## باکس 8.1: سائبر سیکورٹی-ابھرتے ہوئے رجحانات، چیلنجز اور پالیسی ردعمل

ٹیکنالوجی مالی خدمات کے شعبے سمیت دنیا بھر کے مختلف کاروباری شعبوں کے منظر نامے کو تبدیل کر رہی ہے ۔ ٹیکنالوجی کی مدد سے اخراجات میں کمی ، آپریشنل کارکردگی میں بہتری ، اور رسائی میں اضافے سے مالی اداروں کو پہلے سے کہیں زیادہ تیزی سے ترقی کرنے میں مدد مل رہی ہے ۔ کووڈ 19 کی وبا سے بھی صارفین کی ترجیحات میں بھی ایک مثالی تبدیلی آئی جو اب تیزی سے ڈجیٹل مالی مصنوعات اور خدمات کے فوائد حاصل کر رہے ہیں۔ تاہم ، جیسا کہ مالی ادارے تیزی سے ٹیکنالوجی کو اپنا رہے ہیں ، یہ امر انہیں مختلف خطرات اور چیلنجز بشمول غیر دانستہ واقعات اور دانستہ حملوں سے بھی دوچار رہتا ہے ۔ یہ صورت ضابطہ کار کے لیے بھی تشویش کا باعث بنتی ہے کیونکہ انہیں اس بندوبست سے جنم لینے والے خطرات سے فعال انداز میں نمٹنے کے لیے ضوابطی اور نگرانی فریم ورک کو مسلسل بڑھانا ہوگا۔ اگرچہ ، یہ فریم ورک کم از کم لازمی سطح حفاظتی معیارات اور کنٹرولز مہیا کرتے ہیں ، تاہم مالی اداروں کو ایسے خطرات کی مؤثر طریقے سے شناخت ، جانچ ، اور انتظام کی خاطر اور سائبر حملوں اور خطرات کی ابھرتی ہوئی نوعیت کے پیش نظر داخلی سطح پر سخت حفاظتی اقدامات کرنے کی ضرورت ہے

### تیز رفتار اختراع اور صارفین کی جانب سے ڈجیٹل مالی خدمات اپنانے کے سبب سائبرسیکورٹی مالی شعبے کی سلامتی اور استحکام کے لیے ایک اہم چیلنج کے طور پر ابھری ہے - - -

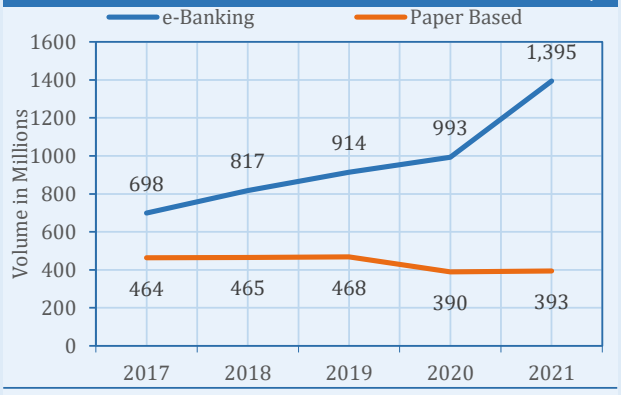
مالی شعبے میں کاروباری عمل اور مصنوعات میں ٹیکنالوجی اپنانے کے لحاظ سے نمایاں اختراع دکھائی دے رہی ہے، اسی لیے اس شعبے میں ارتباط اور پیچیدگیاں بڑھ رہی ہیں۔ تاہم، مصنوعات میں اختراع اور ٹیکنالوجی کے وسیع پیمانے پر استعمال سے دنیا بھر میں سائبر خطرات بڑھ رہے ہیں۔ سائبر حملے مالی صنعت کو مختلف قسم کے نقصانات سے دوچار کرسکتے ہیں، جن میں کاروبار میں تعطل، مالی اور ساکھ کا نقصان، سالمیت کا نقصان اور اثاثوں اور خدمات کی عدم دستیابی وغیرہ شامل ہیں۔ نظامی خطرے کے اعتبار سے کسی بڑے ادارے میں کوئی بڑا واقعہ رونما ہونے سے مالی نظام کو بحیثیت مجموعی خطرہ لاحق ہوجاتا ہے۔ مزید یہ کہ بار بار سائبر حملوں سے کاروباری کاموں میں خلل پڑنے کے ساتھ ساتھ مالی نظام پر عوام کا بھروسہ بھی کم ہوجائے گا۔ جس سے منڈی میں افراتفری کا امکان پیدا ہوسکتا ہے۔

### ڈجیٹل مالی خدمات کے استعمال میں اضافہ جاری ہے جس میں کووڈ 19 نے بھی اپنا کردار ادا کیا - - -

کووڈ19 کی وبا ڈجیٹل مالی خدمات کے فوائد سے صارفین کو روشناس کرا کے ان کی ترجیحات میں تبدیلی کا موجب بنی۔ مالی ادارے اور پالیسی ساز ادارے دونوں اب تیزی سے ٹیکنالوجی اور ڈجیٹل مالیات کے امکانات کا احساس کررہے، اور انتظامی اور لاگتی کارگردگی، صارفین کی سہولت، مالی شمولیت اور معیشت کی دستاویزات کو فروغ دینے کے لیے کوشاں ہیں۔

کووڈ19 کی وبا کے آغاز سے ہی پاکستان میں لین دین کے ڈجیٹل طریقوں کے استعمال میں بھی نمایاں اضافہ دیکھنے میں آیا ہے (**چارٹ 8.1.1**)۔ اس سلسلے میں اسٹیٹ بینک کے خصوصی اعانتی اقدامات اور سائبر جعلسازی کے خلاف احتیاطی تدابیر نے بھی ادائیگی کی خاطر ڈجیٹل طریقوں کے استعمال کو فروغ دینے میں اہم کردار ادا کیا۔[197] حال ہی میں پاکستان میں اسٹیٹ بینک نے بھی "راست" کے نام سے فوری ادائیگی کا پہلا نظام متعارف کرکے ایک تاریخی اقدام کیا ہے، جس سے ڈجیٹل مالی خدمات کے استعمال میں روز افزوں اضافہ متوقع ہے۔ راست نظام ملک بھر میں قدرے کم لاگت پر اور لگ بھگ حقیقی وقت میں بینک اکاؤنٹ سے لے کر بینک اکاؤنٹ کی لین دین میں سہولت فراہم کرتا ہے۔[198]

