RBI's circular on cyber security

Role of CEOs and the questions they should ask

pwc

Background

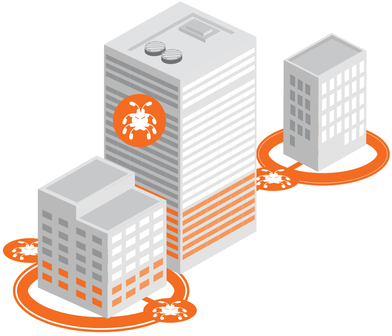
The banking sector is the backbone of the financial system in India and as such it needs to be secure and be able to withstand, detect, rapidly respond and recover from ***precision cyberattacks***. Achieving this objective requires ***integrated cyber resilience strategies*** and ***coordinated continual efforts*** to adequately prepare, prevent, detect, mitigate, respond, and recover against the ever-growing menace of advanced cyberattacks.

We believe that RBI's circular on cyber security is both ***timely and comprehensive*** in its approach while being fairly onerous in terms of expectations from the banking fraternity. Banks should not take a compliance-centric view to this circular, and instead should truly recognise the ***real threat landscape*** in the context of the recent events of cyberattacks such as the Bangladesh Bank hacking incident. We believe this circular is an opportunity for banks to adopt an outcome-centric approach to move towards a ***robust cyber defence mechanism***.

The regulator has set a clear expectation on ***greater participation of the board and top management***. According to the circular, cyber security should no longer be the focus of just the CISO, but will also need to be on the ***CEO's agenda***. While RBI 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. We, at PwC are taking the lead and working with the CISO community to develop some of these implementation themes.

We believe this circular will shift the cyber security needle for the banking industry largely in the following areas:

Business-enabling technology is fast evolving



Need for a forward-looking cyber security framework—RBI's circular is timely

Complex threat landscape

Cyber-aware board and strong governance

Building cyber resilience

Protecting customers

Focus on extended ecosystem

24x7 security operations centre with adaptive threat defence mechanisms

Proactive reporting and collaboration

CEOs need to focus on the following themes:

Cyber-aware board and establishment of strong governance

Banks will need to create programmes and interventions in order to sensitise the board and management about 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. No longer can they just be a ratifying body and instead they will need to be more involved and keep abreast about the latest cyber security developments and accordingly provide necessary guidance and insights.

Building cyber resilience

As attack vectors are increasingly becoming 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, banks not only need to strengthen cyber defence but also build strong resilience. The RBI circular calls for the establishment of a Cyber Crisis Management Plan to address the full life cycle of detection, response, containment and recovery.

Protecting customers

The circular lays emphasis on protecting customer data and protecting customers against financial crimes. Banks 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 the bank's environment or within the vendor's environment. As banks are rapidly adopting digital products, they are also mandated to take stronger measures in areas such as authentication and risk-based transaction monitoring to prevent fraud.

Banks have also been asked to establish strong programmes focussed on customer awareness to reduce the incidence of attacks such as phishing.

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 bank 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. Banks 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.

24x7 security operations centre with adaptive threat defence mechanisms

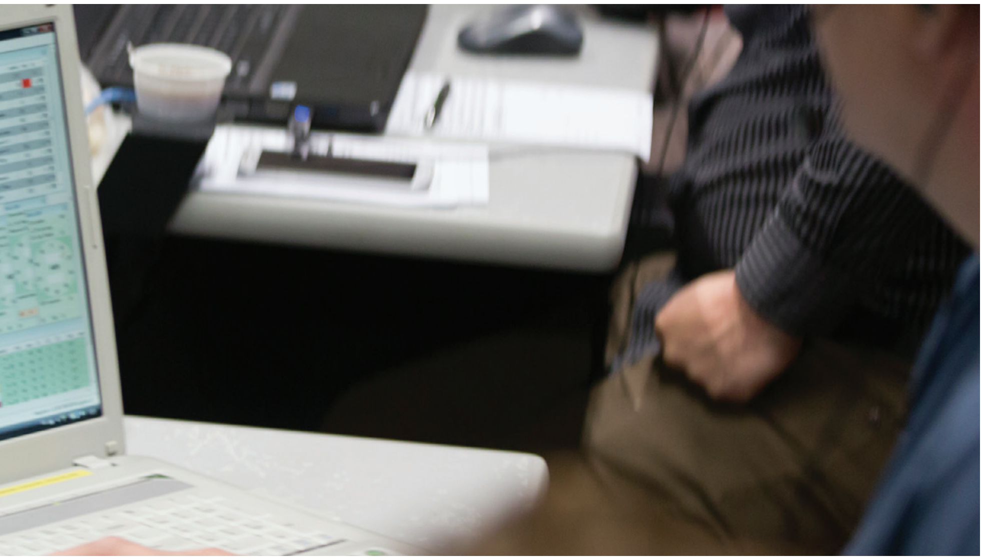
There is a need for effective cyber security monitoring

