SITUATION	CONTINGENCY MEASURE
a. If the Kiosk Voting URL is not accessible or blocked.	• Check if "p12 client certificate" has been installed in the browser used. If yes, reinstall the same. • If issue persists, contact the OFOV for troubleshooting procedures.
b. If the admin voting portal is not accessible/blocked.	• Contact OFOV and provide public IP/static IP address for possible whitelisting of the same.
c. If the Kiosk laptop is malfunctioning or is not working.	• Report the matter to OFOV and perform troubleshooting measures. • Posts are authorized to repurpose their existing Client or Contingency Voter Registration Machines (VRMs) into OVCS Kiosks, upon submission of proper notice to OFOV. Should Posts proceed with the said repurposing, ensure that all voter databases, lists and other related data about voter registration are permanently deleted and the Apache and FileZilla application in the Task Bar are unpinned.
d. If the camera of the Kiosk is not working/detected.	• Post shall report such fact to the OFOV. • Posts are authorized to use the previously issued webcams (used with the VRMs during registration).
e. If the thermal printer is not working.	• Notify OFOV of the said issue, and proceed to download the said reports. Print the said reports on a regular printer. • In case there is no printer available, Post shall seek authority from OFOV to procure a new printer of a similar quality to be charged to the election funds of Posts, subject to procurement and auditing rules and guidelines.
f. If Post did not receive thermal paper rolls or thermal paper rolls issued are not sufficient.	• Notify the OFOV of the issue and proceed to download the reports. Print the said reports on a regular printer. • In case there is no printer available, Post shall seek authority from OFOV to procure a new printer of a similar quality to be charged to the election funds of Posts, subject to procurement and auditing rules and guidelines.
g. If the Teltonika router is not working.	• Contact OFOV about the issue. • OFOV shall request for approval from OFOV-CIC to perform transmission using regular internet connection.
h. If Post did not receive a collapsible ballot box.	• Post is authorized to use a sturdy box that can be securely closed, to store their reports for the elections. Should Post purchase said box, the same can be charged to the election funds of Post. • Kindly note in the Minutes and inform OFOV of the said fact.
i. If Post did not receive sufficient envelopes.	• Post is authorized to use envelope of a similar size. Should Post purchase said envelopes, the same can be charged to the election funds of Post. • Kindly note in the Minutes and inform OFOV of the said fact. OFOV shall provide a template to Post, to be printed and attached to the envelope.
j. If Post did not receive paper seals or quantity is not sufficient.	• Post is authorized to print the paper seal in sticker paper using the provided format of the Commission. • Sign the said seal upon use, and note such fact in the minutes.
k. In case of missing or lacking USB tokens.	• Post is authorized to use a new set of USBs. Should Post purchase new USBs, the same can be charged to the election funds of Post. • Kindly note in the Minutes and inform OFOV of the said fact.
l. In case of ring light or tripod malfunction.	• Notify the OFOV about the matter. • OFOV, upon approval of the OFOV-CIC, shall authorize the procurement of a new ring light or tripod, which will be charged to the Post's election funds.

Section 5. ***Authority of the Commission to Adopt Additional Contingency Procedures.*** – The Commission may adopt additional contingency procedures in the voting, counting, consolidation, transmission, storage, custody distribution and retrieval of accountable and non-accountable forms, supplies and paraphernalia to fulfill its Constitutional mandate to ensure free, orderly, honest, peaceful and credible elections overseas.

Section 6. ***Effectivity and Dissemination.*** The Education and Information Department shall cause the publication of this Resolution in two (2) daily newspapers of general circulation in the Philippines. The Office for Overseas Voting shall furnish copies to the Department of Foreign Affairs – Overseas Voting Secretariat and all Special Board of Election Inspectors, Special Ballot Reception and Custody Group, and Special Board of Canvassers in all Foreign Service Posts abroad.

SO ORDERED.

GEORGE ERWIN M. GARCIA
Chairman

AIMEE P. FEROLINO
Commissioner

REY E. BULAY
Commissioner

ERNESTO FERDINAND P. MACEDA, JR.
Commissioner

NELSON J. CELIS
Commissioner

MARIA NORINA S. TANGARO-CASINGAL
Commissioner

NOLI R. PIPO
Commissioner

CERTIFICATION

APPROVED for publication, April 8, 2025.

CONSUELO B. DIOLA
Director IV
Office of the Commission Secretary

This Resolution can be verified at this number (02)85272987; email address comsec@comelec.gov.ph.

PHL businesses must invest in data protection amid threats

PHILIPPINE BUSINESSES must increase their data protection investments as cyberthreats become more complex, according to Taiwan-based technology platform Synology, Inc.

"As the Philippines undergoes rapid digital transformation, businesses must strengthen their data protection strategies to address the rising demand for secure data storage and management," Joanne Weng, director of International Business at Synology, said in e-mail.

"To ensure business continuity and resilience, Philippine businesses must invest in scalable, reliable data protection solutions."

