RBI/2015-16/418
DBS.CO/CSITE/BC.11/33.01.001/2015-16

জৈষ্ঠ্য 12, 1938 (শকাব্দ)
জুন 2, 2016

চেয়ারম্যান/ প্রাবন্ধিক নির্দেশক/ মূখ্য নির্বাহী আধিকারিক
সকল তফশিলভুক্ত বাণিজ্যিক ব্যাঙ্ক(আরআরবি ব্যতীত)

মহাশয়া/ মাননীয় মহাশয়,

ব্যাঙ্কসমূহে সাইবার নিরাপত্তা পরিকাঠামো

পরিচয়

ব্যাঙ্কসমূহ এবং তার উপাংশ (সহযোগী সংস্থা)গুলির মধ্যে তথ্য প্রযুক্তির ব্যবহার দ্রুতহারে বেড়েছে এবং এটি ব্যাঙ্কের কার্যসম্বন্ধিত কৌশলের অখন্ড অংশ। রিজার্ভ ব্যাঙ্ক, তথ্য সংক্রান্ত নিরাপত্তা, ইলেকট্রনিক ব্যাঙ্কিং, প্রযুক্তি সম্পর্কিত ঝুঁকি নিয়ন্ত্রণ এবং সাইবার প্রতারনার উপর (জি. গোপালাকৃষ্ণ কমিটি) এপ্রিল 29, 2011 তারিখাঙ্কিত সার্কুলার DBS.CO.ITC.BC.No.6/31.02.008/2010-11-এর মাধ্যমে নির্দেশিকা প্রদান করেছে, যেখানে উল্লেখ করা হয়েছে যে রূপায়ন প্রক্রিয়া সম্পর্কিত প্রস্তাবিত পদক্ষেপ গ্রহণ কোনও স্থবির (অনড়) বিষয় হতে পারে না এবং আধুনিক প্রগতি এবং উদ্ভূত সমস্যার ভিত্তিতে ব্যাঙ্কসমূহকে স্বতঃপ্রণোদিতভাবে তাদের নীতি, পদ্ধতি এবং প্রযুক্তি সংক্রান্ত উদ্ভাবন/ পরিমার্জন/ পরিবর্তন ঘটাতে হবে।

2. সেই সময় থেকে ব্যাঙ্কসমূহে প্রযুক্তির ব্যবহার অধিকতর গতি লাভ করেছে। অপরপক্ষে, প্রধানতঃ ব্যাঙ্কসহ আর্থিক ক্ষেত্রগুলিতে সাইবার সম্পর্কিত পরিস্থিতি/ আক্রমণের সংখ্যা, নৈমিত্তিকতা এবং অভিঘাত সাম্প্রতিক অতীতে বহুমাত্রায় বেড়েছে, যা ব্যাঙ্কগুলিতে বলিষ্ঠ সাইবার নিরাপত্তা/ প্রতিরোধ কাঠামো স্থাপনের এবং ব্যাঙ্কগুলিতে যথাযথ সাইবার নিরাপত্তা সংক্রান্ত প্রস্তুতি ধারাবাহিক ভিত্তিতে নিশ্চিত করার আশু প্রয়োজনকে স্পষ্টরূপে নির্দিষ্ট করে। ব্যাঙ্কিং ব্যবস্থায় সাইবার সংক্রান্ত বিপদের প্রবেশ-প্রতিরোধের দুর্বলতা, সাইবার আক্রমণের বিবর্তন প্রবণতা, বর্ধনশীল মাত্রা/ গতি, প্রেরণা এবং সম্পদ-প্রস্তুতির নিরিখে সাইবার ঝুঁকিসমূহকে প্রশমণের জন্য বর্তমান সুরক্ষা ব্যবস্থাপনার উন্নতি ঘটিয়ে ব্যাঙ্কিং ব্যবস্থার প্রতিরোধ কাঠামোর বলিষ্ঠতা বৃদ্ধি করা আবশ্যিক। এর মধ্যে অন্তর্ভুক্ত হবে, যদিও সীমাবদ্ধ হবে না, একটি উদ্ভূত

