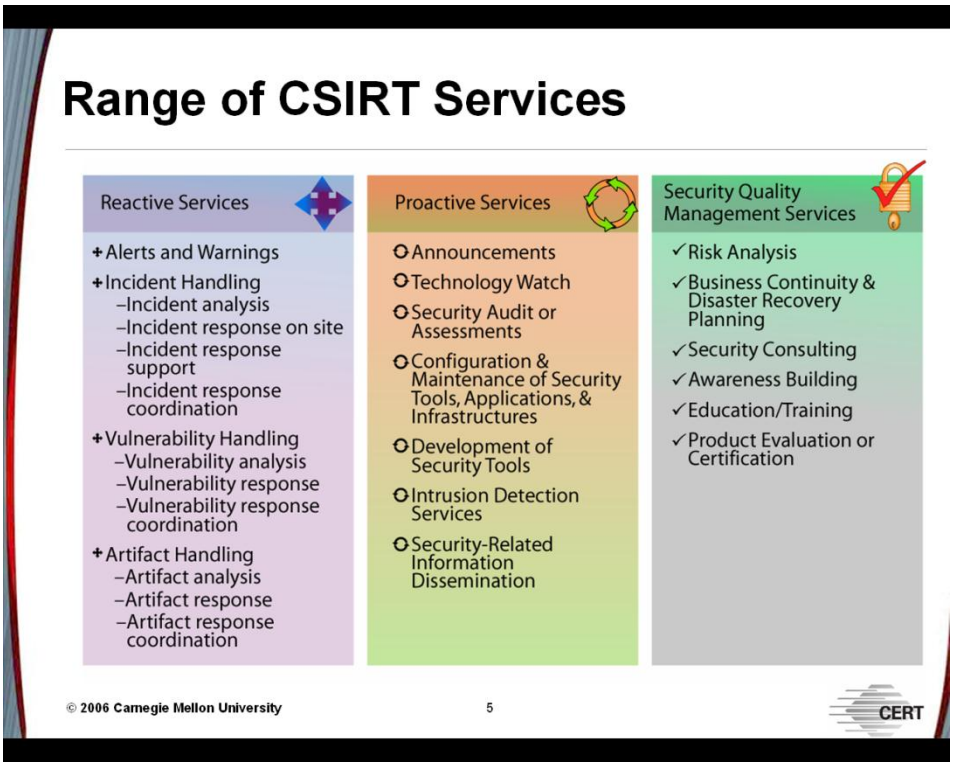
सी०ई०आर०टी०/सी०सी० प्रशिक्षण कार्यक्रम : सी० एस० आई० आर० टी० विकास के चरण से



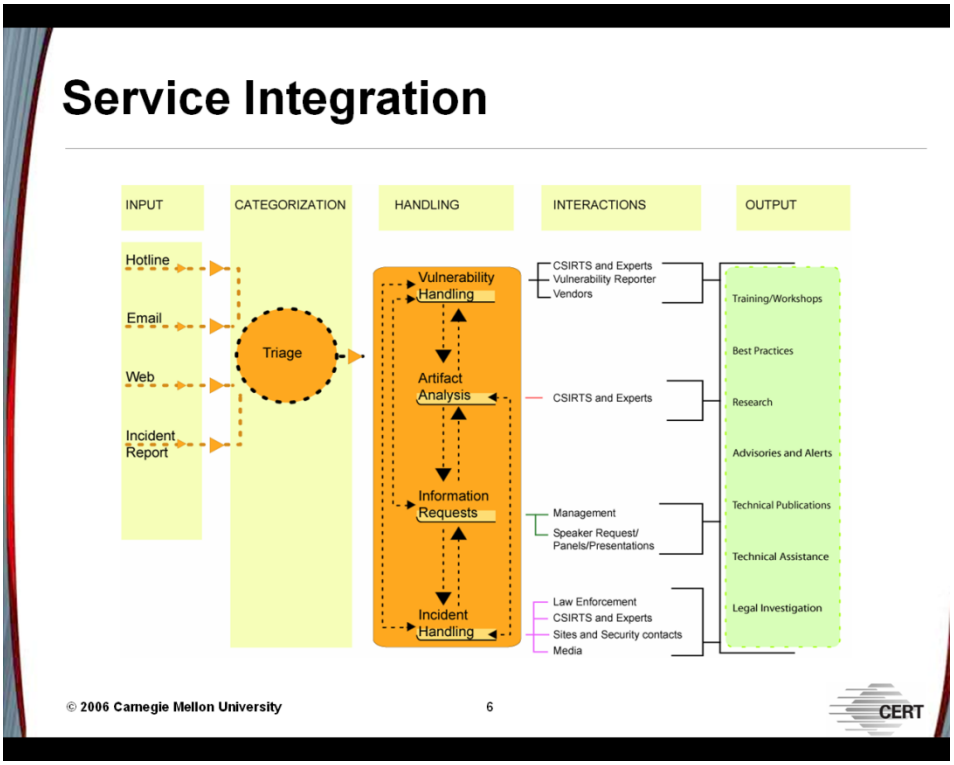
सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : घटना-प्रबंधन के क्षेत्र में बेहतरीन अभ्यास से



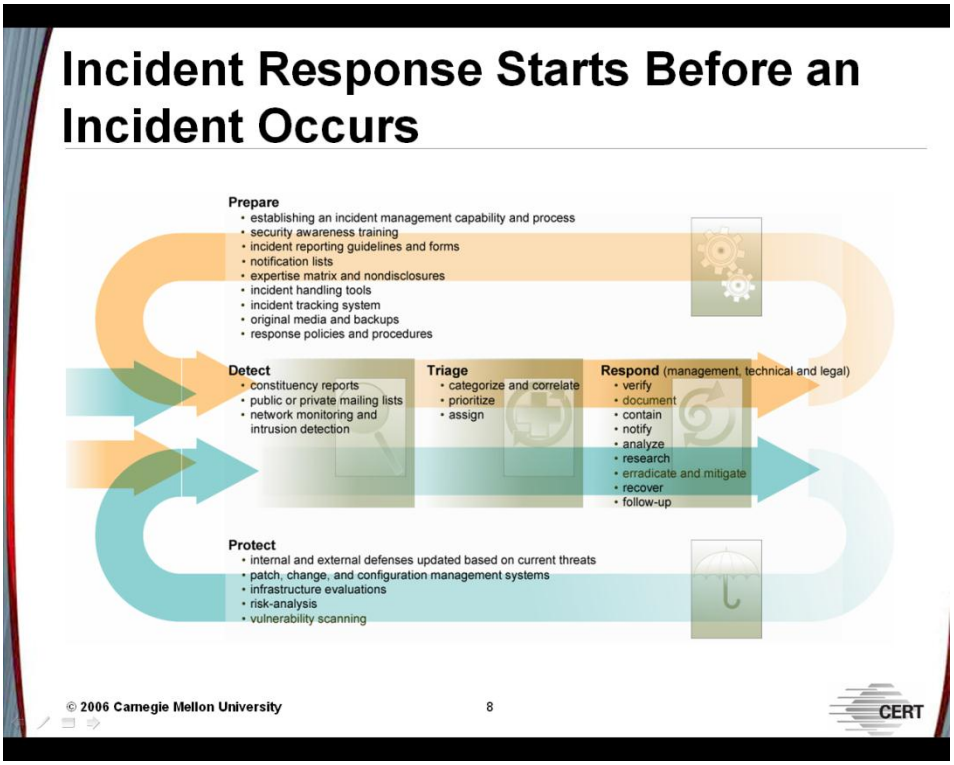
सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : सी० एस० आई० आर० टी० स्थापित करने समय जिन चरणों का अनुसरण करना है से



सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : सी० एस० आई० आर० टी० द्वारा प्रदान की जा सकने वाली सेवायें से



सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : घटना प्रबंधन कार्य-प्रवाह से

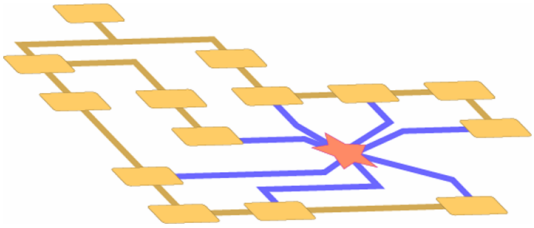


सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : घटना का प्रत्युत्तर से

Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

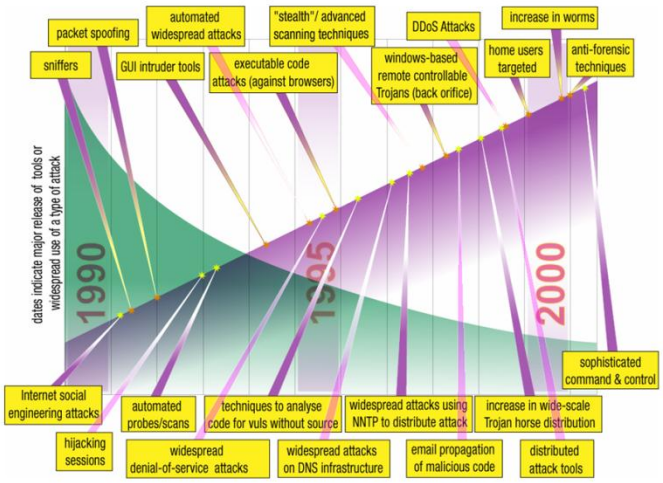
You need to envision a model that can be implemented.



 7 CERT

सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : सी०एस०आई०आर०टी० कैसे व्यवस्थित किया जाएगा ? से

Attack Sophistication versus Required Intruder Knowledge



 9 CERT

सी०ई०आर०टी०/सी०सी० प्रशिक्षण पाठ्यक्रम : कम ज्ञान, अधिक नुक्सान से