भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

सेबी/एच ओ/आईटीडी/आईटीडी_वीएपीटी/पी/सीआईआर/2023/032
SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 *February 22, 2023*

प्रति / To,

सभी स्टॉक एक्सचेंज / All Stock Exchanges
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन) / All Clearing Corporations
सभी निक्षेपागार (डिपॉज़िटरी) / All Depositories
सभी स्टॉक दलाल - एक्सचेंजों के जरिए / All Stock Brokers through Exchanges
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) - निक्षेपागारों (डिपॉज़िटरी) के जरिए
All Depository Participants through Depositories
सभी म्यूचुअल फंड / आस्ति प्रबंध कंपनियाँ (असेट मैनेजमेंट कंपनी) / न्यासी (ट्रस्टी) कंपनियाँ / म्यूचुअल फंडों के न्यासी मंडल / एएमएफआई / All Mutual Funds / Asset Management Companies / Trustee Companies / Boards of Trustees of Mutual Funds / Association of Mutual Funds in India (AMFI)
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ / All KYC Registration Agencies
सभी अर्हित निर्गम रजिस्ट्रार (रजिस्ट्रार टू एन इश्यू) / शेयर अंतरण अभिकर्ता (शेयर ट्रांसफर एजेंट)
All Qualified Registrars to an Issue / Share Transfer Agents

महोदय / महोदया,
Dear Sir / Madam,

विषयः साइबर सुरक्षा हेतु बेहतरीन पद्धतियाँ अपनाए जाने के संबंध में सेबी द्वारा विनियमित (रेग्यूलेटेड) एंटिटियों के लिए एडवाइज़री

Sub: Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices

1. यह देखने में आया है कि वित्तीय क्षेत्र के संगठन, स्टॉक एक्सचेंज, निक्षेपागार (डिपॉज़िटरी), म्यूचुअल फंड और वित्तीय क्षेत्र की अन्य एंटिटियाँ साइबर हमलों की समस्याओं से जूझ रही हैं और साथ ही इन हमलों की तादाद तेजी से बढ़ रही है और

1. Financial sector organizations, stock exchanges, depositories, mutual funds and other financial entities have been experiencing cyber incidents which are rapidly growing in frequency and sophistication.

जिनके नए-नए हथकंडे अपनाए जा रहे हैं । चूंकि वित्तीय एंटिटियों का कामकाज किसी न किसी रूप में या तो एक दूसरे से जुड़ा हुआ है या फिर एक दूसरे पर निर्भर रहता है, यही वजह है कि साइबर हमलों का खतरा आखिरकार किसी एक एंटिटी के सिस्टम (जिनमें वे सिस्टम भी शामिल हैं जिन पर उसका नियंत्रण हो), नेटवर्क आदि पर ही नहीं मंडराता, बल्कि इसका असर तो दूसरी एंटिटियों के सिस्टम, नेटवर्क आदि पर भी पड़ता है ।

Considering the interconnectedness and interdependency of the financial entities to carry out their functions, the cyber risk of any given entity is no longer limited to the entity's owned or controlled systems, networks and assets

2. यही नहीं, बल्कि साइबर हमले करने वाले जिस तरह पूरी साँठगाँठ करके साइबर हमले करने के लिए नए-नए हथकंडे अपनाते जा रहे हैं, उसके चलते अब हमें यह मानना ही होगा कि जोखिम को कम करने (रिस्क मैनेजमेंट) के लिए और संचालन (गवर्नेंस) को सुनिश्चित करने के लिए अब तक जो-जो तौर-तरीके अपनाए जाते थे, वे आज के माहौल में अब शायद इतने कारगर नहीं रहे कि नए-नए पैंतरे अपनाकर आज किए जा रहे साइबर हमलों से निपट पाएँ और न ही इतने कारगर रहे हैं कि सार्वजनिक क्षेत्र की तथा निजी क्षेत्र की कंपनियों में तकनीक की दिशा में हो रहे बदलावों के साथ कदम से कदम मिलाकर चल पाएँ ।

2. Further, given the sophistication and persistence of the threat with a high level of coordination among threat actors, it is important to recognize that many traditional approaches to risk management and governance that worked in the past may not be comprehensive or agile enough to address the rapid changes in the threat environment and the pace of technological change that is redefining public and private enterprise.