**چارٹ 8.1.1: مالی لین دین**

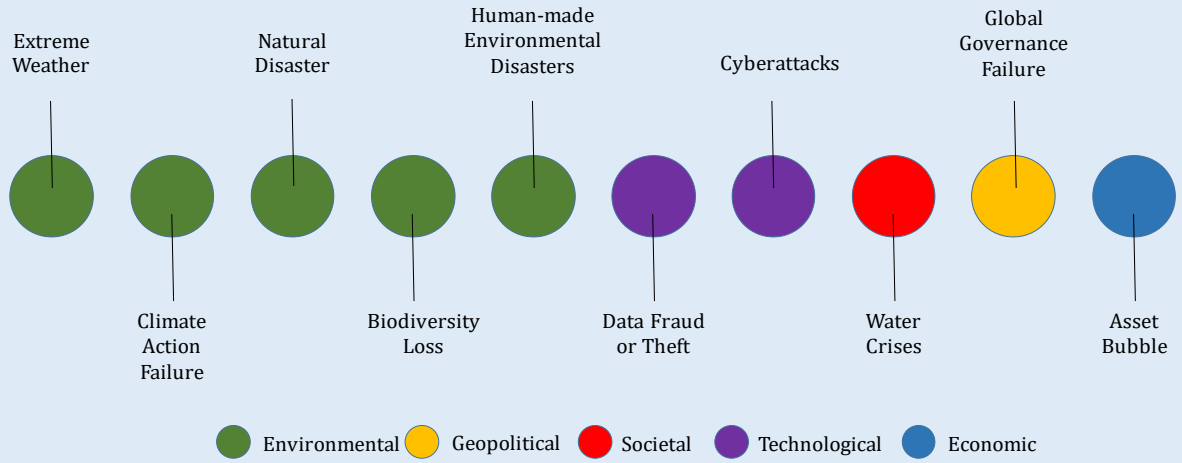



Source: SBP

[197] اسٹیٹ بینک نے مارچ 2020ء میں آئی بی ایف ٹی اور اسٹیٹ بینک کے بڑے پیمانے کی بروقت ادائیگیوں کا نظام جیسے آن لائن بینکنگ چینلز کے ذریعے رقوم کی منتقلی پر تمام چارجز ختم کردیے تھے۔ اسٹیٹ بینک نے بینکوں کو بڑھتے ہوئے ڈجیٹل ٹرانزیکشنز کے پیش نظر ڈجیٹل ذرائع کے جائزے اور نگرانی بڑھانے کی بھی ہدایات جاری کیں۔ مزید تفصیلات کے لیے اسٹیٹ بینک کی 18 مارچ 2020ء کی پریس ریلیز ملاحظہ کریں۔

[198] 'راست' فرد تا فرد فنڈ منتقلی اور تصفیہ خدمات کے تحت بینک صارفین اپنے بینک کی موبائل ایپلی کیشن، انٹرنیٹ بینکاری یا کاؤنٹر سروسز کا استعمال کرتے ہوئے اپنے اکاؤنٹس میں رقوم ارسال اور وصول کرسکتے ہیں۔ بینک اپنے صارفین کو اپنے ترجیحی بین الاقوامی بینک اکاؤنٹ نمبر (آئی بی اے این) کو اپنے رجسٹرڈ موبائل فون نمبر کے ساتھ منسلک کرکے 'راست' آئی ڈی بنانے کی اجازت دیتے ہیں۔ اس کے بعد صارفین اپنے اکاؤنٹ میں رقم وصول کرنے کے لیے دوسروں کے ساتھ 'راست' آئی ڈی کا اشتراک کرسکتے ہیں۔ بینک کے صارفین اپنے آئی بی اے این کا استعمال کرتے ہوئے رقوم بھیجنے یا وصول کرنے کے لئے 'راست' سروس کا استعمال کرسکتے ہیں چاہے ان کے پاس 'راست' آئی ڈی نہ بھی ہو۔ تفصیلات کے لیے اسٹیٹ بینک کی ویب پیج بعنوان Raast homepage ۔

چارٹ 8.1.2: آئندہ 10 برسوں میں درپیش دس بڑے خطرات

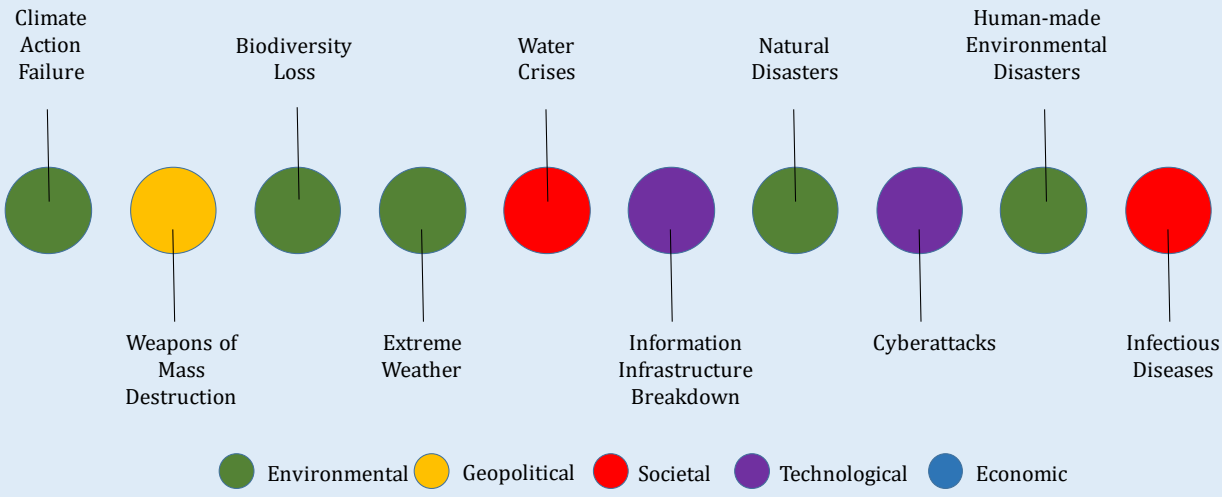



Source: The Global Risks Report 2021, World Economic Forum

## ڈجیٹل طریقوں کے عام ہونے کے ساتھ ساتھ سائبر سیکورٹی خطرات اور چیلینجز نے جنم لیا۔۔۔

ڈجیٹل تبدیلی مالی شعبے کے لیے متعدد نئے خطرات اور چیلنجوں کا باعث بھی بنی ہے۔ جیسے جیسے مالی شعبہ زیادہ ڈجیٹل ہوتا ہے، ویسے ہی اسے مختلف اقسام کے چیلنجز بشمول غیر مطلوبہ واقعات اور دانستہ حملوں کا سامنا کرنا پڑرہا ہے۔ یہ سائبر حملے مختلف اقسام بشمول ، برائے تاوان(ransomware)، فشنگ، ڈیٹا لیکج ، خدمات سے انکار، مالویئر پھیلانا، سائبر بھتہ خوری وغیرہ شامل ہیں۔ گذشتہ برسوں میں جب سے مالی اداروں نے اپنی کاروباری سرگرمیوں میں ٹیکنالوجی کا استعمال بڑھایا ہے، ان پر سائبر حملوں میں اضافہ ہورہا ہے۔ عالمی اقتصادی فورم کی عالمی خطرات رپورٹ 2021ء کے مطابق رپورٹ میں سائبر ناکامیوں کو آئندہ دس برسوں میں امکان اور اثرات دونوں کے اعتبار سے سب سے بڑے خطرے کا درجہ دیا گیا ہے۔ (**چارٹ 8.1.2 اور 8.1.3**)،[199] عالمی خطرات رپورٹ 2022ء میں بھی یہ نوٹ کیا گیا کہ سائبر سیکورٹی کی ناکامی کا خطرہ کووڈ وبا شروع ہونے کے بعد مزید ابتر ہوچکا ہے، پی ڈبلیو سی کے چوبیس ویں سالانہ سی ای او سروے میں نوٹ کیا گیا ہے کہ سائبر خطرات کی وجہ سے دنیا بھر کے اداروں اور ان کی

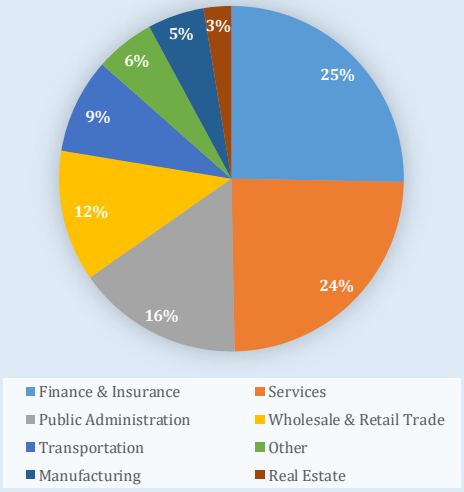
چارٹ 8.1.3: آئندہ 10 برسوں میں درپیش دس بڑے خطرات




Source: The Global Risks Report 2021, World Economic Forum

[199] عالمی خطرات رپورٹ 2021ء، عالمی اقتصادی فورم۔ رسائی بروز 15 مئی 2022ء

**چارٹ 8.1.4: بلحاظِ شعبہ کووڈ19 سے متعلق سائبر واقعات**




Source: BIS

اعلیٰ انتظامیہ میں بے چینی تیزی سے بڑھ رہی ہے۔[200] 2020ء میں 33 فیصد کی نسبت 2022ء میں تقریباً 50 فیصد سی ای اوز سائبر حملوں کے حوالے سے تشویش کا شکار ہیں۔ 2021ء میں س ای اوز کی جانب سے شدید تشویش کے حامل خطرات کی فہرست میں وبا اور صحت کے بحران کے فوری بعد سائبر خطرے کا نمبر آتا ہے۔[201] تاہم پی ڈبلیو سی کے 25ویں سالانہ عالمی سی ای اوز سروے کے مطابق سی ای اوز نے سائبر خطرات کو ترقی کی راہ میں صحت کے شعبے سے متعلق خطرات سے بھی بڑا خطرہ قرار دے دیا۔[202]

## دنیا بھر میں مالی شعبہ سائبر حملوں کی ترجیحی بنا رہا ہے---

مالی صنعت کے پاس بڑے زری اور غیر زری وسائل ہیں، جس میں عوام کی حساس اور قیمتی ذاتی معلومات کے بڑے ڈیٹا بیس شامل ہیں۔ اس طرح، یہ ہیکرز اور جعلسازوں کے لیے متعدد رغبت آمیز راستے پیش کرتا ہے۔ لہٰذا یہ صنعت دنیا بھر میں جعلساز عناصر کے لیے ایک خاص ہدف ثابت ہو رہی ہے۔ وبائی مرض کے پھیلاؤ کے بعد لاک ڈاؤن نے دنیا بھر میں ریموٹ ورکنگ کی ضرورت پیدا کر دی، اور اداروں کو ملازمین کو گھروں سے کام کرنے میں سہولت دینے کی خاطر ریموٹ ایکسس ٹیکنالوجی کا استعمال کرنا پڑا۔ اس رجحان نے سائبر خطرات اور حملوں کے خطرات کے سامنے اداروں کو زیادہ غیر محفوظ بنا دیا۔ مزید برآں، مالی ادارے اپنی خدمات کی فراہمی کے لیے تھرڈ پارٹی سروس فراہم کنندگان کی وسیع رینج کی مصنوعات اور خدمات کا استعمال کرتے ہیں، جس سے ان کے لیے سائبر خطرے مزید بڑھ جاتے ہیں۔ اس حوالے سے گزشتہ دو سالوں میں سائبر سپلائی چین حملوں کی تعداد میں اضافہ دیکھنے میں آیا ہے جہاں سائبر جرائم میں ملوث افراد ان کی سپلائی چین پر کو کمزور کرنے کے قابل ہیں۔ مزید، کچھ آئی ٹی مصنوعات اور خدمات اپنے ارتکاز کی وجہ سے نظامی اثر کی اہلیت رکھتی ہیں۔ لہٰذا، ان مصنوعات یا ان کے فراہم کنندگان کے ساتھ کوئی بھی مسئلہ ہونے کی صورت میں بڑے مالی نظام پر منظم اثرات مرتب ہو سکتے ہیں۔

جنرل کونسل فار اسلامک بینکس اینڈ فنانشل انسٹی ٹیوشنز کی جانب سے گلوبل اسلامک بینکرز سروے 2021ء کے مطابق سائبر سیکورٹی عالمی اسلامی بینکاری صنعت کو درپیش تین بڑے خطرات میں شامل ہے۔[203] بینک فار انٹرنیشنل سیٹلمنٹ (بی آئی ایس) کے مطابق کووڈ 19 وبائی مرض کے دوران دیگر شعبوں کی نسبت مالی شعبے پر ہیکرز کی جانب سے نسبتاً زیادہ حملے کیے گئے ہیں (**چارٹ 8.1.4**)۔[204]

## پاکستان میں بھی خصوصاً کووڈ وبا پھوٹنے کے بعد سائبر حملوں میں اضافہ ہوا ہے---

پاکستان میں بھی سائبر سیکورٹی کا مسئلہ ایک اہم تشویش کے طور پر ابھر کر سامنے آئی ہے۔ سائبر فراڈ کے واقعات میں اضافے کے علاوہ کچھ ریاستی اداروں اور بینکوں پر بڑے پیمانے پر سائبر حملے بھی ہوئے ہیں۔ مزید برآں، اسٹیٹ بینک کے تازہ ترین ایس آر ایس سے سائبر سیکیورٹی خطرات کے بارے میں شرکا کے تصور میں نمایاں اضافہ ظاہر ہوتا ہے۔

اسی طرح اسٹیٹ بینک نے سائبر سیکیورٹی کے خطرات کو کم کرنے کے لیے ایک **جامع ضوابطی اور نگرانی فریم ورک** قائم کیا ہے (**چارٹ 8.1.5**)۔ ذیل میں درج پیراگراف میں فریم ورک کے مختلف پہلوؤں پر تبادلہ خیال کیا گیا ہے۔

## اسٹیٹ بینک کے سائبر سیکورٹی اقدامات- ضوابطی فریم ورک سائبر خطرات سے نمٹنے کے لیے حفاظت کے کم از کم معیارات اور رہنمائی فراہم کرتے ہیں---

بینکوں کی سائبر سیکورٹی سے متعلق اسٹیٹ بینک کا ضوابطی نظام نیشنل انسٹی ٹیوٹ آف اسٹینڈرڈز اینڈ ٹیکنالوجی (این آئی ایس ٹی) کے سائبر سیکیورٹی فریم ورک اور مالی مارکیٹ کے بنیادی ڈھانچے کے لیے سائبر مضبوطی کے بارے میں بی آئی ایس کی رہنمائی پر مبنی ہے۔[205] [206] اسٹیٹ بینک نے اپنے آپ، مالی مارکیٹ کے بنیادی ڈھانچے، مالی اداروں اور ان کے

[200] عالمی خطرات رپورٹ 2021ء، عالمی اقتصادی فورم۔ رسائی بروز 15 مئی 2022ء

[201] پی ڈبلیو سی کا 24واں سالانہ عالمی سی ای اوز سروے۔ رسائی بروز 15 مئی

[202] پی ڈبلیو سی کا 24واں سالانہ عالمی سی ای اوز سروے۔ رسائی بروز 15 مئی

[203] عالمی اسلامک بینکرز سروے 2021ء۔ رسائی بروز 15 مئی 2022ء

[204] بی آئی ایس بلیٹن نمبر 37- مالی شعبے میں کووڈ19 اور سائبر خطرہ۔ اخذ شدہ بتاریخ 15 مئی 2022ء۔

گراف کے نمونے میں صحت کے شعبے (کووڈ سے متعلق 57 کیسز) اور اشیا سازی کے شعبے کی صحت سے متعلق اشیا (163 کیسز) کو شامل نہیں کیا گیا ہے۔