পরিস্থিতির মুখোমুখি হওয়ার মত অভিযোজনক্ষম(অ্যাডাপটিভ), নিয়ন্ত্রণ এবং পুনরুদ্ধারপ্রাপ্তির কাঠামো যা প্রতিকূল ঘটনা/ প্রতিবন্ধকতার মোকাবিলা করতে পারবে, যদি এবং যখন সেগুলি ঘটবে।

বোর্ড অনুমোদিত সাইবার-নিরাপত্তা নীতি

3. ব্যাঙ্কসমূহকে **অবিলম্বে** একটি সাইবার নিরাপত্তা নীতি প্রনয়ন করতে হবে যা স্পষ্টীকরণ করবে কাজের জটিলতার স্তর এবং ঝুঁকি-গ্রহণযোগ্যতার স্তরের উপর নির্ভর করে সাইবার বিপদকে প্রতিহত করার একটি যথাপ্রযোজ্য পথ যা তাদের বোর্ড কর্তৃক যথাযথরূপে অনুমোদিত হবে। এইমর্মে একটি নিশ্চয়তা-স্বীকৃতি আবশ্যিকভাবে সেপ্টেম্বর 30, 2016-এর মধ্যে ওয়ার্ল্ড ট্রেড সেন্টার-I, কাফে প্যারেড, মুম্বই 400005 - স্থিত ভারতীয় রিজার্ভ ব্যাঙ্ক, কেন্দ্রীয় কার্যালয়, ব্যাঙ্কিং তত্ত্বাবধান বিভাগের সাইবার সিকিউরিটি অ্যান্ড ইনফরমেশন টেকনোলজি (সিএসআইটিই) সেল-এ জানাতে হবে।

এটা নিশ্চিত করতে হবে যেন কৌশলটি নিম্নলিখিত সার্বিক বিষয়গুলিকে হিসাবে রাখে

সাইবার নিরাপত্তা নীতিকে ব্যাঙ্কের সার্বিক তথ্য প্রযুক্তি নীতি/ আইএস সিকিউরিটি নীতি থেকে স্বতন্ত্র হতে হবে

4. সাইবার নিরাপদ পরিবেশ গড়ে তোলার প্রয়োজনে সাড়া দিয়ে সম্পূর্ণ ব্যাঙ্কের সাইবার নিরাপত্তা নীতিকে হতে হবে সার্বিক তথ্য প্রযুক্তি নীতি/ আইএস সিকিউরিটি নীতি থেকে স্বতন্ত্র এবং পৃথক যাতে সাইবার বিপদের ঝুঁকি এবং সেইসব ঝুঁকিকে নজরে আনা/ প্রতিহত করার উপায়ের উপর গুরুত্ব আরোপ করা যায়।

5. যেহেতু আকার, ব্যবস্থা, প্রযুক্তিগত জটিলতা, ডিজিটাল প্রোডাক্ট, নির্ভরশীল গোষ্ঠী (স্টেকহোল্ডারস) এবং বিপদসঙ্কুলতা এক ব্যাঙ্ক থেকে অন্য ব্যাঙ্কে ভিন্নতর হয় যথাযথ সাইবার নিরাপত্তা কাঠামো গড়ে তুলতে অন্তর্নিহিত ঝুঁকিকে চিহ্নিত করা এবং নিয়ন্ত্রণ করার ব্যবস্থা তৈরী করা গুরুত্বপূর্ণ। অন্তর্নিহিত ঝুঁকি চিহ্নিতকরণ এবং পরিমাপের সময় ব্যাঙ্কসমূহকে ব্যবহৃত প্রযুক্তি, ব্যবসা এবং বিধিনিয়মের সঙ্গে সমন্বয় সাধন, স্থাপিত সংযোগব্যবস্থা, পরিষেবা প্রদানের উপায়সমূহ(ডেলিভারি চ্যানেল), অনলাইন/ মোবাইল প্রোডাক্ট, প্রযুক্তিগত পরিষেবা, সাংগঠনিক সংস্কৃতি এবং আভ্যন্তরীণ ও বহিরাগত বিপদের সাথে তাল রেখে অনুসৃত প্রযুক্তির দিকে খেয়াল রাখতে হবে। অন্তর্নিহিত ঝুঁকির স্তরের উপর ভিত্তি করে ব্যাঙ্কসমূহকে তাদের ঝুঁকিসঙ্কুলতাকে নিম্ন, মাঝারি, উচ্চ এবং অতি উচ্চ অথবা এরকম কোনও অন্য প্রকারভেদ ব্যবস্থা অনুসরণ করে চিহ্নিত করতে হবে। অন্তর্নিহিত ঝুঁকি পরিমাপ করার সময় ব্যবসা সংক্রান্ত

