Deloitte.

Cybersecurity in the Indian banking industry: Part 1

Will 2020 redefine the cybersecurity ecosystem?

November 2020

Contents

Executive summary

The year 2020 has been quite challenging for Indian banks when it comes to cybersecurity. After the onset of the COVID-19 crisis, banking operations disrupted severely as banks struggled to provide uninterrupted services to their clients during various stages of lockdowns. In the following months, they accelerated their digital transition efforts (such as digital banking and remote access to employees) to ensure contactless business operations. With a surge in digitisation, banks also witnessed a spike in cyberattacks as cybercriminals found new opportunities and vulnerabilities.

In all likelihood, COVID-19 is here to stay. This means banks will have to keep a foot on the accelerator, and continue with digital transformation to sustain and thrive during and after the pandemic. This will also mean banks are likely to continue to experience rising financial frauds due to the increasing digital attack surface.

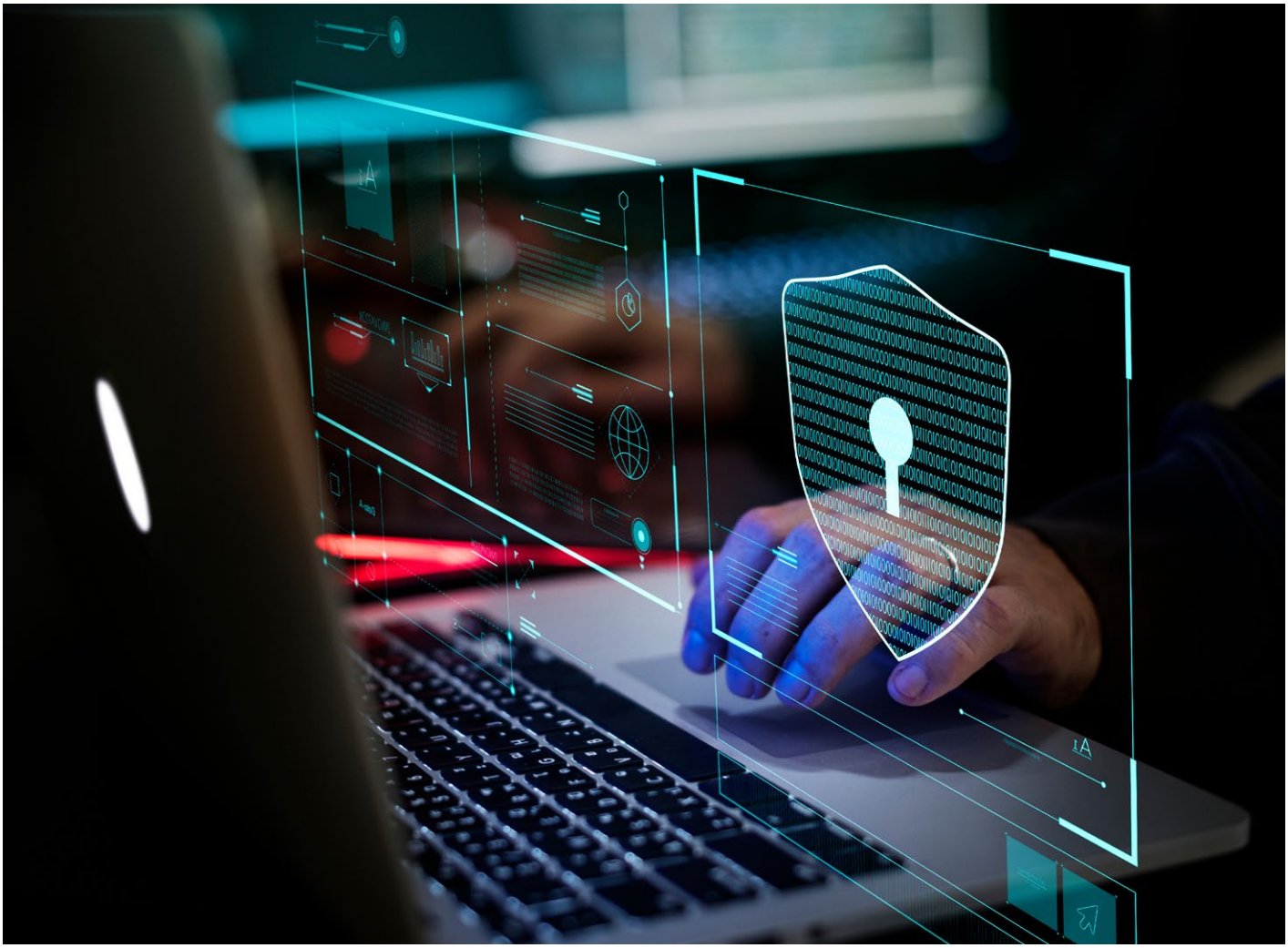
Rising cyber threats after COVID-19 pose serious concerns for Indian banks and the Reserve Bank of India (RBI). What makes the challenge acute is that different banks are currently at varying stages of digital transformation and cybersecurity maturity levels determined by their past investments, budget allocation, and size in terms of customer outreach and service offerings. To cope with challenges associated with COVID-19, bank executives will have to embrace new digitisation and cybersecurity norms to meet business requirements, irrespective of the cybersecurity maturity levels of their banks.