3. इसलिए, विनियमित एंटिटियों के लिए यह जरूरी है कि वे साइबर हमलों पर न केवल कारगर ढंग से काबू पाएँ, बल्कि सिस्टम को सामान्य स्थिति में भी लाएँ, ताकि ऐसे हमलों की वजह से वित्तीय स्थिरता पर आँच न आए।

3. Thus, an efficient and effective response to and recovery from a cyber-incident by REs are essential to limit any related financial stability risks. For ensuring the same,

यही सुनिश्चित करने के लिए, 'फाइनेंशियल कंप्यूटर सिक्यूरिटी इंसिडेंट रिस्पॉन्स टीम' ने सेबी के पास प्रस्तुत की गई अपनी रिपोर्ट में अपने अहम सुझाव दिए हैं । इस प्रकार जो भी सुझाव लागू हैं, वे इस परिपत्र (सर्कुलर) के साथ "संलग्नक-क" में एडवाइज़री के रूप में संलग्न हैं ।

Financial Computer Security Incident Response Team (CSIRT-Fin) has provided important recommendations in its report sent to SEBI. The applicable recommendations, in the form of an advisory, are enclosed at *Annexure-A* of this circular.

4. इस एडवाइज़री के साथ-साथ सेबी के लागू परिपत्रों (जिनमें साइबर सुरक्षा तथा साइबर आघात सहने संबंधी ढाँचा, वार्षिक सिस्टम ऑडिट संबंधी ढाँचा, आदि विषयों पर जारी किए गए परिपत्र भी शामिल हैं) और उसके बाद सेबी द्वारा समय-समय पर दी जाने वाली सूचनाओं आदि (अपडेट) पर भी अवश्य गौर किया जाए ।

4. This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework, Annual System Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

5. विनियमित (रेग्यूलेटेड) एंटिटियाँ अपनी साइबर सुरक्षा की ऑडिट रिपोर्ट (यह ऑडिट साइबर सुरक्षा और साइबर आघात सहने के संबंध में सेबी द्वारा निर्धारित किए गए ढाँचे के अनुसार किया गया हो) के साथ इस एडवाइज़री का पालन किए जाने के संबंध में भी रिपोर्ट प्रस्तुत करेंगी । यह रिपोर्ट रिपोर्टिंग की मौजूदा व्यवस्था के अनुसार प्रस्तुत की जाएगी और यह रिपोर्ट साइबर सुरक्षा की ऑडिट रिपोर्ट प्रस्तुत करते समय प्रस्तुत की जाएगी ।

5. The compliance of the advisory shall be provided by the REs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism and frequency of the respective cybersecurity audit.

6. इस परिपत्र के साथ संलग्न एडवाइज़री तुरंत प्रभाव से लागू होगी ।

6. The advisory annexed with this circular shall be effective with immediate effect.

7. यह परिपत्र (सर्कुलर) प्रतिभूतियों (सिक्यूरिटीज़) में निवेश करने वाले निवेशकों के हितों का संरक्षण करने, प्रतिभूति बाजार (सिक्यूरिटीज़ मार्केट) के विकास को बढ़ावा देने तथा उसे विनियमित (रेग्यूलेट) करने की दिशा में, भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 1992 की धारा 11(1) के तहत प्रदान की गई शक्तियों का प्रयोग करते हुए जारी किया जा रहा है ।

7. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

भवदीय / Yours Faithfully,

श्वेता बनर्जी Shweta Banerjee
उप महाप्रबंधक Deputy General Manager
दूरभाष / Phone: 022-26449509
ईमेल / Email: shwetas@sebi.gov.in

Annexure-A

In view of the increasing cybersecurity threat to the securities market, SEBI Regulated Entities (REs) are advised to implement the following practices as recommended by CSIRT-Fin:

1. **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer**:
   REs are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.

2. **Measures against Phishing attacks/ websites**:
   i. The REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
   ii. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.

3. **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**
   i. All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
   ii. Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time.

The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.

4. Measures for Data Protection and Data breach:

i. REs are advised to prepare detailed incident response plan.
ii. Enforce effective data protection, backup, and recovery measures.
iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.
iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.
v. Deploy data leakage prevention (DLP) solutions / processes.

5. Log retention:

Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.

6. Password Policy/ Authentication Mechanisms:

i. Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.
ii. Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
iii. Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

7. Privilege Management:

i. Maker-Checker framework should be implemented for modifying the user's right in internal applications.
ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should

be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.

8. Cybersecurity Controls:

i. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.

iii. Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

iv. Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.

v. Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

9. Security of Cloud Services:

i. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.

ii. Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.

iii. Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.

iv. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

10. Implementation of CERT-In/ CSIRT-Fin Advisories:

The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.

11. Concentration Risk on Outsourced Agencies:

i. It has been observed that single third party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.

ii. Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.

iii. Further, REs also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.

12. Audit and ISO Certification:

i. SEBI's instructions on external audit of REs by independent auditors empaneled by CERT-In should be complied with in letter and spirit.

ii. The REs are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cybersecurity.

iii. Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits.