अध्याय 4 – आईटी सुरक्षा की समीक्षा

लेखापरीक्षा उद्देश्य 3

आईटी सुरक्षा तंत्र की समीक्षा यह सुनिश्चित करने के लिए कि यह सभी व्यवसाय की महत्वपूर्ण जानकारी और आईटी परिसंपत्ति को हानि, क्षति या दुरूपयोग से उचित रूप से बचाने में सक्षम है।

आपदा बहाली योजना (डीआरपी)/व्यवसाय निरंतरता योजना (बीसीपी) की समीक्षा, आकस्मिक परिस्थितियों की स्थिति में संस्था के व्यवसाय में निरंतरता सुनिश्चित करने के लिए।

कर्मीदल प्रबंधन प्रणाली भाड़ा संचालन सूचना प्रणाली (एफओआईएस) का भाग है, जिसमें एफओआईएस के अन्य मॉड्यूल/एप्लीकेशन्स से इंटरफेस हैं और विभिन्न रेलगाड़ियों के लिए कर्मीदल की बुकिंग और तैनाती, रेल संचालन के लिए कर्मीदल की सक्षमता की पुष्टि जैसे महत्वपूर्ण कार्य कवर करता है और महत्वपूर्ण डेटा कैप्चर कर लेता है जो सुरक्षित रेल संचालन के लिए बहुत महत्वपूर्ण हैं। इसके अलावा, सीएमएस कर्मीदल के विभिन्न भत्तों से संबंधित डेटा भी व्यवस्थित रखता है। इस प्रकार यह महत्वपूर्ण है कि पर्याप्त निवारक, खोजी और सुधारात्मक उपाय अपनाये जाएं ताकि सीएमएस की गोपनीयता, अखंडता; उपलब्धता सुरक्षित की जा सके और सुरक्षित, सुगम, समय पर और निरंतर रेल संचालन सुनिश्चित किया जा सके।

रेलवे बोर्ड ने अप्रैल/मई 2008 में अपनी बेसलाइन आईटी सुरक्षा नीति बनाई जिसके अंतर्गत क्रिस/जोनल रेलवे/एकल इकाईयों द्वारा सहायक प्रक्रिया और निर्देश निकाले जाने थे। बेसलाइन आईटी सुरक्षा नीति आईटी सुरक्षा के विभिन्न पहलुओं को सम्बोधित करती हैं जिसमें पर्यावरण और स्थान सुरक्षा, उपकरण सुरक्षा, भौतिक अभिगम नियंत्रण, डेटा अभिगम अधिकार, प्रयोगकर्ता पहचान और विशेषाधिकार प्रबंधन, पासवर्ड प्रबंधन, व्यवसाय निरंतप्ता योजना, डेटा बैकअप, एप्लीकेशन विकास और रखरखाव सुरक्षा, वायरस और दुर्भावपूर्ण सॉफ्टवेयर के प्रति सुरक्षा, इंटरनेट/ई-मेल सुरक्षा, सॉफ्टवेयर और पैच प्रबंधन आदि शामिल हैं।

लेखापरीक्षा ने देखा कि आरबी की बेसलाइन सुरक्षा नीति के बाद, 13 जोनल रेलवे[63] में सीएमएस से संबंधित कोई भी आईटी सुरक्षा नीति या सहायक प्रणाली और निर्देश तैयार नहीं किये गये। उत्तर में, उरे, पूरे, दपूमरे और दपूरे ने कहा कि मामला क्रिस/सीएओ (एफओआईएस) कार्यालय से संबंधित है।

तथापि, सीएमएस एप्लीकेशन सुरक्षा की लेखापरीक्षा आईआर की बेसलाइन आईटी सुरक्षा नीति/क्रिस सूचना सुरक्षा नीति को ध्यान में रखते हुये व्यापक रूप से की गई थी। इस संबंध में लेखापरीक्षा निष्कर्ष निम्नलिखित प्रकार हैं:

4.1 भौतिक अभिगम नियंत्रण

प्रणाली के भौतिक जोखिमो में भौतिक क्षति, सूचना की चोरी तथा प्रकटन/कॉपी करना शामिल है। आईटी प्रणाली का भौतिक नियंत्रण आईटी प्रणाली या उनके खराब होने के लिए अप्राधिकृत पहुंच से बचाव सुनिश्चित करता है।

आईआर की बेसलाइन आईटी सुरक्षा प्रणाली के अनुसार, कम्प्यूटर रूम प्रतिबंधित क्षेत्र होना चाहिये, परिसर में केवल अधिकृत व्यक्ति को प्रवेश करने की अनुमति होनी चाहिये और उचित अभिगम प्रणाली होनी चाहिये। कम्प्यूटर रूम में सभी आंगतुकों के रेलवे स्टाफ के प्राधिकृत सदस्य द्वारा हमेशा निगरानी की जानी चाहिये।

12 जोनल रेलवे[64] की विभिन्न लॉबियों के दौरे के दौरान, यह देखा गया कि लॉबियों में अनाधिकृत व्यक्तियों के प्रवेश रोकने और पता लगाने और चोरी/क्षति से आईटी परिसंपत्तियों को बचाने के लिए पर्याप्त उपाय[65] नहीं अपनाये गये थे। विभिन्न जोनों में, सीसीटीवी कैमरों जैसे खोजी सुरक्षा उपाय या तो लगाये ही नहीं गये थे या उनकी अपर्याप्त संख्या लगाई थी जैसाकि ***परिशिष्ट XXV*** में विस्तृत रूप से दिया गया है।

उत्तर में (सितम्बर 2015), आरबी ने कहा कि जोनल रेलवे को आवश्यक निर्देश जारी कर दिये गये है।

---

[63] *दरे, मरे, उपरे, उरे, पूरे, उपूरे, दपरे, उमरे, दपूमरे, पमरे, दमरे, परे और दपूरे*

[64] *प.रे, द.प.रे, पू.रे, द.रे, द.पू.रे, उ.प.रे, द.म.रे, पू.त.रे, उ.म.रे, उ.पू.रे, पू.म.रे,एवं प.म.रे*

[65] *इलैक्ट्रॉनिक दरवाजे का ताला, बायो मेट्रिक दरवाजे का ताला, स्वाइप कार्ड, सुरक्षा गार्ड आदि।*

सीएमएस प्रयोगकर्ता: सीएमएस का प्रयोग विभिन्न स्तरों पर विभिन्न प्रयोगकर्ताओं, जिन्हें विभिन्न सुविधाएं प्राप्त है, के द्वारा किया जाता है। यह मुख्यत: प्रणाली प्रशासक, डेटाबेस प्रशासक, डेटाबेस प्रयोगकर्ता और सॉफ्टवेयर (एप्लीकेशन) अभिगम प्रयोगकर्ता द्वारा प्रयोग किया जाता है। सॉफ्टवेयर एप्लीकेशन अभिगम प्रयोगकर्ताओं में लॉबी के लिए पर्यवेक्षक प्रयोगकर्ता बनाने हेतु मुख्य प्रयोगकर्ता, लॉबी के लिए रेलगाड़ी क्लर्क (टीएनसी) प्रयोगकर्ता बनाने हेतु और साइन ऑन/ऑफ अनुमोदित करने के लिए पर्यवेक्षक प्रयोगकर्ता (लोको/ट्रैफिक), विभिन्न यातायात परामर्श पर कर्मीदल की बुकिंग हेतु टीएनसी प्रयोगकर्ता और क्योस्क के लिए कर्मीदल कंसोल प्रयोगकर्ता जो प्रत्येक कर्मीदल कंसोल प्रयोगकर्ता को उसका व्यक्तिगत विवरण देखते हुये साइन ऑन/ऑफ के लिए क्योस्क के माध्यम से सीएमएस अभिगम के लिए सक्षम करता है आदि शामिल हैं।

