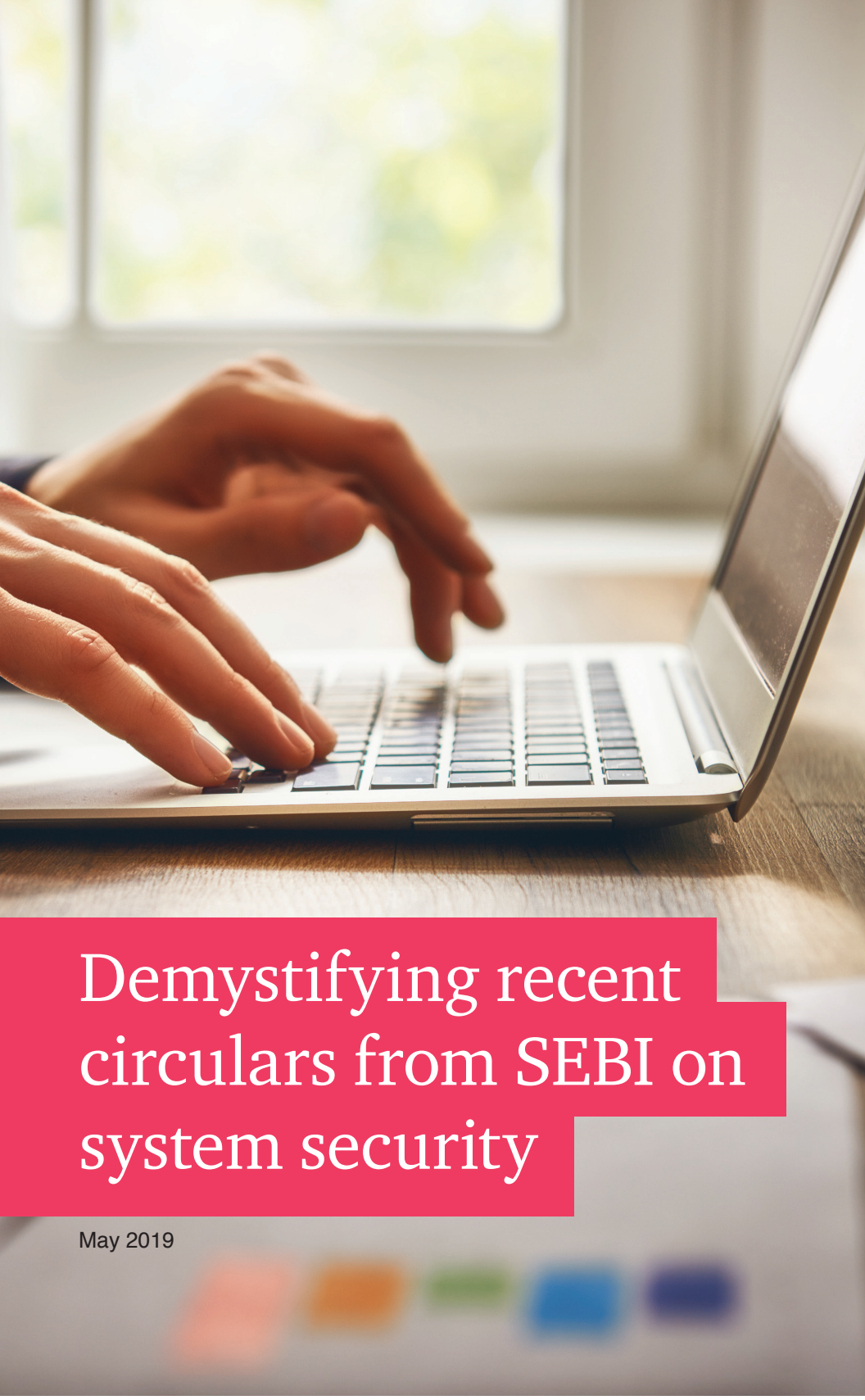


Demystifying recent circulars from SEBI on system security

May 2019

pwc

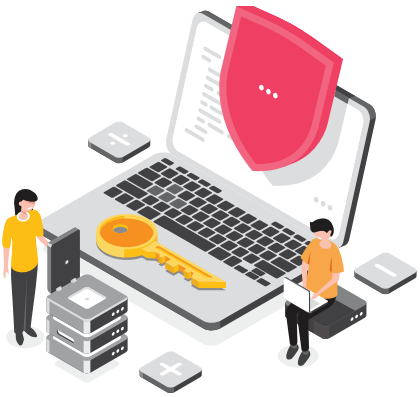
Background

Since 2009, the Securities and Exchange Board of India (SEBI) has sought to focus on securing systems and processes in asset management companies (AMCs). Due to rapid technological advancement in the securities market, SEBI has issued a couple of circulars on cyber security this year to enforce the importance of system security. We believe that the circulars are comprehensive in terms of their approach, although they are fairly onerous in terms of expectations from the AMC fraternity. AMCs should not take a compliance-centric view of these circulars, and instead should truly recognise the real threat landscape in the context of the recent cyberattacks in the financial services (FS) sector.

While SEBI has set clear expectations regarding greater participation of the board and top management and has done a commendable job with respect to the coverage and vision of the circular, in our view, implementation-centric approaches will need to be developed. In many ways, this is an opportunity for AMCs to take a step forward and assess themselves with a view to improving their cyber security posture.