[205] نسٹ سائبر سیکورٹی فریم ورک۔ رسائی بروز 15 مئی 2022ء

[206] بی آئی ایس مالی منڈی انفراسٹرکچر کے لیے سائبر مضبوطی پر رہنمائی

صارفین کو سائبر خطرات سے بچانے کے لیے متعدد پالیسی اور ضوابطی اقدامات کیے ہیں۔ ان اقدامات کا مقصد مالی اداروں اور خدمات فراہم کندہ اداروں کے مجموعی گورننس انتظامات کو بہتر بنانا ہے، جو مالی اداروں کو آئی ٹی خدمات فراہم کرتے ہیں، اسٹیٹ بینک اور اس کے زیر انتظام مالی ادارے آپریشنل مضبوطی میں پختگی لانے اور حقیقی وقت میں سائبر خطرات سے نبرد آزما ہونے کے لیے اس صنعت میں تعاون اور اشتراک کی روایت کو فروغ دینا ہے۔ چونکہ ٹیکنالوجی مالی اداروں کے آپریشنز کا ایک لازمی حصہ بن چکی ہے، لہٰذا، اس طرح کی ٹیکنالوجی کا استعمال اور اس پر انحصار کا اگر مناسب طریقے سے انتظام نہیں کیا گیا تو اس سے ٹیکنالوجی کے خطرات بڑھ سکتے ہیں۔ اسٹیٹ بینک نے ان خطرات کا ادراک رکھتے ہوئے، 2017ء میں مالی اداروں میں انٹرپرائز ٹیکنالوجی گورننس اینڈ رسک مینجمنٹ فریم ورک کے حوالے سے ایک فریم ورک تشکیل دیا، جس کا مقصد مالی اداروں کو ٹیکنالوجی گورننس اور انتظامی اصولوں کی خطِ بنیاد تفویض کرنا ہے (چارٹ 8.1.6)۔[207] مالی اداروں پر لازم ہے کہ وہ اپنے ٹیکنالوجی پلیٹ فارمز کی ممکنہ خامیوں کی نشاندہی کرنے کے مقصد سے ڈجیٹل انفراسٹرکچر کا ہمہ جائزہ لیں اور نفوذ کی جانچ کریں۔ اسٹیٹ بینک نے مالی اداروں کو مزید یہ ہدایت کی ہے کہ وہ سائبر سیکورٹی تھریٹ انٹیلی جنس اور ایڈوائزری سروسز کا مناسب احاطہ کریں جن میں سمجھوتے کے اشاریوں (آئی او سیز) اپ ڈیٹ کرنا اور فوری تعمیل کو یقینی بنانا بھی شامل ہے۔ چونکہ ٹیکنالوجی کا منظر نامہ اور اس سے وابستہ خطرات تیزی سے بڑھ رہے ہیں، اس لیے اسٹیٹ بینک نے ضوابطی فریم ورک کے مسلسل جائزے اور مضبوطی کے حوالے سے اپنی توجہ میں اضافہ کر دیا ہے۔

### اسٹیٹ بینک نے اپنے اطلاعی سلامتی کے خطرات سے نمٹنے کے لیے

**چارٹ 8.1.5: اسٹیٹ بینک کے سائبر سیکورٹی خطرات کم کرنے کے اقدامات**


Source: SBP

### وقف ڈھانچہ اور طریقہ کار تشکیل دی---

اسٹیٹ بینک کے پاس اپنے اطلاعی اثاثوں کی سائبر مضبوطی یقینی بنانے کے مقصد سے اطلاعی سلامتی کا ایک مخصوص شعبہ ہے جو بینک کے نیٹ ورک، انفراسٹرکچر اور متعلقہ آئی ٹی سسٹم کے تحفظ کو یقینی بنانے کے لیے حکمتِ عملی کے اقدامات کرتا ہے۔ یہ شعبہ حکمتِ عملی طور پر پورے ادارے میں اطلاعی سلامتی کا انتظام کرتا ہے اور اسٹیٹ بینک کے آئی ٹی سسٹم اور بنیادی ڈھانچے کو سہارا دینے کے لیے سستی سیکورٹی خدمات فراہم کرتا ہے۔ یہ سائبر سیکورٹی کے تینوں پہلوؤں میں باقاعدگی سے آپریشنل سیکورٹی سرگرمیاں انجام دیتا ہے جس میں افراد، عمل اور ٹیکنالوجی کا احاطہ کیا جاتا ہے۔ حال ہی میں اسٹیٹ بینک نے اپنے اہم سیکورٹی نظاموں کی مضبوطی کی استعداد کاری کے لیے سرمایہ کاری کی اور سائبر واقعات کے انتظام کی فرضی مشقوں میں متعلقہ فریقوں کو شامل کر کے اپنی داخلی سائبر مضبوطی کی صلاحیت کو جلا بخشی۔ آئی ٹی انفراسٹرکچر کی چوبیس گھنٹے سائبر سیکورٹی نگرانی کے ساتھ اس استعداد کاری کے نتیجے میں خطرات کا جلد پتہ چلا ہے اور ٹیموں کی مجموعی اثر انگیزی اور ردِ عمل کے وقت میں بہتری آئی ہے۔

اسٹیٹ بینک نے مستقبل میں آئی ٹی کی ترقی اور سمت اور متعلقہ ابھرتے ہوئے سائبر خطرات مد نظر رکھتے ہوئے اپنی داخلی آئی ٹی سیکیورٹی پالیسیوں اور انتظامِ خطر فریم ورک میں کنٹرول کی ضروریات کا ایک نیا مجموعہ متعارف کرایا ہے اور جو آئی ٹی کے افعال اور سپورٹ سسٹم کے بڑے خطرات کا جائزہ لیتا ہے۔

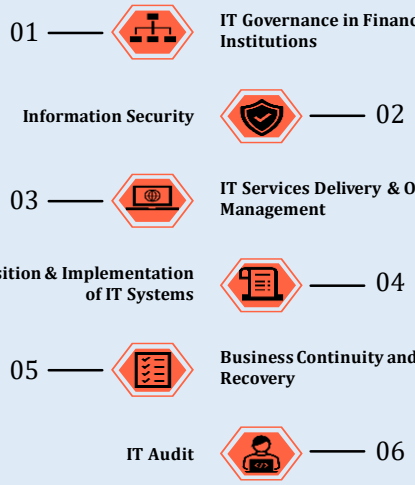
مزید برآں، اسٹیٹ بینک نے کرونا وائرس کے تناظر میں، سائبر سیکیورٹی آگاہی کے ورچوئل سیشنز کا اہتمام کر کے ثقافتی تبدیلی لانے کے لیے اپنی کوششیں جاری رکھیں۔ جس میں سوالات کے ذریعے صارفین کی صلاحیتوں کا تعین بھی جاتا ہے، اور جہاں بھی ضرورت ہوتی ہے وہاں ہدفی تربیتیں فراہم کی جاتی ہے۔ اسٹیٹ بینک کی ان تمام کوششوں سے سائبر سیکیورٹی صورتِ حال، پختگی اور مضبوطی کے ساتھ ساتھ مالی شعبے کے لیے اس کی میزبانی کی خدمات میں اضافہ ہوا ہے۔

### اسٹیٹ بینک کی سائبر سیکورٹی خطرات کے حوالے سے مجموعی ضوابطی رہنما خطوط میں اہم امور کے بارے میں تفصیلی رہنمائی موجود ہے---