आईआर की बेसलाइन आईटी सुरक्षा नीति के अनुसार, प्रत्येक यूजर आईडी को विशेष रूप से एक ही उपयोगी को पहचानना चाहिये। ग्रुप या साझे यूजर आईडी नहीं बनाने चाहिये जब तक आईटी विभाग, सुरक्षा प्रबंधक द्वारा स्पष्ट रूप से अनुमत और अनुमोदित न हो। प्रत्येक पासवर्ड में न्यूनतम लंबाई, प्रतिबंधित शब्द/फार्मेट होना चाहिए और अन्य प्रतिबंधों के बीच वैध अवधि होनी चाहिए। सभी सूचना प्रणाली लाभ उस समय वापस लेने चाहिए जब सदस्य का स्थानांतरण होगा या रेलवे की सेवा समाप्त हो जाती है। इसके अतिरिक्त, डेटा अभिगम अधिकार जानने की आवश्यकता के आधार पर दिये जायेंगे। इस संबंध में, लेखापरीक्षा निष्कर्ष निम्नलिखित प्रकार हैं:

4.2 तार्किक अभिगम नियंत्रण- पासवर्ड नीति

अनधिकृत पहुंच के प्रति कम्प्यूटर स्रोतों (डेटा, प्रोग्राम आदि) को सुरक्षित करने के लिए लक्षित साफ्टवेयर नियंत्रण के रूप में एक सिस्टम को तार्किक पहुंच नियंत्रण के रूप में वर्गीकृत किया जाता है। इस संदर्भ में, लेखापरीक्षा में निम्नलिखित मामले देखे गए:

पासवर्ड नीति

क्रिस की आईएस सुरक्षा (पासवर्ड) नीति के अनुसार, पासवर्ड की लम्बाई प्रयोगकर्ता एकाउंट के लिए न्यूनतम छह अक्षर तथा प्रशासक

एकाउंट के लिए 10 अक्षर होनी चाहिए तथा अपर केस और लोवर केस अक्षरों, अंकों तथा स्वीकृत विशेष अक्षरो का एक संयोजन होना चाहिए।

- नमूना जांच से पता चला कि सीएमएस ने न तो लोवर/अपर केस अक्षर, अंक और विशेष अक्षर वाला पासवर्ड सुनिश्चित किया न ही प्रणाली प्रशासक/डेटाबेस प्रयोगकर्ता के लिए न्यूनतम 10 अंक का पासवर्ड सुनिश्चित किया और '123456' जैसा न्यूनतम छः अंक का सामान्य पासवर्ड स्वीकार किया। एप्लीकेशन स्तर पर, सीएमएस ने प्रथम लॉगइन में पासवर्ड के परिवर्तन तथा पासवर्ड के आवधिक परिवर्तन का दबाव दिए बिना एकल अक्षर प्रयोगकर्ता आईडी के साथ पासवर्ड स्वीकृत किया और सिस्टम के लॉगइन/अभिगम में कर्मीदल को सक्षम बनाया।
- विभिन्न प्रकार के प्रयोगकर्ताओं से संबंधित डेटा के विश्लेषण से निम्नलिखित का पता चला:

प्रयोगकर्ता का प्रकार	विवरण
कर्मीदल कंसोल प्रयोगकर्ता (ड्राइवर/गार्ड)	सभी जोनल रेलवे के 11.91 प्रतिशत से 100 प्रतिशत के बीच प्रयोगकर्ता समान पासवर्ड का प्रयोग कर रहे थे, यद्यपि यह कूट रूप से डिफॉल्ट पासवर्ड था।
लोको निरीक्षक/ वरिष्ठ लोको निरीक्षक/ मुख्य लोको निरीक्षक	सभी जोनल रेलवे के 74.01 प्रतिशत (दपूम) और 98.53 प्रतिशत (पूरे) के बीच प्रयोगकर्ता एक ही पासवर्ड का प्रयोग कर रहे थे।
सीएमएस प्रयोगकर्ता (पर्यवेक्षक/टीएनसी)	सभी जोनल रेलवे के 36.68 प्रतिशत और 87.82 प्रतिशत के बीच प्रयोगकर्ता एक ही पासवर्ड का प्रयोग कर रहे थे।

इस तथ्य को ध्यान में रखते हुये कि आईडी सभी को दिखाई देती है और पासवर्ड का आसानी से अनुमान लगाया जा सकता है, प्रोक्सी प्रयोगकर्ता द्वारा अनाधिकृत अभिगम/लॉग इन की संभावना को समाप्त नहीं किया जा सकता इसके अतिरिक्त जैसा कि रिपोर्ट में पैराग्राफ 2.5.4.5 के अंतर्गत उल्लिखित तथ्यों से स्पष्ट है कि कर्मीदल अपनी अनुपस्थिति के दौरान लॉग इन पाया गया था।