ঝুঁকিসঙ্কুলতাকেও একটি ঝুঁকি উপাদান হিসাবে গণ্য করতে হবে। প্রয়োজনীয় নিয়ন্ত্রণ ব্যবস্থা, বোর্ড নজরদারির ব্যাপ্তি, নীতি, প্রক্রিয়া নির্ণয় করার সময়, সাইবার ঝুঁকি নিয়ন্ত্রণ পরিকাঠামো তৎসহ অভিজ্ঞ ও যোগ্যতাসম্পন্ন মানবসম্পদ, প্রশিক্ষণ ও সংস্কৃতি, সম্ভাব্য বিপদ সম্পর্কিত তথ্য সংগ্রহের ব্যবস্থাপনা, ব্যাঙ্কে পরিস্থিতির বৈচিত্রের উপর সংগৃহিত তথ্যের সাথে তাল রেখে সম্ভাব্য বিপদ সম্পর্কে গৃহিত তথ্যাদির পরিলক্ষণ ও বিশ্লেষণ, তথ্য আদান প্রদান ব্যবস্থাপনা ও পরিচালনা(অন্যান্য সমগোত্রীয় ব্যাঙ্ক, আইডিবিআরটি/ আরবিআই/ সিইআরটি-ইন), প্রতিরোধমূলক, অনুসন্ধানমূলক এবং সংশোধনক্ষম সাইবার নিরাপত্তা পরিচালনা, ভেন্ডর ব্যবস্থা পরিচালনা এবং পরিস্থিতি অনুসারে ঘটমানতা বিশ্লেষণ এবং তদনুসারে ব্যবস্থা গ্রহণ পদ্ধতির রূপরেখা তৈরী করতে হবে।

ধারাবাহিক সর্বেক্ষণের ব্যবস্থা পরিচালনা

6. যুক্তিগ্রাহ্য সময় ব্যবধানে বিপদসঙ্কুলতা পরীক্ষা করা খুবই গুরুত্বপূর্ণ। সাইবার-আক্রমণের প্রকৃতি এমনই যে তা যেকোনও সময় বা যেকোন ভাবে ঘটতে পারে যা আগে থেকে অনুমান করা সম্ভব নাও যেতে পারে। একারণে, যত শীঘ্র সম্ভব একটি এসওসি(সিকিউরিটি অপারেশন সেন্টার) গড়ে তোলা আবশ্যিক করা হয়েছে , যদি এখনও তা না হয়ে থাকে, তবে। এটাও আবশ্যিক যে এই ব্যবস্থাকেন্দ্রটি ধারাবাহিক সর্বেক্ষণ নিশ্চিত করবে এবং উদ্ভূত হতে থাকা সাইবার বিপদের আধুনিকতম প্রকৃতি সম্বন্ধে নিজেকে সচেতন রাখবে।