We believe that this circular will improve the cyber security posture of the AMC industry, largely in the following areas:

1. Strong cyber security governance
2. Building cyber resilience
3. Protecting customer data
4. Continuous surveillance
5. Focus on extended ecosystem
6. Proactive audit and collaboration
7. Adequate training
8. Foolproof business controls



Strong cyber security governance

AMCs will need to create programmes and interventions in order to sensitise the board and management towards the evolving threat landscape and the current and future state of their cyber security posture. This will help in setting the right tone at the top. The circular clearly calls for greater participation of the board in terms of creating a technology committee comprising experts proficient in technology. They can no longer be just a ratifying body and will instead need to be more involved and keep abreast of the latest cyber security developments and accordingly provide necessary guidance and insights.

Building cyber resilience

As attack vectors are becoming increasingly sophisticated, the cost of launching an attack is going down, the scale and velocity of attacks are increasing, and there is greater recognition of the possibility of incidents. Accordingly, AMCs not only need to strengthen cyber defence but also build strong resilience. The SEBI circular calls for the establishment of a cyber resilience framework to address the full life cycle of identify, protect, detect, respond and recover.

Protecting customer data

The circular lays emphasis on protecting customer data and protecting customers against financial crimes. AMCs are required to put in place strong controls to protect customer data across the life cycle regardless of whether data is at rest or in motion, within their own environment or within the vendor's environment.

Continuous surveillance

There is a need for effective cyber security monitoring and detection capabilities that focus on building resilient systems that traverse a large volume of system events and deduce intelligence. A resilient ecosystem is characterised by its ability to detect threats in advance, prevent cyber incidents, recover from an incident should one materialise, and learn from threat intelligence to prevent similar incidents. AMCs will have to shift some of their security operations priorities and augment their current security operations centre (SOC) to make it more robust by focusing on cyberthreats on a real-time basis.

Focus on Extended Ecosystem

There is also a clear recognition that information cuts across boundaries and it is no longer adequate to have strong controls with respect to security within the organisation and a light-touch approach to the vendor ecosystem. The circular calls for strong governance over the entire vendor life cycle with respect to cyber security. AMCs would need to embed into their relationship with all vendors the right to audit and the fact that they may be subjected to review by the regulator itself.

Proactive audit and collaboration

AMCs can only achieve so much by improving their organisational cyber security capabilities based on historical incidents and generic threat intelligence. In its circular, SEBI has recognised that collaborating with and contributing to financial institutions can have mutual benefits and further help others to make informed decisions, thus enabling them to respond to attacks proactively and quickly. In many ways, the circular will move the industry to a new evolved state with respect to cross-leveraging learnings from one another.

Adequate training

AMCs have been asked to establish strong training programmes focused on enhancing the awareness levels of employees, outsourced staff and vendors in order to reduce the incidence of attacks and increase resilience.

Foolproof Business Controls

The circular has not only prescribed technical controls to prevent breaches but also put adequate emphasis on embedding process control in the business functions. SEBI has defined clear segregation of multiple business functions, especially for its mutual fund operations, and provided guidelines for controls that need to be established under each of the functions. All this is aimed towards better management of operational risk, considering the fact that mutual fund schemes are essentially pools of public money managed by professional asset managers.

How can PwC help?

1

Gap analysis

Perform assessment to determine if existing controls satisfy requirements mentioned in the SEBI circular.

2

Remediation

Develop work streams to address identified control gaps via both technology and process changes.

3

Attestation

Validate successful compliance with the SEBI circular controls and transition to ongoing compliance team..

Additional services

Cyber security services	Business process services
Penetration testing	Review of existing processes and workflows
Cyber security benchmarking	Design and document target state processes and workflows
Red team testing	Review functional and tech architecture
Breach indicator assessment	Application portfolio rationalisation and vendor management strategy – in-house vs outsourced

Why PwC?

01

Deep AMC industry knowledge

PwC has been associated with many AMCs on a plethora of projects of varied scope, location, scale, duration and complexity. PwC understands the regulatory framework, organisation and culture of AMCs in India and is one of the pioneering organisations to have a dedicated vertical focusing on the industry. PwC has been providing consulting services in this sector for over a decade.

02

Experience in system audit

PwC has a vast amount of experience in the field of IT system review and has significantly contributed towards ensuring a high degree of assurance for many leading organisations across India and abroad.

03

Knowledge-driven consultancy

PwC has invested extensively in internal knowledge management initiatives. It has identified relevant knowledge manager best practices both within and outside the firm, and created an integrated and effective knowledge management function. PwC leverages these knowledge management tools to provide the best value to its clients.

04

Adapting to your requirements

PwC will formulate and tailor an approach that suits your immediate requirements and future ambitions. To achieve these, PwC will provide pragmatic insights and balanced views on how to prioritise any associated actions.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

For deeper conversations, please connect with:

Siddharth Vishwanath
Partner, Cyber Security
M: +91 9167190944
E: siddharth.vishwanath@pwc.com

Anirban Sengupta
Partner, Cyber Security
M: +91 9810755426
E: anirban.sengupta@pwc.com

Unnikrishnan Padinjyaroot
Partner, Cyber Security
M: +91 9845118097
E: unnikrishnan.padinjyaroot@pwc.com

PVS Murthy
Partner, Cyber Security
M: +91 9867743050
E: pvs.murthy@pwc.com

Amol Bhat
Director, Cyber Security
M: +91 9823264155
E: amol.bhat@pwc.com

pwc.in

Data Classification: DC0

KS/May2019-17667