इस प्रकार, आईआर की बेसलाइन आईटी सुरक्षा नीति/क्रिस सूचना सूरक्षा नीति में निर्धारित मूल सुरक्षा उपायों को सीएमएस संसाधनों की सुरक्षा और संरक्षा सुनिश्चित करने के लिए नहीं अपनाया गया था।

उत्तर में (सितम्बर 2015), आरबी ने सुधारात्मक कार्यवाही हेतु लेखापरीक्षा निष्कर्षों को स्वीकार किया।

(अनुबंध – 35, 36, 37)

4.3 खराब प्रयोगकर्ता प्रोफाइल प्रबंधन

प्रशासनिक/पर्यवेक्षी विशेषाधिकार अवास्तविक(डमी) प्रयोगकर्ताओं को दिए गए थे। दिए गए विशेषाधिकार प्रयोगकर्ताओं की आवश्यकता व पदनाम के अनुरूप नहीं थे, पर्यवेक्षी विशेषाधिकारों से समझौता किया गया तथा इसके परिणामस्वरूप डेटा सत्यनिष्ठा की हानि/सिस्टम का दुरूपयोग तथा कर्मीदल की गलत बुकिंग हो सकती है। सीएमएस प्रयोगकर्ता अस्पष्ट/लॉबी नाम में बनाये गये थे और आउटसोर्सड स्टाफ को अलग से यूजर आईडी नहीं दिया गया था। इससे वास्तविक व्यक्ति जिसने डेटा बनाया था, उसको पहचानने की विफलता, सीएमएस के गलत संचालन के लिए जिम्मेदारी निर्धारित करने में विफलता हो सकती है। लेखापरीक्षा निष्कर्षों/इस संबंध में देखी गई अनियमितताओं के उदाहरण निम्नलिखित प्रकार हैं:

- **आउटसोर्सड स्टाफ को अनियमित विशेषाधिकार:** दरे में कर्मीदल बुकिंग लॉबियों[66] में सीएमएस में अनुबंधात्मक आउटसोर्सड एजेंसी के माध्यम से डेटा डाला गया जबकि आउटसोर्सड स्टाफ को पृथक प्रयोगकर्ता आईडी व पासवर्ड आवंटित नहीं किया गया था। प्रत्येक सीएमएस प्रयोगकर्ता द्वारा सामान्य प्रयोगकर्ता आईडी तथा पासवर्ड को शेयर किया गया था।
- दमरे में, 1,16,383 मामलों में व्यक्ति जिसने कर्मीदल को बुक किया था, उसी ने पर्यवेक्षण स्वीकृति भी दी थी। जो यह दर्शाता है कि अधिकतर मामलों में बाहरी स्टाफ द्वारा पर्यवेक्षण स्वीकृति मंजूर की जा रहीं थी जो निर्धारित प्रक्रियाओं के विपरीत तथा इसलिए अनियमित थी।

[66] *तम्बरम, चेन्नई इग्मोर, चेन्नई सेन्ट्रल, टीरूवोट्टीयुर, अराक्कोनम तथा जोलरपेट्टई*

- पूरे में, जांच की गई लॉबियों के बाहरी स्टाफ सहित सारे स्टाफ ने सामान्य प्रयोगकर्ता आईडी तथा पासवर्ड का उपयोग किया।

- **रेलवे सीएमएस प्रयोगकर्ता को अनियमित विशेषाधिकार:** डेटा विश्लेषण के दौरान, लेखापरीक्षा ने विभिन्न जोनों में देखा कि प्रशासिनक/पर्यावेक्षीय विशेषाधिकार गैर-वर्तमान/ अवास्तविक (डमी) रेलवे प्रयोगकताओं को दिये गये थे या दिये गये अधिकार प्रयोगकर्ता के पद के अनुसार नहीं थे। प्रयोगकर्ता अस्पष्ट/लॉबी नाम में बने हुये पाये गये थे जो वास्तविक प्रयोगकर्ता की पहचान प्रकट नहीं करते थे। ***(परिशिष्ट - XXVI)***