আইটি কাঠামোকে নিরাপত্তাপ্রবণ হতে হবে

7. আইটি কাঠামোর রূপরেখা এরূপে অঙ্কণ করতে হবে যাতে সেটি সবসময়ের জন্য সাইবার নিরাপত্তা পদক্ষেপ গ্রহণে সহায়ক হয়। সেটির উপর বোর্ডের আইটি সাব কমিটি পর্যালোচনা করবে এবং ঝুঁকি বিচারে যদি প্রয়োজনীয় বলে মনে হয় তবে পর্যায়ভিত্তিকভাবে উন্নত করতে হবে। ঝুঁকি মূল্য/ সম্ভাব্য মূল্যের ভারসাম্য রক্ষা সম্বন্ধিত সিদ্ধান্ত যা কোনও ব্যাঙ্ক গ্রহণ করবে তাকে লিখিতভাবে খতিয়ানভুক্ত করতে হবে যাতে পরবর্তী ক্ষেত্রে তত্ত্বাবধান সম্পর্কিত মূল্যায়নকার্যে যথাযথরূপে সক্ষম হওয়া যায়।

8. ব্যাঙ্কসমূহকে রূপায়িত করতে হবে একটি 'নির্দেশমূলক(ইন্ডিকেটিভ) কিন্তু সামগ্রিক (এক্সসটিভ) নয়' এমন একটি বুনিয়াদী সাইবার নিরাপত্তা এবং প্রতিরোধমূলক কাঠামো যা অ্যানেক্স **1** এ দেওয়া হয়েছে। ব্যাঙ্কসমূহকে রিয়েল টাইম ভিত্তিতে সাইবার ঝুঁকি পর্যবেক্ষণ এবং নিয়ন্ত্রণের উদ্দেশ্যে

স্বতঃপ্রণোদিতভাবে সিকিউরিটি অপারেশন সেন্টার গড়ে তোলার এবং চালু করার প্রক্রিয়ার উৎসাহব্যঞ্জক সূচনা করতে হবে। এসওসি-র একটি নির্দেশমূলক গঠনশৈলী অ্যানেক্স 2 তে দেওয়া হয়েছে।

সুসংবদ্ধভাবে নেটওয়র্ক এবং ডাটাবেস নিরাপত্তা ব্যবস্থার দিকে মনোযোগ প্রদান

9. সাম্প্রতিক কিছু ঘটনায় এই বিষয়টি উঠে আসে যে বিস্তারিতভাবে প্রত্যেকটি ব্যাঙ্কের সাইবার নিরাপত্তা ব্যবস্থার সমীক্ষা করা প্রয়োজন। তার সাথে, এও পরিলক্ষিত হয়েছে যে অনেক সময় নেটওয়র্ক/ডেটাবেসে সংযোগব্যবস্থা একটি নির্দিষ্ট মেয়াদের জন্য কিছু ব্যবসা অথবা কার্যসম্পর্কিত প্রয়োজনের সুবিধার্থে অনুমতিপ্রদত্ত হয়। যদিও, যথার্থ মনোযোগের অভাবে এই প্রবেশপথটি সম্পূর্ণরূপে অবরুদ্ধ হয়ে যায় না তার ফলে নেটওয়র্ক/ডেটাবেস ব্যবস্থাটি সাইবার-আক্রমণের জন্য ভেদ্য হয়ে যায়। এটা আবশ্যিক যে নেটওয়র্ক এবং ডেটাবেসে যেন অননুমোদিত প্রবেশাধিকার না দেওয়া হয় এবং যেখানে অনুমতি দেওয়া হবে, সেখানে যেন সুনির্দিষ্ট পদ্ধতি অনুসরণ করে দেওয়া হয় এবং পদ্ধতিটি যেন নির্ভুলভাবে অনুসৃত হয়। এরকম নেটওয়র্ক এবং ডেটাবেসের উপর দায়িত্বভার যেন স্পষ্টরূপে চিহ্নিত থাকে এবং তা যেন আবশ্যিকভাবে ব্যাঙ্ক অধিকারিকদের উপর ন্যস্ত থাকে।

