RBI's circular on cyber security

pwc

www.pwc.in

Background

Since 2010, banks in India have rapidly adopted newer technologies and digital channels, with the underlying objective of increasing footprints and revenues. We have also seen customer preferences shift towards digital platforms. There is a perception, though, that the adoption of advanced cyber security practices has not kept pace with the rate of evolution of core business-enabling technology. While in comparison to several other sectors, banks are definitely seen to be more proactive in investing and improving security practices, such measures may still be inadequate considering the challenges that the industry is facing today. Some challenges with the traditional approach to IT security are:

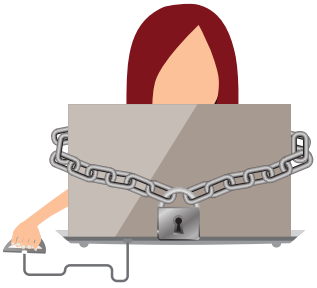
1. Proliferation of attack vectors and enhanced attack surface
2. Proliferation of digital and shifting customer preference
3. Sophistication of threat actors and enhanced targeting of banks
4. Banking increasingly operating as a 'boundary-less' ecosystem

Inadequate traditional IT security measures

A paradigm shift has recently been observed in attacks exploiting the source, behaviour, motives and vectors. This indicates that the traditional multilayered defence that banks already have is not adequate. Globally, there is a rise in cyber security incidents and several of them have been large-scale breaches, frauds and heists. The impact of such breaches does not end with serious financial loss but, in most cases, can also potentially erode substantial brand value.

RBI realises that banks need to take a holistic and integrated approach towards cyber security operation transformation.

RBI has taken a step in the right direction by realising the inherent need for banks to strengthen their cyber security posture in the wake of the increasingly sophisticated nature and quantum of attacks.



An opportunity for banks to establish next generation cyber defence

In many ways, through its circular, RBI holistically addresses several aspects related to cyber security that a bank should put in place. The circular is quite comprehensive in its coverage. It clearly recognises that cyber security focus is distinct from a focus purely on information security. Further, it clearly lays out the need for setting up a cyber security operations centre (SOC) and cyber-aware board and top management, focussing on securing the ecosystem, creating a resilience framework and ensuring proactive information sharing.

CISO has a key responsibility to act as an interface between business and technology.

In many ways, this is an opportunity for banks to take a step forward and assess themselves with a view to improving their cyber security posture. Chief information security officers (CISOs) of tier 1 banks should seize this opportunity to embark on a journey to establishing the next generation of cyber security defence, while CISOs of smaller banks should look to move from an asset-centric security approach to establishing a holistic baseline security programme. We believe that banks should guard against taking a compliance-centric approach to the circular.

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

- Cyber-aware board and establishment of strong governance
- Protecting customers
- Proactive reporting and collaboration within industry
- 24x7 operations centre with advanced real-time capabilities (continuous surveillance)
- Building cyber resilience
- Focus on extended ecosystem

Cyber-aware board and establishment of strong governance

Banks will need to create programmes and interventions 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. It will make cyber security as important as investing in business-enabling technologies.

Board-level awareness and participation critical

The circular also calls for banks to strengthen enterprise-wide cyber security governance. It articulates aspects that need the approval/oversight of the IT subcommittee of the board. Further, there is a clear emphasis on the establishment of metrics to measure and monitor outcomes of cyber initiatives.

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.

Protecting customer information and customers themselves from financial crimes

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

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.

Call for deeper collaboration within the industry and with the regulator

24x7 operations centre with advanced real-time capabilities (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 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.

Combating cyberthreats not possible without continuous surveillance and real-time analytical capabilities

Banks will have to refocus some of their security operations priorities and augment their current 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 to ensure that lateral movement of malicious code is prevented on a real-time basis using integrated honeypots. Static rule-based systems will have to make way for dynamic and adaptive security systems that draw intelligence based on behaviour analysis and detection capabilities across all categories of interconnected systems.

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.

A cyber crisis management plan must address the entire life cycle of incident detection, response, containment and recovery.

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.

Challenges for the industry

In our view, the journey towards upgrading cyber security driven by this circular, though very exciting, is fraught with several challenges that banks have to address. Banks are already considering several cost reduction strategies to address cost pressures such as managing non-performing assets (NPAs) and shrinking margins. In the wake of this, cyber security investment will not occur very easily. The circular highlights several aspects that banks need to adopt in their roadmap; however, there is a need to strike a balance between a wish list and realistic, achievable objectives. Banks will need to take a risk-based approach while building advanced capabilities; however, they may not be able to avoid baseline investments.

This circular will push the entire industry forward in terms of strengthening cyber defence, and detecting and building resilience both at the organisation and industry level. While some leading banks already have programmes addressing many of these issues, they too would need to strengthen their posture on many fronts.

From an implementation perspective, the details will still need more deliberation and we at PwC intend to take the front seat in working with leading banks to build reference guides.

About the authors

This point of view has been co-authored by Siddharth Vishwanath and Shashikant Pathak. Siddharth Vishwanath is a Partner and leads the Financial Services focus for the Cyber Security practice. Shashikant Pathak is an Associate Director with the Cyber Security practice; he works with several banks.

For deeper conversations, please reach out to

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

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 2,08,000 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.

SUS/July2016-6734