and detection capabilities that focus on building resilient systems that traverse a large volume of system events and deduce intelligence. A resilient banking ecosystem is characterised by banks' 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. Banks will have to refocus some of their security operations priorities and augment their current security operations centre (SOC) to make it more robust by focussing on cyberthreats on a real-time basis. The current practice of analysing security logs passively must be challenged to implement advanced systems or improved such that analysis occurs real time or near real time. Banks would need to move from basic security operations capabilities to setting up advanced next generation security operations centres with capabilities such as analytics enabled by device and user behaviour based machine learning and defence.

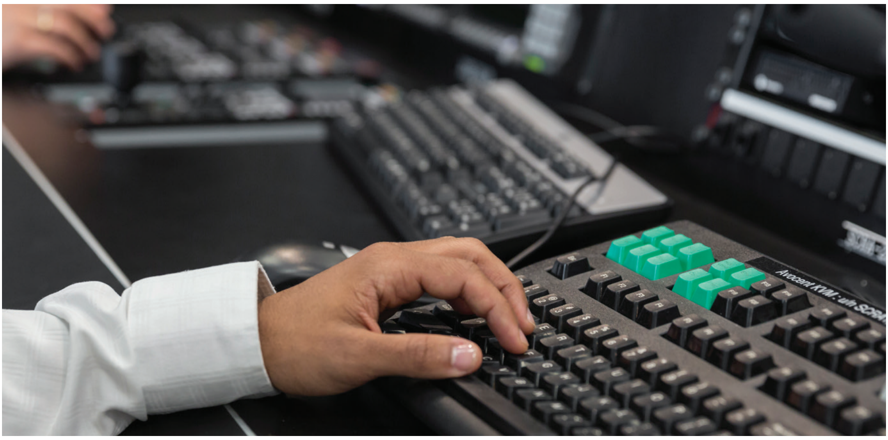
Proactive reporting and collaboration

Financial institutions can only achieve so much by improving their organisational cyber security capabilities based on historical incidents and generic threat intelligence. In its circular, RBI has recognised that collaborating and contributing financial institutions can benefit mutually 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.



Key questions that PwC believes CEOs should consider in order to build effective cyber security programmes

- Is an integrated cyber security strategy a pivotal part of our business model? Does the strategy consider the full scope of security: technical, process, and human capital? Have we applied the required resources and investments?
- Does our leadership team understand the implications of cyberthreats? Do we have the right tone at the top to ensure appropriate implementation of cyber security?
- Is the effectiveness of a cyber security programme measured through a clearly-defined security metric based scorecards and dashboards?
- Do we have a granular inventory of our IT assets, including information about OS/applications (example, MacBook Air, OSX 10.0, JRE, Adobe Flash, .NET, etc.) and is our strategy for managing known or unknown cyberthreat vectors aligned to risk-based IT asset prioritisation?
- Are we aggregating and analysing both internal as well as external cyberthreat intelligence? Is cyberthreat intelligence fully integrated with real-time monitoring, detection and cyber response capabilities?
- Do we know what needs to be done in the event of a cyber crisis? Do we have the right technology and skilled resources to be able to detect, contain and resurrect from a cyber crisis?
- Do we actively monitor, audit, and remediate cyber risk emanating on account of vendors? Do we have a cyber security policy and related controls which can be extended throughout the life cycle of the vendor relationship?
- Do we have an awareness programme that addresses all stakeholders, including top management, board, employees, customers and partners?
- Do we have risk-based continuous surveillance systems to protect customers from fraudulent transactions?



Important dates

Activities	*End date*	*Activities*	*End date*
Submission of final gap assessment report to RBI	*31 July 2016*	***Confirmation to RBI on board-approved cyber security policy and commencement of implementation of the policy***	*30 September 2016*

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 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.com/in

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

For deeper conversations, please connect with:

Sivarama Krishnan
Leader,Cyber Security
Tel: +91 (124) 626 6707
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
Tel: +91 (22) 66691559
siddharth.vishwanath@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
Tel: +91 (0) 80 4079 7027
manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
Tel: +91 (22) 6119 8171
sundareshwar.krishnamurthy@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
Tel: +91 (124) 626 6717
hemant.arora@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
Tel: +91 (22) 66691214
pvs.murthy@in.pwc.com

pwc.in

Data Classification: DC0

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.