গ্রাহক তথ্যের সুরক্ষা নিশ্চিতকরণ

10. ব্যাঙ্ক কেবলমাত্র কার্যপ্রণালীর মসৃণ সম্পাদনের জন্যই প্রযুক্তির উপর প্রবলভাবে নির্ভরশীল নয় তার সাথে তাদের গ্রাহকদের অত্যাধুনিক ডিজিটাল প্রোডাক্টগুলি পৌঁছে দেবার ব্যাপারেও এটি প্রয়োজনীয় এবং এই প্রক্রিয়ায় ব্যাঙ্ক বিভিন্ন ব্যক্তিগত এবং সংবেদনশীল তথ্যাদিও সংগ্রহ করে থাকে। ব্যাঙ্ক, এইসমস্ত ডেটার ধারক হিসাবে (সেই ডেটা তাদের সাথেই রক্ষিত / তাদের পারস্পরিক তথ্য আদানপ্রদানের মধ্যপথে(ট্রানজিট) থাকুক বা গ্রাহকের কাছে থাকুক বা তৃতীয় পক্ষ পরিষেবাপ্রদানকারী কারো কাছে থাকুক) সেই ডেটার গোপনীয়তা, অখন্ডতা এবং লভ্যতা অক্ষুণ্ন রাখতে যথাযথ পদক্ষেপ নেবে; এরকম হেফাজতভুক্ত তথ্যাদির গোপনীয়তার সাথে কোনও পরিস্থিতিতেই যেন আপস না করা হয় এবং এই লক্ষ্যে ব্যাঙ্ক ডেটা/ তথ্যের "জীবনচক্র"(লাইফসাইকেল) ব্যাপী সময়কালে উপযুক্ত পদ্ধতি এবং প্রকরণের ব্যবস্থা করবে।

সাইবার ক্রাইসিস ম্যানেজমেন্ট প্লান

11. অবিলম্বে সাইবার ক্রাইসিস ম্যানেজমেন্ট প্লান(সিসিএমপি) গঠন করতে হবে এবং এটিকে বোর্ড স্বীকৃত পদ্ধতি-কৌশলের অংশ হতে হবে। এই বিষয়টি বিবেচনা করে যে সাইবার-ঝুঁকি অন্য অনেক ঝুঁকির থেকে পৃথক, যার জন্য প্রচলিত বিসিপি/ডিআর ব্যবস্থাপনা পর্যাপ্ত নাও হতে পারে এবং একারণে সাইবার-ঝুঁকির বিপত্তির কথা মাথায় রেখে একে নৈমিত্তিক ভিত্তিতে নজরে রাখতে হবে। হয়ত আপনাদের অবগত আছেন যে ভারতে সিইআরটি-ইন (কম্পিউটার এমারজেন্সি রেসপন্স টিম- ইন্ডিয়া, একটি সরকারি সংস্থা) স্বতঃপ্রণোদিত এবং প্রতিক্রিয়া ভিত্তিক পরিষেবা তথা নির্দেশিকা প্রদান, বিপদ সম্পর্কিত তথ্য প্রদান, আর্থিক ক্ষেত্র সমেত বিবিধ ক্ষেত্রজুড়ে থাকা বিভিন্ন সংস্থাসমূহের প্রস্তুতির পরিমাপ করার মাধ্যমে সাইবার নিয়াপত্তা ব্যবস্থা শক্তিশালী করতে গুরুত্বপূর্ণ উদ্যোগ নিয়ে চলেছে। এরসাথে সিইআরটি-ইন ন্যাশনাল সাইবার ক্রাইসিস ম্যানেজমেন্ট প্লান এবং সাইবার সিকিউরিটি অ্যাসেসমেন্ট ফ্রেমওয়র্ক প্রকাশ করেছে। সিসিএমপি প্রয়োগ করার সময় সিইআরটি-ইন/এনসিআইআইপিসি/আরবিআই/আইডিআরবিটি নির্দেশিকাও নজরে রাখতে হবে।