پاکستان میں کام کرنے والے مالی ادارے گزشتہ برسوں کے دوران محتاط انداز میں اپنے چند امور کے لیے آؤٹ سورسنگ کے استعمال میں اضافہ کر رہے ہیں۔ اس نقطۂ نظر نے تھرڈ پارٹی خدمات فراہم کرنے والوں پر اِن کے انحصار میں اضافہ کیا ہے اور اس کے نتیجے میں ان کے خاکۂ خطر میں اضافہ ہوا ہے۔ اسٹیٹ بینک بینکوں کو پابند کرتا ہے کہ وہ اس بات کو یقینی بنائیں کہ آؤٹ سورسنگ نہ تو ڈپازٹرز اور سرمایہ کاروں کو دستیاب تحفظ میں کمی کا سبب بنیں اور نہ ہی اسے ضوابطی تقاضوں کی تعمیل سے بچنے کے طریقے کے طور پر استعمال کیا جائے۔ اسٹیٹ بینک نے بینکوں کی جانب سے متعدد خدمات کی آؤٹ سورسنگ کے بڑھتے ہوئے

[207] بی پی آر ڈی سرکلر نمبر 5 برائے 2017ء

**چارٹ 8.1.6: مالی اداروں کے لیے اسٹیٹ بینک انٹرپرائز ٹیکنالوجی گورننس اور انتظامِ خطر کے فریم ورک کا جائزہ**




Source: SBP

استعمال اور بینکوں پر متعلقہ خطرات کے ممکنہ اثرات کے پیش نظر، سب سے پہلے 2007ء میں آؤٹ سورسنگ انتظامات [208] کے حوالے سے رہنما خطوط جاری کیے تھے۔ جن کی ہدایات کے تحت بینکوں کو صرف اپنے غیر اہم افعال اور کاروباری معاونت کے افعال کو آؤٹ سورس کرنے کی اجازت ہے جبکہ بنیادی افعال کو آؤٹ سورس کرنے کی اجازت نہیں ہے۔[210،209] اسٹیٹ بینک باقاعدگی سے ابھرتے ہوئے بہترین طریقوں اور اسباق کی روشنی میں ان ہدایات کا جائزہ لیتا ہے (**چارٹ 8.1.7**) اور ان کی تازہ کاری کرتا ہے تاکہ مالی اداروں کو مؤثر انتظام میں سہولت دی جاسکے۔[211]

## پائیدار اختراع اسٹیٹ بینک کی پالیسی کی بنیاد ہے کیونکہ مرکزی بینک خطرات کے موثر انتظام اور ٹیکنالوجی اور جدت طرازی کے نپے تلے نقطہ نظر کو اپنائے ہوئے ہے۔۔۔

اسٹیٹ بینک متعلقہ خطرات کو مدنظر رکھتے ہوئے اپنے صارفین کی حفاظت اور سلامتی پر سمجھوتہ کیے بغیر ان کی خدمات کی فراہمی میں بہتری کے لیے جدت طرازی اور ٹیکنالوجی کے استعمال کی حوصلہ افزائی کرنے کی کوشش کرتا ہے۔ اسٹیٹ بینک اپنی ٹیکنالوجی اپنانے کی پالیسیوں کو مرحلہ وار طریقے سے نافذ کررہا ہے۔ اس کا مقصد مالی اداروں کو اپنے کاروباری آپریشنز میں جدید تکنیکی نظاموں کو استعمال کرنے سے پہلے اپنے سائبر سیکورٹی سسٹم کو تیار کرنے اور اسے مضبوط بنانے کے لیے کافی وقت دینا ہے۔ مثال کے طور پر اسٹیٹ بینک نے پہلی بار 2019ء میں برقی زری اداروں (ای ایم آئیز) کے لیے قواعد وضوابط تشکیل دیے اور جاری کیے۔[212] اس کے بعد اسٹیٹ بینک نے 2021ء میں دو برقی زری اداروں کو اپنے کمرشل آپریشنز شروع کرنے کے لیے لائیو لائسنس جاری کیے جبکہ 2020ء اور 2021ء کے دوران چار برقی زری اداروں کو آزمائشی طور پر منظوری دی گئی۔[213] مزید برآں، اسٹیٹ بینک نے حال ہی میں بینکاری شعبے کی حفاظت اور مضبوطی یقینی بناتے ہوئے بینکاری کاروبار میں ایک علیحدہ اور منفرد زمرے کے طور پر پاکستان میں ڈجیٹل بینکوں کے قیام کے لیے لائسنسنگ اور ضوابطی فریم ورک کا آغاز کیا ہے۔[214] اسٹیٹ بینک نے سی ڈی او فریم ورک بھی متعارف کرایا جس کے ذریعے ڈجیٹل طریقے سے اکاؤنٹ کھولے جائیں گے۔ اس سے قبل 2020ء میں اسٹیٹ بینک نے مالی اداروں کے ذریعے کلاؤڈ خدمات فراہم کنندگان (سی ایس پیز) کو آؤٹ سورسنگ سے متعلق اپنے رہنما خطوط کا دائرہ کار بھی بڑھادیا تھا (**چارٹ 8.1.8**)۔[215] اس سے قبل ہر قسم کی کلاؤڈ سروسز بشمول سافٹ ویئر بطور سروس (ساس)، پلیٹ فارم بطور سروس (پی اے اے ایس) اور انفراسٹرکچر بطور سروس (آئی اے اے ایس) کے لیے کلاؤڈ خدمات فراہم کنندگان کا پاکستان میں وجود ہونا لازمی تھا اور تمام فزیکل سرورز اور سروسز (ڈیٹا سینٹرز اور الائیڈ انفراسٹرکچر) کو پاکستان میں ہونا اور کام کرنا ہوتا تھا۔ نظر ثانی شدہ رہنما کے تحت اب مالی ادارے مخصوص شرائط کی بنیاد پر نان کور آپریشنز کے لیے ملکی اور آف شور کلاؤڈ خدمات فراہم کنندگان سے ہر قسم کے کلاؤڈ سروس ماڈلز حاصل کرسکتے ہیں اور ان آؤٹ سورسنگ انتظامات میں تسلی بخش داخلی گرفت یقینی بناسکتے ہیں۔ آگے چل کر اسٹیٹ بینک بنیادی خدمات کو پہلے مقامی کلاؤڈ خدمات فراہم کنندگان اور بعد میں بین الاقوامی کلاؤڈ خدمات فراہم کنندگان کو آؤٹ سورس کرنے کی اجازت دینے کی تجویز پر نظر ثانی کرنے کا ارادہ رکھتا ہے تاکہ اس بات کو یقینی بنایا جاسکے کہ مالی اداروں کے پاس اطمینان بخش سیکیورٹی نظام اور گرفت موجود ہو تاکہ قانونی تقاضوں کی تعمیل یقینی بنائی اور مطلوبہ حد مقرر کی جاسکے۔

