گورنر کا خطاب

اسٹیٹ بینک آف پاکستان، پی بی اے کی بینکاری صنعت میں مشترکہ سائبر سیکورٹی مشقیں۔ ایوارڈز کی تقریب

23 جنوری 2026ء

چیئرمین پاکستان بینکس ایسوسی ایشن،
بینکوں کے صدور، سی ای اوز، اور چیف انفارمیشن سیکورٹی افسران
بینکاری صنعت اور اسٹیٹ بینک آف پاکستان کے ساتھیو!

معزز مہمانان، خواتین و حضرات!
السلام علیکم اور آپ سب کو شام بخیر!

یہ میرے لیے نہایت مسرت کی بات ہے کہ آج میں آپ کے ساتھ ایوارڈز تقسیم کرنے کی تقریب میں شریک ہوں۔ یہ تقریب پاکستان کے بینکاری شعبے میں پہلی بار منعقد ہونے والی سائبر سیکورٹی مشقوں کی کامیاب تکمیل پر اداروں اور افراد کو خراجِ تحسین پیش کرنے کے لیے منعقد کی گئی ہے۔ اگرچہ اس مشق کا مقصد ہمارے تکنیکی ردِ عمل کی اجتماعی صلاحیتوں کو جانچنا تھا، تاہم اس سے بھی زیادہ اہم یہ بات تھی کہ کسی سائبر بحران کی صورت میں یہ جانچا جاسکے کہ اعلیٰ انتظامیہ کا فیصلہ سازی کا طرز فکر کیا ہو گا۔ جیسا کہ آپ جانتے ہیں، اس مشق میں ایک یا ایک سے زائد اداروں پر مربوط سائبر حملوں کے فرضی حالات بنائے گئے، اور ایسے منظر نامے شامل کیے گئے جن کا اگر مؤثر انداز میں انتظام نہ کیا جائے تو وہ مالی نظام کے استحکام کے لیے سنگین خطرات پیدا کر سکتے ہیں۔

چنانچہ آج کی تقریب کا مقصد صرف اعزازات تقسیم کرنا نہیں ہے، بلکہ سائبر سیکورٹی کے شعبے میں مستعدی، جوابدہی اور قیادت کی ایک مضبوط ثقافت کو فروغ دینا ہے۔ آج جن اداروں اور افراد کی صلاحیتوں کا اعتراف کیا جارہا ہے انہوں نے ضوابطی تقاضوں کی تکمیل سے بڑھ کر وابستگی دکھائی ہے۔ انہوں نے صلاحیت، تعاون اور بحران سے نمٹنے کی تیاری میں سرمایہ کاری کی ہے—اور یہی وہ اوصاف ہیں جو مسلسل اور پیچیدہ سائبر خطرات کے اس دور میں مالی استحکام کے تحفظ کے لیے ناگزیر بن چکے ہیں۔

مالی نظام میں بڑھتے ہوئے باہمی روابط اور پیچیدگی کے ساتھ ٹیکنالوجی کے وسیع پیمانے پر استعمال نے نئے خطرات اور کمزوریوں کو جنم دیا ہے۔ آج کے دور میں خطرات پیدا کرنے والے عناصر اب محض الگ تھلگ ہیکرز نہیں ہیں، بلکہ وہ مہارت یافتہ، وافر وسائل کے حامل اور منظم ہیں۔ مزید برآں، بڑھتی ہوئی جغرافیائی و سیاسی کشیدگی نے سائبر خطرات بڑھا دیے ہیں اور سائبر خطرات کے

منظر نامے میں ایک نئی جہت کا اضافہ کیا ہے۔ اس کے علاوہ، ملک میں سائبر سیکورٹی کے مہارت یافتہ افراد کی کمی ہے جس کی وجہ سے ہمارے اداروں کی سائبر خطرات سے مؤثر تحفظ کی صلاحیت محدود ہو جاتی ہے۔

اس تناظر میں، میں اس بات پر زور دینا چاہوں گا کہ سائبر resilience انفرادی سطح پر حاصل نہیں کی جا سکتی۔ اس کے لیے اجتماعی تیاری، معلومات کا شفاف تبادلہ، اور ضابطہ کاروں (regulators) اور زیرِ ضابطہ (regulated) اداروں کے درمیان اعتماد ضروری ہے۔ آج کے ماحول میں سائبر resilience کا اندازہ اس بات سے نہیں لگایا جاتا کہ سائبر حملے ہو رہے ہیں یا نہیں، بلکہ اس بات سے لگایا جاتا ہے کہ ہم ان کا کتنا مؤثر جواب دیتے ہیں۔

جیسے جیسے پاکستان کا بینکاری شعبہ ڈجیٹل تبدیلی کے سفر میں آگے بڑھ رہا ہے، اس میں عوام کا اعتماد برقرار رکھنا نہایت اہم ہوتا جا رہا ہے۔ اس طرح کی سائبر سکیورٹی کی مشقیں صارفین، مارکیٹوں اور بین الاقوامی شراکت داروں کو ایک مضبوط اور حوصلہ افزا پیغام دیتی ہیں کہ پاکستان کا مالی نظام فعال، مستعد، اور عالمی معیارات سے ہم آہنگ ہے۔ یہ اقدام بلاشبہ ایک اہم سنگِ میل ہے — جو cyber risks جیسے نمایاں ابھرتے ہوئے خطرات سے نمٹنے کے لیے ہمارے مالی نظام کی بڑھتی ہوئی پختگی، دور اندیشی اور اجتماعی عزم کی عکاسی کرتا ہے۔