12. সিসিএমপি- কে নিচের চারটি বিষয়ের উপর কাজ করতে হবে (i) অনুসন্ধান (খুঁজে বের করা) (ii)ব্যবস্থা গ্রহণ (iii)প্রতিকার সাধন (iv)বিস্তার প্রতিরোধ। ব্যাঙ্কের তরফ থেকে সাইবার-আক্রমণের বিরুদ্ধে প্রতিরোধ গড়ে তোলার জন্য কার্যকরী পদক্ষেপ গ্রহণ এবং কোনও সাইবার-অনুপ্রবেশ ঘটলে তা তৎপরতার সাথে চিহ্নিত করতে হবে যাতে ব্যবস্থা গ্রহণ/প্রতিকার সাধন/বিস্তার প্রতিরোধ সম্ভবপর হয়। ব্যাঙ্কসমূহের কাছ থেকে প্রত্যাশা করা হচ্ছে যে তারা নতুন নতুন সাইবার-বিপদ যেমন 'জিরো-ডে' আক্রমণ, দূর থেকে অনুপ্রবিষ্ট বিপদ(রিমোট অ্যাকসেস থ্রেট), এবং লক্ষ্যনির্দিষ্ট আক্রমণ(টারগেটেড অ্যাটাকস)-এগুলির সম্মুখীন হবার জন্য যথাপ্রস্তুত থাকে। অন্যান্য বিষয়ের মধ্যে, ব্যাঙ্কসমূহ বিভিন্ন সাইবার বিপদের জন্য প্রয়োজনীয় প্রতিরোধমূলক এবং প্রতিকারমূলক ব্যবস্থা নেবে যার মধ্যে অন্তর্ভুক্ত থাকবে(কিন্তু এগুলিতেই সীমাবদ্ধ থাকবে না)- পরিষেবা প্রদানে অসম্মতি, পরিষেবা প্রদানে অসম্মতির বন্টিত রূপ(ডিসট্রিবিউটেড ডিনায়াল অফ সার্ভিস), র‍্যানসম অয়ার/ ক্রিপটো অয়ার, ধবংসাত্মক ম্যালঅয়ার, স্প্যাম সহ ব্যবসা সংক্রান্ত ই-মেল প্রতারণা, ই-মেল ফিশিং, স্পিয়ার ফিশিং, হোয়েলিং, ভিশিং প্রতারণা, ড্রাইভ-বাই ডাউনলোডস, ব্রাউজার গেটওয়ে প্রতারণা, ঘোস্ট অ্যাডমিনিস্ট্রেটর এক্সপ্লয়েটস, পরিচিতি সম্পর্কিত প্রতারণা, মেমরি আপডেট সম্পর্কিত প্রতারণা, পাসওয়র্ড সম্পর্কিত প্রতারণা ইত্যাদি।

সাইবার নিরাপত্তা জনিত প্রস্তুতির সূচকসমূহ

13. সাইবার প্রতিরোধী মূলকাঠামো কতটা পর্যাপ্ত এবং তা কতটা অনুসৃত হচ্ছে সেটির অনুধাবন এবং পরিমাপ করা হবে ঝুঁকি/প্রস্তুতির স্তর যেসব সূচক দ্বারা বোঝা যায় তাদের পরিস্থিতি পরিবর্তনের মাধ্যমে। এই সূচকগুলিকে ব্যবহার করতে হবে স্বাধীন অনুপালন যাচাই-এর মাধ্যমে ব্যাপকভাবে পরীক্ষণকার্য সম্পাদনের জন্য এবং যোগ্য ও উপযুক্ত পেশাদারদের দ্বারা পরিচালিত অনুপালন যাচাই এবং অডিট-এর জন্য। কর্মীবর্গ সহ যাবতীয় অংশীদারদের(স্টেকহোল্ডার) সচেতনতাকে এই অনুধাবন প্রক্রিয়ার অংশ হিসাবে ধরা হবে।