Amid increasing digitalization in the country, many organizations in the Philippines struggle to keep up with evolving cyberthreats due to limited information technology (IT) expertise and inadequate protection measures, Ms. Weng said.

About 35% of Asia-Pacific's chief executive officers are now prioritizing investments in data management and robust cybersecurity, according to the 2024 EY CEO Outlook Pulse survey.

In March, Synology launched its newest data protection system called ActiveProtect, which features a pre-configured, all-in-one solution that streamlines IT management and centralizes data backup across different environments.

"Its advanced source-side deduplication technology reduces storage demands by over 50% and saves up to 99% of transmission bandwidth, helping businesses minimize infrastructure costs while ensuring fast and reliable recovery," Ms. Weng said.

ActiveProtect also allows users to scale their data easily as needed. It can also detect and restore corrupt data, verify backups, and test disaster recovery.

With the solution, a company can protect up to 150,000 workloads and monitor up to 2,500 sites and view its entire backup infrastructure, including primary backups, backup copies, tiered, and archived data.

Following its post-pandemic surge, the company expects significant growth as more firms shift to digital operations and hybrid work, Ms. Weng said.

For this year, the company is looking to expand its enterprise user base, she added.

"Since our last update in fourth quarter of last year, we remain optimistic about the Philippine market, which continues to be one of our fastest-growing countries in the Asia-Pacific region," Ms. Weng said.

"The demand for a scalable, secure, and user-friendly data protection solution has never been greater, and ActiveProtect is positioned to meet that need in the Philippines," Synology Regional Sales Manager Thachawan Chinchanakarn said in a separate statement.

As of 2024, Synology protects over 25 million workloads worldwide, managing over 350 extrabytes of data across 13 million servers. — **Beatriz Marie D. Cruz**

Is your mainframe a security blind spot?

By Praveen Kumar

OPINION

ALTHOUGH cloud platforms and applications have become widely popular, many businesses still rely on mainframes to handle their most mission-critical tasks. According to IBM, over 70% of information technology (IT) workloads worldwide are handled by mainframes — and business leaders are steadily increasing their reliance on mainframes in parallel with cloud-based technologies. This is reflected in the Asia-Pacific mainframe market's continued expansion, with GII Research expecting an increase in market value to about $1.78 million by 2030 from $1.249 million in 2022, with a compounded annual growth rate of 4.6%.

When it comes to security, companies have traditionally considered mainframes to be safer and far less vulnerable to cyberattacks. Such perceptions can create a false sense of security and cause organizations to prioritize other security investments and neglect important mainframe enhancements over time.

In life and in the realm of business, perceptions that don't match reality can be perilous, especially amid the growing threat of cyberattacks in the Asia-Pacific region. In the Philippines, the Department of Information and Communications Technology's National Cybersecurity Plan showed that the National Computer Emergency Response Team tracked 57,400 cybersecurity threats and managed 3,470 incidents from 2021 to February 2023. Most of these attacks targeted critical sectors such as government emergency systems (61%), academia (13%), and telecommunications (8%). These attacks can be financially devastating, with a PwC report showing that 35% of organizations suffered losses anywhere from $1 million to $20 million over the past three years.

The rise in frequency and potency of cyberattacks is a consequence of threat actors' improving sophistication, as cybercriminals now have access to advanced technologies and artificial intelligence (AI)-powered tools. The only logical response to this is for organizations to evolve accordingly.

COMMON MAINFRAME VULNERABILITIES

While mainframes have a reputation for robust security, they are hardly immune to vulnerabilities. In the Philippines where digital transformation is rapidly advancing, the risk of cyberthreats is also on the rise. Statista reported that data breaches in the Philippines reached roughly 140,000 in the fourth quarter of 2023 driven by rapid digitalization, advanced hacking techniques, and insufficient cybersecurity measures. Given the growing reliance on mainframes in industries that handle mission-critical operations, businesses must rethink their approach to mainframe security.

Awareness is always the first step, and every organization should understand the following vulnerabilities:

– Configuration-based vulnerabilities, stemming from errors in system setup and parameters, create unintended access points for malicious actors.

– Code-based vulnerabilities grow out of programming errors or flaws within the mainframe's software code, which can be exploited by malicious actors as entry points to infiltrate the system to siphon off data or cause system disruptions.

– Insider threats also pose a significant risk. Employees and contractors with authorized access can be weak links.

– Relying solely on passwords significantly weakens mainframe security. Multi-factor authentication (MFA), for instance, adds a layer of protection by requiring multiple forms of verification.

PRACTICAL STEPS TO WIN CONTROL BACK

New research by Rocket Software found that only 28% of IT leaders said they can assure that they could proactively navigate threats despite acknowledging mainframe security as a top priority.

To protect mainframe systems effectively and improve confidence, organizations should consider the following:

– Employ a mainframe security architect — A dedicated security architect aids the design and maintenance of a secure mainframe environment that is also tailored for an organization's specific needs.

– Implement code-based vulnerability scanning — Regularly scrutinizing code for vulnerabilities helps identify issues before they escalate into more serious threats.

– Conduct regular mainframe penetration tests — To uncover possible weaknesses, scheduled penetration testing can unlock valuable insights, which can be used to enhance defenses.

– Implement real-time compliance checking — Compliance is crucial for cyber resilience, and continuously monitoring adherence to organizational policies ensures alignment with regulations and upholds mainframe security.

– Deploy MFA systemwide — MFA is central to a modern cybersecurity strategy. Implementing MFA across the system adds an additional layer of security that minimizes the risk of unauthorized access.

PROTECT YOUR BUSINESS, INVEST IN MAINFRAME SECURITY

The Philippine government is driving digital growth through infrastructure improvements and fostering local business development. As part of this effort, mainframes play a critical role in supporting essential functions for banks, government institutions, and large firms, but as cyberthreats evolve, organizations cannot afford to overlook their mainframe security. Failing to address these vulnerabilities not only increases the risk of financial losses and exposure to potential liabilities but also makes compliance with crucial regulations, such as PCI 4.0 or the Payment Card Industry Data Security Standard and the Data Privacy Act, more difficult.

IT and security leaders need to understand that mainframe security is an ongoing commitment and not just a one-time task. By being constantly aware of the vulnerabilities inherent to mainframes and implementing proactive security measures, they can significantly bolster their organization's defenses against costly breaches and stay within the bounds of industry regulations.

Praveen Kumar is the vice-president for Asia-Pacific at Rocket Software.

Fintech companies caught up in US tariff turmoil

FINANCIAL TECHNOLOGY (fintech) companies like Robinhood and buy now, pay later provider Affirm have been caught in the whirlwind of President Donald J. Trump's sweeping tariffs, sending shares sharply downward amid fears about worsening consumer finances.

Global markets have been battered since Trump last week introduced a new baseline 10% US tariff on goods from all economies. Investors fear that the duties could lead to higher prices, weaker demand and potentially a global recession.

That could spell trouble for fintech companies, many of which rely heavily on consumers to be able to repay loans and deploy extra income toward stocks and other investments.

Some fintech companies, including Affirm and Robinhood, also earn fees from debit card and credit card purchases — revenue that could be vulnerable if consumer spending cools.

While banks can have a diverse client base that could insulate firms from sudden market contractions, fintech companies are more likely to serve consumers that would be at the forefront of an economic shock, analysts say.

"A recession typically hits nice-to-have mass-market consumer businesses, including fintechs, harder than other sectors because the first group to pull back spending in a recession is lower-income consumers," said James Ulan, director of research, emerging technology at PitchBook.

Shares in Affirm are down more than 21% since Mr. Trump launched his global trade war on April 2, while shares in Robinhood are down more than 17%. Shares in SoFi, which offers loans and banking services, are down nearly 20%.

"The adoption of honest financial products like Affirm is a secular and enduring trend across market cycles," a spokesperson for Affirm said. "Against a backdrop of increased market volatility and uncertainty, Affirm's products become even more compelling to both consumers and merchants."

Robinhood declined to comment. A spokesperson for SoFi did not immediately respond to a request for comment.

For companies that extend credit, like Affirm and SoFi, worsening consumer sentiment and fears that tariffs could drive up prices have called into question the ability of borrowers to pay off loans.

Affirm reported that for the quarter ending Dec. 31, 2.5% of its monthly loans were delinquent by more than 30 days. That was a slight increase compared with the year prior, but the company attributed that increase to a pricing adjustment.

SoFi said that for the quarter ending Dec. 31, 0.55% of its personal loans were delinquent by more than 90 days.

Across banks, 2.75% of consumer loans were more than 30 days delinquent for the quarter ending Dec. 31, according to the US Federal Reserve.

"We know renewed inflation would be a drag on consumer credit. It crowds out excess cash flows, which means you have deteriorating ability to pay off debt," said John Hecht, an analyst at Jeffries.

Goldman Sachs joined other investment banks in raising the odds of a US recession on Monday due to fears that Mr. Trump's tariffs would roil the global economy. Mr. Trump has said his policies could cause short-term pain, but will ultimately boost the US economy and add more American jobs.

"The administration's talking point seems to be tariffs are a one-time price adjustment different from systemic inflation. Now I would say, to the average household, higher prices are higher prices," said Ted Rossman, senior industry analyst at Bankrate, a consumer finance publisher.

US consumer sentiment had already plunged to a nearly 2-1/2-year low in March amid worries that tariffs would boost prices and undercut the economy, according to the University of Michigan Surveys of Consumers.

Still, some analysts are optimistic about how fintech companies might fare.

If Mr. Trump's tariffs push down Treasury yields, the cost of borrowing for companies could become much cheaper, making it less risky for lenders to extend credit, said Dan Dolev, senior analyst at Mizuho.

"This could have unintended positive consequences for all these names. I'm much more optimistic than what the market is suggesting right now," he said. — ***Reuters***