(अनुबंध - 38)

- **पर्यवेक्षी आईडी का उपयोग करते हुए सीएमएस प्रयोगकर्ताओं द्वारा निष्पादित विभिन्न भूमिकाऐं/कार्य**

  क्रिस के सीएमएस दस्तावेजीकरण के अनुसार रेलगाड़ी लिपिक व पर्यवेक्षक को भिन्न भूमिकाएं प्रदान की गई है तथा इसे वास्तविक प्रयोगकर्ताओं द्वारा निष्पादित करना अपेक्षित होता है।

- सीएमएस प्रयोगकर्ता नियमावली के अनुसार, कर्मीदल के साइन ऑन/ऑफ गतिविधि को स्वीकृत करने के पर्यवेक्षी कार्य को कर्मीदल पर्यवेक्षक द्वारा किया जाना है। कर्मीदल कॉलिंग, बुकिंग तथा उनके साइन के अनुमोदन से संबंधित डेटा के विश्लेषण से पता चला कि 11 जोनल रेलवे[67] में, 2071319 मामलों में से 669393 मामलों में, कॉलिंग लिपिक, बुकिंग लिपिक तथा पर्यवेक्षक की उपयोगकर्त्ता आईडी एक ही पाई गई।

(अनुबंध - 39)

- उरे के दिल्ली मंडल के लॉबी दौरे के दौरान यह देखा गया कि एकीकृत[68] प्रयोगकर्ता आईडी को सीएमएस प्रचालन के लिए बनाया गया था तथा अधिकांश लॉबियों में सहायक लोको पॉयलट/लोको पायलट शंटर (एएलपी/एलपीएस) कर्मीदल बुकिंग तथा उनके साइन ऑन/साइन ऑफ को स्वीकृत करने हेतु अपने कर्मीदल

[67] *पूरे, उरे, उपरे, परे, पूसीरे, मरे, दमरे, दपूरे, दपूमरे, दरे, उमरे*

[68] *उपयोगकर्ता जिसके पास पर्यवेक्षीय कार्य और ट्रेन लिपिक कार्य का विशेषाधिकार हो*

नियंत्रक/पर्यवेक्षक की एकीकृत[69] प्रयोगकर्ता आईडी तथा पासवर्ड का उपयोग कर रहे थे। दरे, दपरे तथा अन्य जोनल रेलवे में भी यही स्थिति देखी गई।

इस प्रकार, वास्तविक प्रयोगकर्ता द्वारा पर्यवेक्षी कार्यो का निष्पादन न करना सीएमएस के परिचालनों पर प्रभाव डाल सकता था जैसाकि पैराग्राफ संख्या 2.5.4.5, 3.1 आदि में बताया गया है तथा इससे सिस्टम की सुरक्षा से भी समझौता किया गया, जिससे रेल संचालन में जोखिम हो सकता है।

- **विविध यूजर आईडी (विभिन्न प्रोफाइल) बनाना और सीएमएस एप्लीकेशन प्रयोगकर्ता अकाउंट का निष्क्रियकरण न करना**

सीएमएस प्रयोगकर्ता डेटा के विश्लेषण के साथ-साथ लॉबी में सीएमएस संचालन/अभिलेखों की संवीक्षा से पता चला कि प्रयोगकर्ताओं के पास विविध आईडी थे, प्रयोगकर्ता आवश्यकता से अधिक बनाये गये थे, पूर्व अधिकारी सीएमएस प्रयोगकर्ता के रूप में सक्रिय थे जैसा कि ***परिशिष्ट XXVII*** में दिये गये विवरण से स्पष्ट है।

इस प्रकार, प्रयोगकर्ता का डेटाबेस समय पर अपडेट नहीं किया गया है और पूर्व अधिकारियों के आईडी के प्रयोग से दुरूपयोग हो सकता है।

4.4 डेटाबेस प्रशासक (डीबीए) के कार्यों की निगरानी न करना/लेखापरीक्षा ट्रेल का अभाव

सीएमएस विकास और रखरखाव कार्य नई दिल्ली में क्रिस, सीएमएस समूह, द्वारा किया जाता है, जिसमें अन्य कार्यों के साथ, एप्लीकेशन की प्रोग्रामिंग, सॉफ्टवेयर के विकास/बदलाव की जांच, डेटाबेस का प्रबंधन/डेटाबेस अपडेट करना, प्रयोगकर्ताओं का प्रबंधन आदि शामिल होता हैं।