خواتین و حضرات،

اسٹیٹ بینک میں ہم مالی صنعت میں سائبر سکیورٹی کو یقینی بنانے کے حوالے سے بہترین بین الاقوامی طریقوں کو برقرار رکھنے کے لیے پرعزم ہیں۔ ہمارے اسٹریٹجک پلان — وژن 2028ء — کے تحت لچک، اعتماد اور استحکام ہمارے مالی نظام کے بنیادی ستون ہیں۔ اور آج کے انتہائی ڈجیٹل اور باہم مربوط (interconnected) ماحول میں سائبر خطرات ان ستونوں کے لیے سب سے نمایاں خطرہ بن چکے ہیں۔ یہ خطرات اب محض آئی ٹی سسٹمز یا آپریشنل رکاوٹوں تک محدود نہیں رہے بلکہ ایک نظامی خطرہ بن چکے ہیں، جو مالی استحکام، عوام کے اعتماد اور معاشی ترقی پر براہِ راست اثرات مرتب کرتے ہیں۔

حالیہ برسوں میں، اسٹیٹ بینک نے بینکوں، مالی منڈی کے بنیادی ڈھانچوں، اور — سب سے اہم — صارفین کی حفاظت کے لیے کئی اہم اقدامات کیے ہیں۔ ہم نے بینکاری شعبے میں سائبر خطرات کی نگرانی مضبوط بنانے کے لیے ایک خصوصی سائبر رسک مینجمنٹ ڈپارٹمنٹ بنایا ہے، جو نگرانی کے طریقہ کار کو بہتر بنا رہا ہے، زیرِ ضابطہ اداروں کے ساتھ اس موضوع پر رابطوں کو مضبوط کر رہا ہے، اور شکایات کے اندراج اور ازالے کے طریقہ کار کو مستحکم بنا رہا ہے۔ کیا ان مقاصد کا حصول اب تک خامی سے پاک رہا ہے؟ ایسا

نہیں ہے، لیکن ہم صحیح سمت میں آگے بڑھ رہے ہیں اور ہم اسٹیٹ بینک میں اور وسیع تر تناظر میں پوری بینکاری صنعت میں سائبر سکیورٹی اور عملی کارکردگی کے مابین قابلِ عمل توازن کے لیے کوشاں ہیں۔

بینکاری شعبے کی مجموعی سائبر سکت (resilience) کو بہتر بنانے کی غرض سے اس صنعت کو حکمت عملی کی واضح سمت اور روڈمیپ دینے کے لیے، ہم بہت جلد اپنے زیرِ ضابطہ اداروں کے لیے ایک جامع Cyber Resilience Strategy جاری کریں گے۔ ہم اس حکمت عملی کو 'سائبر شیلڈ 30-2025' کا نام دے رہے ہیں۔ یہ حکمت عملی ہمارے مالی شعبے کی صلاحیت کو بڑھانے کے لیے مستقبل کا روڈمیپ ہوگی تاکہ وہ سائبر خطرات کو پہچاننے، ان سے حفاظت اور انہیں برداشت کرنے کے ساتھ ساتھ ان سے مقابلے کے بھی قابل ہو سکے۔ اس حکمت عملی کے یہ پانچ بنیادی ستون ہیں: (1) cyber resilience کی مضبوطی، (2) سائبر سکیورٹی گورننس کو بہتر بنانا، (3) تعاون اور شراکت داری کو فروغ دینا، (4) سائبر ورک فورس کی تشکیل اور (5) سائبر سکیورٹی پروگرامز کا مسلسل ارتقا۔

اس کے ساتھ ساتھ میں تمام شریک اداروں کو سراہنا چاہوں گا کہ انہوں نے پاکستان کی بینکاری تاریخ میں پہلی مرتبہ صنعت گیر سائبر سکیورٹی مشق مشترکہ طور پر منعقد کی اور تعاون کے معیار کو نئی بلندیوں پر پہنچا دیا۔ میں خصوصی طور پر SBP-PBA کی مشترکہ کمیٹی کا شکریہ ادا کرنا چاہوں گا– جس میں اسٹیٹ بینک کے افسران اور ایم سی بی، فیصل بینک، میزان بینک، یو بی ایل، عسکری بینک، اور بینک آف پنجاب کے چیف انفارمیشن سکیورٹی آفیسرز شامل ہیں، جنہوں نے پچھلے دو سال کے دوران اس سائبر سکیورٹی مشق کی منصوبہ بندی اور نفاذ کے لیے محنت کی۔ نیز، تمام ایوارڈ حاصل کرنے والوں کو بھی مبارکباد پیش کرتا ہوں۔

میں اس مشق سے حاصل ہونے والے بصیرت اور اسباق کے حوالے سے یہ دیکھنے کا منتظر ہوں کہ ہم انہیں اجتماعی طور پر اپنے آپریشنز میں کس طرح شامل کرتے ہیں، اور یہ مشقیں ہماری سائبر مزاحمت کے قومی فریم ورک کا ایک باقاعدہ اور لازمی ستون کیسے بنتی ہیں۔

شکریہ

****