## نگرانی کا فریم ورک مالی اداروں کے آپریشنل اور انتظامِ خطر کی روایات میں خامیاں دور کرکے ضوابطی فریم ورک کو سہارا دیتا ہے۔۔۔

اسٹیٹ بینک نے سائبر سیکیورٹی خطرات کے مسلسل جائزے اور نگرانی کے لیے اپنے بینکنگ سپرویژن گروپ میں ایک مخصوص ڈویژن قائم کیا ہے۔ اسٹیٹ بینک کے نگران

---

[208] بی پی آر ڈی سرکلر نمبر 9 برائے 2007ء

[209] نان کور آپریشنز اور بزنس سپورٹ فنکشنز میں ایچ آر ماڈیولز، پروکیورمنٹ فنکشنز، نان پروڈکشن انوائرمنٹ، سینڈ باکسنگ، انوینٹری مینجمنٹ، سپلائی چین مینجمنٹ، آفس پروڈکشن، کسٹمر ریلیشن شپ مینجمنٹ ٹولز (واٹس ایپ، فیس بک وغیرہ)، کمیونیکیشن ٹولز، سیکیورٹی ٹولز، کمپیوٹیشن اینڈ پروسیسنگ سروسز، ڈیٹا تجزیات اور رسک ماڈلنگ، مڈل ویئر اور پیمنٹ پروسیسنگ سروسز / پلیٹ فارمز وغیرہ شامل ہیں۔

[210] بنیادی آپریشنز اور کاروباری افعال میں تمام بینکاری ایپلی کیشنز اور متعلقہ بنیادی ڈھانچے شامل ہیں، جو صارفین / قرض گیروں کے لیجر اکاؤنٹس میں ڈپازٹس، قرضوں اور کریڈٹ سے متعلق صارفین کی معلومات اور بیلنس اور لین دین کی تفصیلات کو جمع کرنے اور پروسیس کرنے کے لیے استعمال ہوتے ہیں۔

[211] بی پی آر ڈی سرکلر نمبر 6 برائے 2017ء

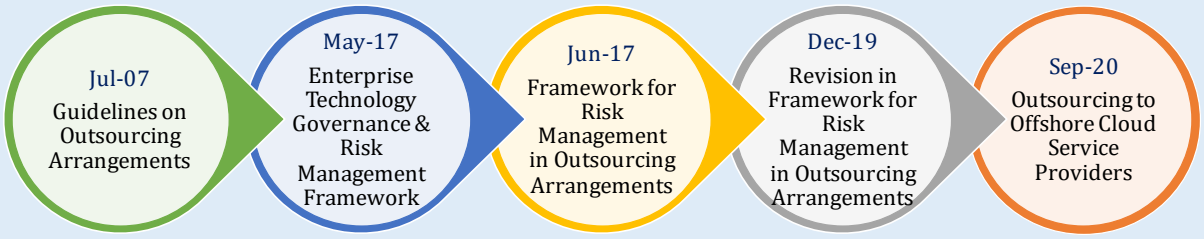
[212] برقی زری ادارے (ای ایم آئیز) ادارے وہ ادارے ہیں جو جدید، صارف دوست اور سستے ڈجیٹل ادائیگی کے آلات جیسے والیٹ، پری پیڈ کارڈز اور رابطے کے بغیر ادائیگی کے آلات پیش کرتے ہیں۔ ای منی نے مختلف ممالک میں مختلف قسم کی ادائیگیوں کو ڈجیٹائز کرنے میں اہم کردار ادا کیا ہے۔ توقع ہے کہ پاکستان میں ای ایم آئیز صارفین کو انٹر آپریبل اور محفوظ ڈجیٹل ادائیگی کی مصنوعات اور خدمات پیش کریں گی۔

[213] ایس بی پی ایم آئیز کی فہرست

[214] بی پی آر ڈی سرکلر نمبر 1 برائے 2022ء

[215] بی پی آر ڈی سرکلر نمبر 4 برائے 2020ء

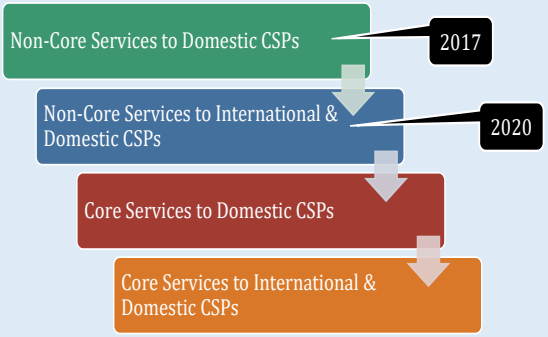
چارٹ 8.1.7: اسٹیٹ بینک - آؤٹ سورسنگ کے رہنما خطوط اور ہدایات




Source: SBP

عمل کا بنیادی مقصد مالی اداروں کی نگرانی کے لیے نگرانی کی سرگرمیوں کو ان کے حجم، پیچیدگی اور خطرے کے مطابق بیان کرنا ہے۔ خطرے پر توجہ مرکوز کرنے والے اس طرزِ فکر کے نتیجے میں مالی اداروں کی زیادہ سخت نگرانی ہوتی ہے، جو مالی نظام کے لیے بڑھتے ہوئے خطرے کا باعث بنتے ہیں۔ اس مقصد کے لیے نگرانی کے عمل میں برمقام اور فاصلاتی دونوں تشخیصیں شامل ہیں۔