लेखापरीक्षा को उपलब्ध कराई गई सूचना के अनुसार, सात प्रयोगकर्ताओं के पास डीबीए विशेषाधिकार थे। इसके अलावा, 40 क्रिस प्रयोगकर्ताओं के पास एप्लीकेशन स्तर पर प्रशासनिक विशेषाधिकार थे तथा उनमें से एक के पास कई आईडी के साथ प्रशासनिक विशेषाधिकार थे। डीबीए विशेषाधिकार वाले प्रयोगकर्ता सीएमएस तालिकाओं तक पहुंच सकते हैं तथा उनकी गतिविधियों की किसी मॉनीटरिंग के बिना डेटाबेस में

[69] *उपयोगकर्ता जिसके पास पर्यवेक्षक और ट्रेन लिपिक (टीएनसी) का विशेषाधिकार हो*

बैकएंड से कर सकते हैं क्योंकि न तो डीबीए की गतिविधियों की मॉनीटरिंग के लिए किसी लॉग/लेखापरीक्षा ट्रायल को अनुरक्षित किया गया न ही एकल व्यक्ति तक पहुंच को प्रतिबंधित करने जैसे अन्य उपायों को डेटाबेस में किसी अनधिकृत तथा न पता लगने वाले परिवर्तनों से बचाने के लिए अपनाया गया।

अपेक्षित लॉग/लेखापरीक्षा ट्रायल अथवा अन्य सुधारात्मक उपायों (पहुंच प्रतिबंधित करने जैसे) के अभाव के परिणामस्वरूप प्रशासनिक विशेषाधिकारो वाले प्रयोगकर्ताओं की अनाधिकृत गतिविधियों को मॉनीटर करने/उनका पता लगाने में विफलता होगी।

उत्तर में (सितम्बर 2015) आरबी ने क्रिस की टिप्पणी को समर्थित किया कि लेखापरीक्षा निष्कर्षों को आवश्यक कार्यवाही हेतु नोट कर लिया गया है।

4.5 एंटी वायरस और ऑपरेटिंग सिस्टम के पैचेज को संस्थापित/अपडेट न करना

क्रिस की आईएस नीति के अनुसार, संबंधित समूहों के सिस्टम प्रशासक/प्रयोगकर्ताओं को यह सुनिश्चित करना चाहिए कि उनके द्वारा प्रबंधित सर्वर तथा अन्य घटकों में उचित एन्टी वायरस सॉफ्टवेयर[70] तथा नवीनतम परिचालन सिस्टम (ओएस) पैचेज[71] को संस्थापित किया गया है। इसके अतिरिक्त, आईआर बेसलाइन आईटी सुरक्षा नीति के अनुसार, व्यक्तिगत कम्प्यूटर और आंतरिक नेटवर्क से जुड़े कम्प्यूटरों में रिमोट एक्सेस चैनल द्वारा एंटीवायरस को हमेशा चालू रखना चाहिये और नियमित रूप से अपडेट करना चाहिये।

- 2 मार्च 2015 को सीएमएस की समीक्षा से पता चला कि विंडो ओएस आधारित सर्वरों में अपडेटेड एन्टी–वायरस सॉफ्टवेयर नहीं था। (24 फरवरी 2015 को अंतिम बार अपडेट किया गया था)।

[70] ***एंटी वायरस या एंटीवायरस सॉफ्टवेयर कम्प्यूटर सॉफ्टवेयर हैं जो, गलत सॉफ्टेवयर को रोकने, पहचानने और हटाने के लिये प्रयोग किया जाता हैं।***

[71] ***पैच एक सॉफ्टवेयर है जो कम्प्यूटर प्रोग्राम या उसके सहायक डेटा को अपडेट करने, प्रणाली के निष्पादन को सुधारने या समस्या दूर करने के लिये बनाया गया है। इसमें सुरक्षा भेद्यता सही करना भी शामिल है।***

- लीनक्स/एआईएक्स ओएस वाले सर्वरों पर पैचेज को 27 जनवरी 2012 को अंतिम बार अपडेट/संस्थापित किया गया था।
- थिन क्लाइंट/विंडोज आधारित पीसी सीएमएस परिचालनों के लिए विभिन्न जोनों में उपयोग में थे। द.रे में, चयनित कीयोस्क में उपयुक्त एन्टीवायरस सॉफटवेयर का वर्जन (क्वीक हील एन्टी वायरस प्रो 2014) पुराने था तथा उन्हें 4 मई 2014 से अपडेट नहीं किया गया था। द.म.रे में, एन्टी वायरस सॉफ्टवेयर हैदराबाद (एचवाईबी) लॉबी की सीएमएस मशीनों में उपयोग में थे परन्तु सिकंदराबाद (एससी) लॉबी की सीएमएस मशीनों में नहीं। उ.रे की जींद लॉबी में, बुकिंग के लिए उपयुक्त पीसी में एन्टी वायरस का ट्रायल वर्जन था।
- लेखापरीक्षा के लिए चयनित म.रे, पू.रे, पू.त.रे, उ.म.रे, उ.पू.रे, द.पू.रे, उ.प.रे, द.प.रे तथा पू.म.रे में लॉबियो की सीएमएस मशीनों में एन्टी वायरस सॉफ्टवेयर संस्थापित/अपडेट नहीं था।

इस प्रकार, अपडेट एन्टी वायरस सॉफ्टवेयर/अपडेट सॉफ्टवेयर पैचेज की कमी का अनुचित लाभ लिया जा सकता है तथा सीएमएस के सुचारू परिचालनों में विघ्न पड़ता है।

4.6 व्यवसाय निरन्तरता योजना/आपदा बहाली योजना (बीसीपी/डीआरपी) की समीक्षा

बीसीपी/डीआरपी के उत्पादन तथा अनुरक्षण करने का उद्देश्य संगठन की आईटी परिसंपत्ति की अखंडता सुनिश्चित करना तथा महत्वपूर्ण सिस्टमों के अप्रत्याशित अवरोधन से उत्पन्न जोखिमों को कम करना तथा व्यवसायिक गतिविधियों में निरन्तरता लाना है।

सीएमएस प्रणाली का नई दिल्ली में एक केन्द्रीकृत कम्प्यूटर डेटा केन्द्र है जिसका प्रबंधन क्रिस द्वारा 2007-08 से प्रणाली की शुरूआत से ही किया जा रहा है। क्रिस ने सीएमएस की बाधारहित प्रचालन को सुनिश्चित करने के लिए जून 2012 में एक बीसीपी/डीआरपी रखने की प्रक्रिया प्रारम्भ की और जनवरी 2015 की समाप्ति तक, बीसीपी/डीआरपी के क्रियान्वयन का कार्य अभी प्रक्रियाधीन था।

जोनल/मंडलीय/लॉबी स्तर पर, सभी जोनल रेलवे में संरचित और दस्तावेजीकृत बीसीपी/डीआरपी नहीं थी। 24x7 कनेक्टिविटी को

सुनिश्चित करने के लिए रूट एवं मीडिया विविधता/वैकल्पिक संचार माध्यम विभिन्न जोनों की लॉबियों में उपलब्ध नहीं थे। कनेक्टिविटी/लिंक खराबी, सेन्ट्रल सर्वर और सीएमएस क्लाइंट मशीनों के बीच नेटवर्क की धीमी स्पीड विभिन्न जोनों की लॉबियों में अनवरत सीएमएस प्रचालनों की बाधा हेतु मुख्य कारण थी।

कई लॉबियों में वैकल्पिक विद्युत आपूर्ति की व्यवस्था पर्याप्त नहीं थी। अधिकतर लॉबियों में सीएमएस उपस्कर/उपकरणों को एएमसी के अंतर्गत कवर नहीं किया गया था।

विभिन्न लॉबियों में त्रुटिपूर्ण उपस्कर को तत्काल बदलने के लिए चालू स्पेयर उपस्कर/उपकरण उपलब्ध नहीं थे।