সাইবার নিরাপত্তা সংক্রান্ত ঘটনার উপর তথ্য আদান প্রদান

14. এটা পরিলক্ষিত হয়েছে- ব্যাঙ্কসমূহ যে সাইবার নিরাপত্তা সংক্রান্ত ঘটনার সম্মুখীন হয় তার সম্পর্কে তথ্য আদান প্রদান করতে ইতস্ততঃ বোধ করে। যদিও, এই বিষয়ে বিশ্বব্যাপী সংগৃহিত অভিজ্ঞতা এই যে সাইবার-ঘটনা সম্পর্কে সংস্থাসমূহের মধ্যে পারস্পরিক যোগাযোগ এবং সর্বাপেক্ষা গ্রহণযোগ্য পদ্ধতির অনুপালন সাইবার-ঝুঁকি প্রশমণে সহায়তা করে। এই বিষয়টিকে বারংবার গুরুত্ব আরোপ করে বলা হচ্ছে যে ব্যাঙ্কের যাবতীয় অস্বাভাবিক সাইবার-নিরাপত্তা সংক্রান্ত ঘটনা সম্পর্কে ভারতীয় রিজার্ভ ব্যাঙ্কের কাছে রিপোর্ট করা প্রয়োজন(সেগুলি সফল হোক অথবা নিষ্ফল প্রয়াস হোক)। তদুপরি ব্যাঙ্কসমূহকে উৎসাহিত করা হচ্ছে আইডিআরবিটি পরিচালিত তাদের সিআইএসও-র ফোরামের কার্যক্রমে সক্রিয়ভাবে অংশগ্রহণ করতে এবং কোনও ঘটনা ঘটলে তা তৎপরতার সাথে আইডিআরবিটি দ্বারা স্থাপিত ইন্ডিয়ান ব্যাঙ্কস-সেন্টার ফর অ্যানালাইসিস অফ রিস্কস অ্যান্ড থ্রেটস(আইবি-সিএআরটি)-তে রিপোর্ট করতে। এইরূপ পারস্পরিক সহযোগিতামূলক প্রয়াস ব্যাঙ্কসমূহকে সমষ্টিগতভাবে বিপদ সংক্রান্ত তথ্য সংগ্রহ, সময়মত সাবধানতা গ্রহণ এবং স্বতঃপ্রণোদিতভাবে সাইবার নিরাপত্তা পদক্ষেপ গ্রহণে সহায়তা করবে।

তত্তাবধান সম্পর্কিত রিপোর্টিং-এর মূলকাঠামো

15. সিদ্ধান্ত নেওয়া হয়েছে যে সাইবার-ঘটনা সহ নিরাপত্তা সম্পর্কিত ঘটনাসমূহ সম্পর্কে সংক্ষিপ্ত স্তরীয় এবং বিস্তারিত তথ্য সংগ্রহ করা হবে। ব্যাঙ্কসমূহকে তৎপরতার সাথে ঘটনাসমূহ অ্যানেক্স-3 ফর্মায় রিপোর্ট করতে হবে।

প্রস্তুতিতে ফাঁক থাকলে তা তৎক্ষণাৎ অনুধাবন করে আরবিআই-কে রিপোর্ট প্রেরণ

16. কন্ট্রোল ব্যবস্থায় বড় ধরণের ফাঁক(ম্যাটেরিয়াল গ্যাপ) থাকলে তা আগে থেকে চিহ্নিত করতে হবে এবং বোর্ডের আইটি সাবকমিটি তথা বোর্ডের নজরদারির অধীনে সক্রিয় উপদেষ্টা ব্যবস্থা অবিলম্বে প্রয়োগ করতে হবে। চিহ্নিত ফাঁকগুলি, প্রস্তাবিত নিয়ন্ত্রণ/পদক্ষেপ এবং তাদের থেকে কাম্য উপযোগিতা, প্রস্তাবিত নিয়ন্ত্রণ/পদক্ষেপগুলি রূপায়নের সময়সূচীর মাইলফলক এবং তাদের কার্যকারীতা পরিমাপের মাপকাঠি যার মধ্যে অন্তর্ভুক্ত আছে ঝুঁকি মূল্যায়ণ এবং ঝুঁকি নিয়ন্ত্রণ পদ্ধতি যা ব্যাঙ্ক অনুসরণ/প্রস্তাব করবে(তাদের স্ব-মূল্যায়ণের ভিত্তিতে), সেগুলিকে জুলাই 31, 2016 –এর মধ্যে চিফ ইনফরমেশন সিকিউরিটি অফিসারের মাধ্যমে ব্যাঙ্কিং তত্ত্বাবধান বিভাগ, কেন্দ্রীয় কার্যালয়-এর সাইবার সিকিউরিটি অ্যান্ড ইনফরমেশন টেকনোলজি এক্সামিনেশন(সিএসআইটিএসই)সেল-এ জমা করতে হবে।