چارٹ 8.1.8: اسٹیٹ بینک کا کلاؤڈ اپنانے کا طرزِ فکر




Source: SBP

مالی اداروں سے پیدا ہونے والے سائبر خطرات کی موثر نگرانی کے لیے **آر بی ایس** کے طریقہ کار پر مبنی ایک سائبر سیکیورٹی نگرانی فریم ورک تشکیل اور نافذ کیا گیا تھا۔ یہ فریم ورک متعلقہ سائبر سیکورٹی معیارات اور بہترین طریقوں پر غور کرنے کے بعد تیار کیا گیا تھا۔ یہ فریم ورک ابھرتے ہوئے سائبر خطرات اور متعلقہ کنٹرولز کا جائزہ لینے کے لیے طریقہ کار فراہم کرتا ہے۔ اہم تشخیصی امور میں سائبر سیکیورٹی گورننس، انفارمیشن اثاثوں کا انتظام، انتظامِ خطر، رسائی پر گرفت، ڈیٹا سیکورٹی، سائبر سیکیورٹی آگاہی، واقعات کا پتہ لگانا اور ردِ عمل وغیرہ شامل ہیں۔ اس فریم ورک کا استعمال کرتے ہوئے مالی اداروں کا سائبر سیکورٹی معائنہ کیا جاتا ہے۔

سائبر حفظان صحت (سی ایچ) سائبر واقعات کے خلاف خطِ بنیاد کی تشکیل فراہم کرنے میں نمایاں کردار ادا کرتا ہے۔ اس سلسلے میں مالی اداروں کے سائبر حفظان صحت کو مضبوط بنانے کے لیے خود تشخیص اور ان کی سینئر مینجمنٹ کی ملکیت کے ذریعے ایک مشق کی جارہی ہے۔

اسٹیٹ بینک کے لیے تشویش کا ایک اور اہم امر ڈجیٹل بینکاری فراڈ ہے۔ اس کی آگاہی مہمات اور نگرانی سے لے کر مالی اداروں کے ساتھ بڑے پیمانے پر مصروفیت تک متعدد اقدامات کیے گئے۔ مزید برآں اسٹیٹ بینک پاکستان ٹیلی کمیونیکیشن اتھارٹی (پی ٹی اے) اور ایف آئی اے کے ساتھ ڈجیٹل بینکاری فراڈ کی روک تھام کے لیے تعاون کررہا ہے۔

## مستقبل کا منظر نامہ ۔۔۔

دنیا میں تکنیکی ترقی تیزی سے ابھر رہی ہے اور اسی طرح ان پیشرفتوں کے نتیجے میں پیدا ہونے والے متوازی چیلنجز بھی ہیں۔ مالی اداروں کو بڑھتی ہوئی نفاست کی سطح کے ساتھ بڑھتے ہوئے سائبر حملوں کا سامنا کرنا پڑرہا ہے۔ اس طرح، مالی اداروں کو مضبوط سائبر سیکیورٹی اقدامات اور کنٹرول رکھنے کی ضرورت ہے اور مختلف قسم کے سائبر واقعات سے نمٹنے کے لیے ان پروٹوکولز کی مسلسل نگرانی اور تازہ کاری کرنے کی ضرورت ہے۔ تکنیکی کنٹرول کے علاوہ، انسانی وسائل بھی سائبر حملوں کے خلاف کسی بھی دفاعی پروٹوکول کا ایک اہم حصہ ہیں۔ سوشل انجینئرنگ کے حملے مؤثر طریقے سے لوگوں کو نظام کی خلاف ورزی کرنے کے لیے استعمال کرتے ہیں۔ لہٰذا یہ انتہائی اہمیت کا حامل ہے کہ ادارے کے اندر استعداد کار بڑھانے پر وسائل خرچ کیے جائیں۔ اس کے علاوہ، اس طرح کی تمام کوششوں کو صنعت کے ممبروں اور ضابطہ کاروں کے مابین موثر ہم آہنگی کے ذریعہ پورا کرنے کی ضرورت ہے۔ متعلقہ فریقوں کے درمیان معلومات کا بہاؤ مضبوط اور بروقت ہونے کی ضرورت ہے تاکہ سائبر حملوں کا موثر انداز میں جواب دیا جاسکے۔ اس موقع پر اسٹیٹ بینک وزارت انفارمیشن ٹیکنالوجی اور ٹیلی کمیونیکیشن کی جانب سے

نیشنل سائبر سیکیورٹی پالیسی 2021ء کے اختیار کے تحت فنانشل سیکٹر میں کمپیوٹر ایمرجنسی رسپانس ٹیم (فن سرٹ) کے قیام پر کام کر رہا ہے۔

مزید برآں اسٹیٹ بینک پہلے ہی مالی اداروں کو معیاری فارمیٹس کے ساتھ ہدایات جاری کر چکا ہے کہ وہ کال سینٹرز کے ذریعے ڈجیٹل بینکنگ فراڈ یا فراڈ کی کوششوں کے بارے میں معلومات اکٹھی کریں۔[216] اس بات کو مدنظر رکھتے ہوئے کہ کسی ایک مالی ادارے پر سائبر حملے کا باقی نظام پر اثر پڑتا ہے، یہ ضروری ہے کہ صنعت مجموعی طور پر اس طرح کے حملوں کا مقابلہ کرنے کے لیے اپنے وسائل لگائے۔ آخر میں، سائبر حملوں سے پیدا ہونے والے خطرات کا مقابلہ کرنے میں بین الاقوامی تعاون انتہائی اہمیت کا حامل ہے۔ یہ حملے زیادہ تر عالمی نوعیت کے ہوتے ہیں اور ریاستوں، ضوابطی اور نگران اتھارٹیز، قانون نافذ کرنے والے اداروں اور مالی اداروں کے درمیان تعاون ان حملوں سے پیدا ہونے والے خطرات کو مؤثر طریقے سے منظم اور کم کرنے کے لیے ضروری ہے۔

[216] بی سی اینڈ سی پی ڈی سرکلر نمبر 2 برائے 2021ء