अग्नि शमन पुराने हो गए थे/प्रतिष्ठापित नहीं किए गए थे और स्मोक डिटेक्टर/फायर अलार्म प्रणाली प्रतिष्ठापित नहीं की गई थी। ***(परिशिष्ठ -XXVIII)***

रेलवे बोर्ड ने उत्तर (सितम्बर 2015) में क्रिस की टिप्पणी का पृष्ठांकन किया कि लोकल साइट (डेटा सैन्टर/उत्पादन परिवेश) पर उनके आपदा बहाली सेटअप को चालू कर दिया गया है।

रेलवे बोर्ड का उत्तर स्वीकार्य नहीं है क्योंकि क्रिस डीआर योजना के केवल चरण-I को लोकल साइट (अर्थात डेटा सेंटर/उत्पादन परिवेश) पर चालू किया गया है और दूरस्थ स्थान पर डीआर साइट के लिए डीआर योजना के चरण-II को कार्यान्वित नहीं किया गया हैं। चूंकि लोकल डीआर सेटअप (साथ-साथ डेटा सेंटर/उत्पादन परिवेश सेटअप) में कई जोखिमों की संभावना है जो 24x7 आधार पर निरंतर सीएमएस परिचालनों के लिए डीआर साइट रखने के उद्देश्य को प्राप्त नहीं कर सकता, इसलिए दूरस्थ स्थान पर डीआर सेटअप रखने के लिए डीआर योजना के चरण-II के कार्यान्वयन को शीघ्रता से किए जाने की आवश्यकता है।

इसके अलावा, विभिन्न जोनों में पर्याप्त अवसंरचना उपलब्ध कराने और सुधारात्मक एवं निवारक उपायों को अपनाने की आवश्यकता का समाधान नहीं किया गया है जिससे निरंतर सीएमएस सेवाओं में या तो बाधा आती है या आ सकती है।

4.7 सीएमएस डेटा बैकअप का गैर/अनियमित रख-रखाव

क्रिस आईएस नीति के अनुसार, विभिन्न रेलवे परियोजनाओं के निरन्तर परिचालन को सुनिश्चित करने के लिए सभी परियोजनाओं द्वारा डेटा के दूरस्थ/ऑफसाइट बैकअप को अनुरक्षित करना अपेक्षित है। क्रिस का सीएमएस ग्रुप, जो सीएमएस का केन्द्रीकृत डेटाबेस रख-रखाव कर रहा है, के पास डेटा/सूचना की महत्वपूर्णता की पहचान, डेटा के बैकअप हेतु प्रक्रियाओं, डेटा के बैकअप का इसकी एकरूपता सुनिश्चित करने हेतु सत्यापन तथा समय पर बहाली, ऑनसाइट/ऑफसाइट डेटा बैकअप की सुरक्षा, बैकअप डेटा के अनुरक्षण की अवधि आदि जैसे मामलों को सम्बन्धति करने वाली कोई औपचारिक प्रलेखित बैकअप नीति नहीं थी।

विभिन्न सीएमएस ग्रुप सदस्यों के लिए निर्धारित ड्यूटी सूची के अनुसार, डेटा के दैनिक बैकअप तथा साप्ताहिक बैकअप को क्रिस द्वारा अनुरक्षित किया जाना था। जनवरी 2015 में क्रिस द्वारा अनुसरित की जा रही बैकअप प्रक्रिया की लेखापरीक्षा समीक्षा के अनुसार, दैनिक बैकअप को नहीं लिया जा रहा था। क्रिस कोई दूरस्थ साइट बैकअप का भी अनुरक्षण नहीं कर रहा था। यह कहा गया कि सीएमएस के बैकअप की रैन्डम रूप से जांच की जाती है परन्तु अभिलेखों/लॉग्स के अभाव में इस तथ्य की पुष्टि नहीं की जा सकी कि जांच कब की गई।

इस प्रकार, सीएमएस प्रणाली में किसी उचित डेटा बैकअप प्रक्रियाओं का अभाव अप्रत्याशित परिस्थितियों में सीएमएस के परिचालन को जोखिम भरा बनाता है।

उत्तर (सितम्बर 2015) में रेलवे बोर्ड ने क्रिस की टिप्पणी का पृष्ठांकन किया कि दूरस्थ साइट बैकअप का अनुरक्षण किया जाएगा।