সংগঠন ব্যবস্থাপনা

17. ব্যাঙ্কসমূহ সংগঠন ব্যবস্থাপনার সমীক্ষা করবে যাতে নিরাপত্তা সম্পর্কিত ভাবনাচিন্তা গুরুত্ব, পর্যাপ্ত মনোযোগ পায় এবং দ্রুত পদক্ষেপ গ্রহনের জন্য একে পদমর্যাদাগতভাবে যথাপ্রযুক্ত স্তরে উন্নিত করা যায়।

নির্ভরশীল গোষ্ঠী/ উচ্চতম কর্তৃপক্ষ/ বোর্ড-এর মধ্যে সাইবার নিরাপত্তা সম্পর্কিত সচেতনতা

18. এটা উপলব্ধি করা প্রয়োজন যে সাইবার ঝুঁকি নিয়ন্ত্রণের জন্য সংগঠনের প্রয়োজন সার্বিকভাবে সাইবার-সুরক্ষিত পরিবেশ তৈরী করা। এর জন্য দরকার সর্বস্তরের কর্মচারীগণের মধ্যে উচ্চস্তরীয় সচেতনতার বিকাশ। বিপদের সূক্ষ্ম বিষয়গুলি সম্পর্কে উচ্চতম কর্তৃপক্ষ এবং বোর্ডকেও যথেষ্ট মাত্রায় সচেতন থাকতে হবে এবং এব্যপারে যথাযথভাবে পরিচিতিকরণের ব্যবস্থাপনা গড়ে তুলতে হবে। ব্যাঙ্কসমূহকে স্বতঃপ্রবৃত্ত হয়ে তাদের গ্রাহকগণ, ভেন্ডর, পরিষেবা প্রদানকারী এবং অন্যান্য নির্ভরশীল পক্ষ যাঁরা জড়িত তাঁদের মধ্যে সাইবার সংক্রান্ত প্রতিরোধব্যবস্থার উদ্দেশ্য সম্পর্কে সচেতনতার প্রসার ঘটাতে হবে এবং ধারাবাহিক সঙ্গতি রেখে রূপায়নকার্য সম্পাদন এবং পরীক্ষণের প্রয়োজন স্থিরিকৃত ও নিশ্চিত করতে হবে। এই বিষয়টি সুপরিচিত যে সাইবার-বিপদের অভিঘাত সম্বন্ধে নির্ভরশীল গোষ্ঠীর(যার মধ্যে অন্তর্ভুক্ত থাকবে গ্রাহকগণ,কর্মচারী, অংশীদার এবং ভেন্ডরসমূহ)সচেতনতা ব্যাঙ্কের সাইবার-নিরাপত্তা প্রস্তুতিতে সহায়তা

করে। ব্যাঙ্ককে এরূপ সচেতনতা তৈরীতে যথাপ্রযোজ্য পদক্ষেপ গ্রহণ করতে হবে। যুগপৎভাবে, ব্যাঙ্কের বোর্ড অফ ডিরেক্টরস এবং উচ্চতম কর্তৃপক্ষকে জরুরি ভিত্তিতে সাইবার-নিরাপত্তা সম্পর্কিত বিষয়ে যেখানে প্রয়োজন সেখানে গতি আনতে হবে, এবং সেকারণে ব্যাঙ্কসমূহকে বলা হচ্ছে এই মর্মে অবিলম্বে পদক্ষেপ গ্রহণ করতে।

এই সার্কুলারটির একটি প্রতিলিপি বোর্ড অফ ডিরেক্টরদের আশু বৈঠকে উপস্থাপন করতে হবে।

আপনার প্রতি আন্তরিকতার সাথে

(আর রবিকুমার)

মুখ্য মহাপ্রবন্ধক

সংযোজিত অংশ: যথাপ্রদত্ত