Bank executives need to be well prepared to analyse and respond to cyber incidents as they unfold, and manage consequences. Deloitte's two-series report focusing on cybersecurity in the banking industry is written with the following objectives in mind:

- Analyse the rising cybersecurity risks in banks after COVID-19 in the wake of rapid digitisation.
- Advocate the possible cybersecurity solutions for banks to cope with the challenges.
- Examine how the banking industry is responding to the changing operating environment (based on experts' views).

This is the first of the two-series report that attempts to answer three questions pertaining to the first two objectives mentioned above.

- Why will the pandemic result in rapid digitisation of banks unlike in the past?
- What will be the nature of cybersecurity challenges because of rapid digitisation?
- How can banks deal with cyber threats by focussing on a few suggested possible solutions?



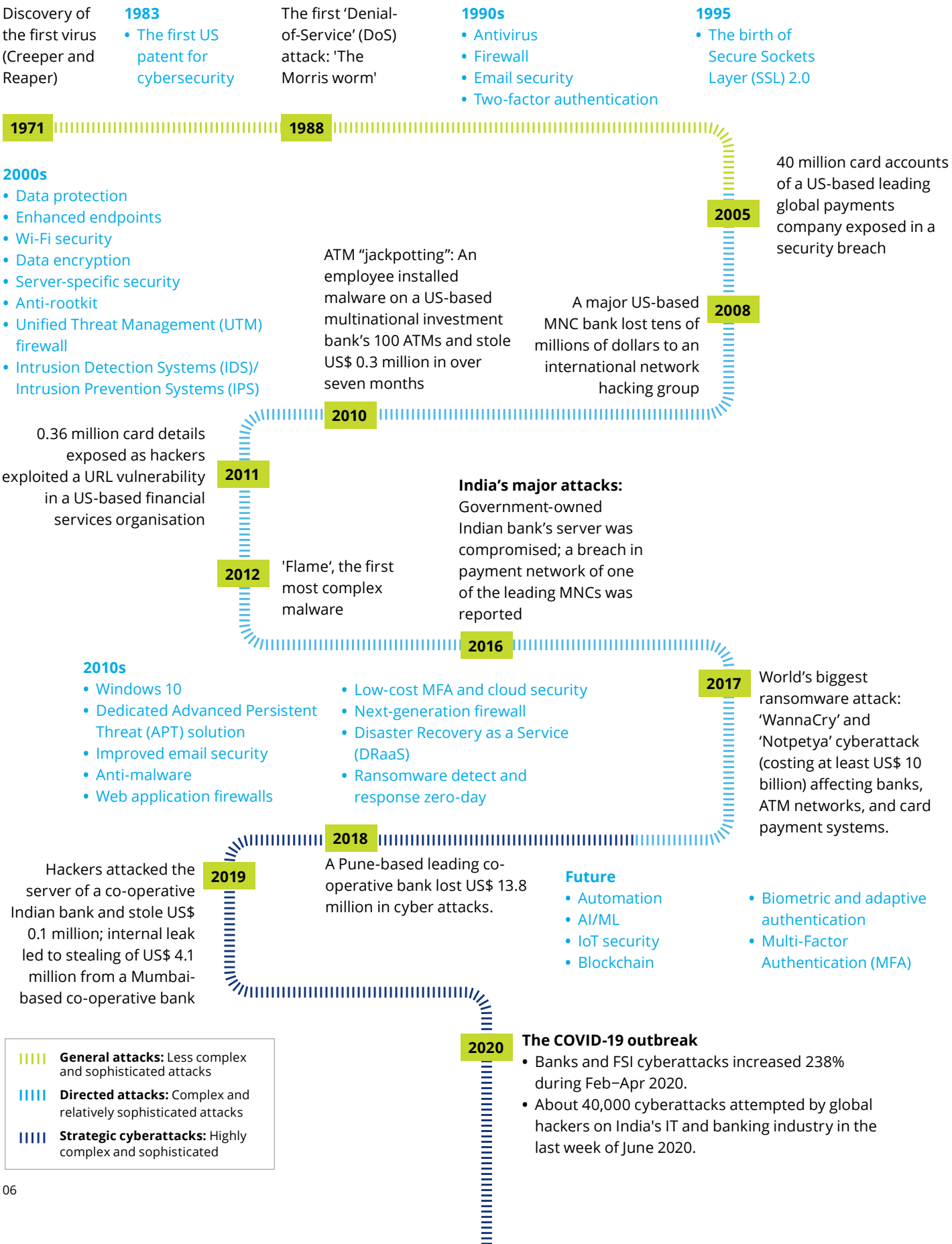
The past may not be prologue

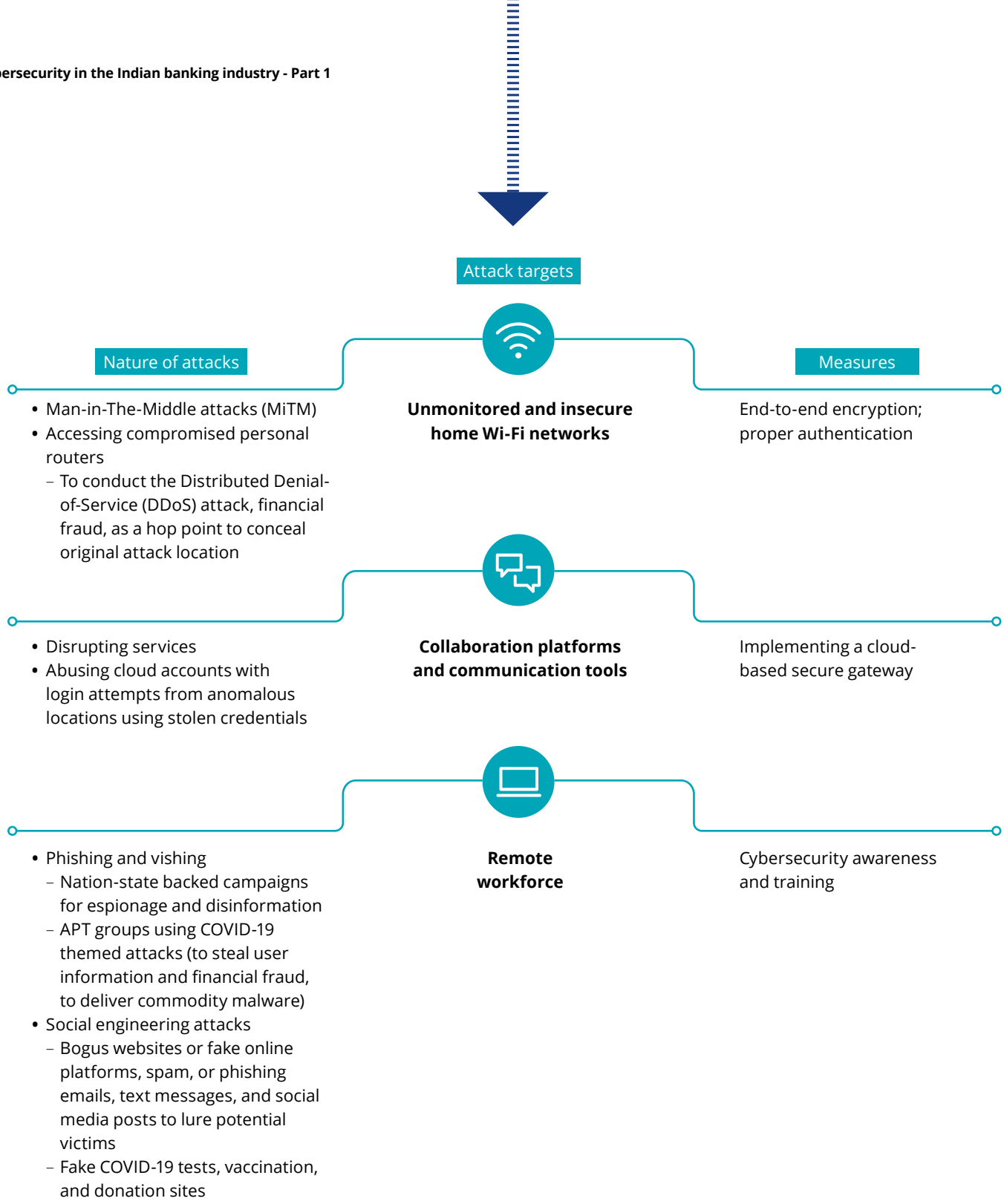
Since the pandemic has set foot worldwide in 2020, cyberattacks in banks have hogged headlines across the world. Moody warned banks globally of "increased risks of cyberattacks during the ongoing COVID-19 pandemic".[i] According to a VMware Carbon Black report, cyberattacks against banks and financial institutions globally increased 238 percent amidst the COVID-19 crisis between February 2020 and April 2020.[ii] Ransomware attacks increased nine times during the same period.

In India, the RBI red-flagged cybersecurity issues in its financial stability report in July 2020. The report underscored the challenges due to rising cyber threats with the banking industry being a primary target for such attacks.[iii] In a recent statement, the national security advisor affirmed that "financial frauds increased exponentially due to greater dependence on digital payment platforms following the COVID-19 pandemic".[iv] In other news, global hackers made headlines as they attempted more than 40,000 cyberattacks on India's banking industry, amongst others, over a period of five days in the last week of June.[v]

However, cybersecurity incidents are not new to the banking world. The history of the first cyber threat goes back to 1970 (Figure 1). For decades, banks across the world have been fighting countless borderless battles with faceless criminals in cyberspace. With the rapid digitisation of the banking industry (and other industries), cyber threats and attacks have become more pervasive and sophisticated. This has led to an increasing evolution of cybersecurity (Figure 1). The constant threat from cybercriminals compromising banks' defence systems has compelled them to understand the importance of individual cyberattacks, and comprehend patterns, sophistication, and life cycle of such threats they face daily to protect their businesses.

Figure 1: The evolution of cyber threats; cyberattacks in the financial industry; and the cybersecurity

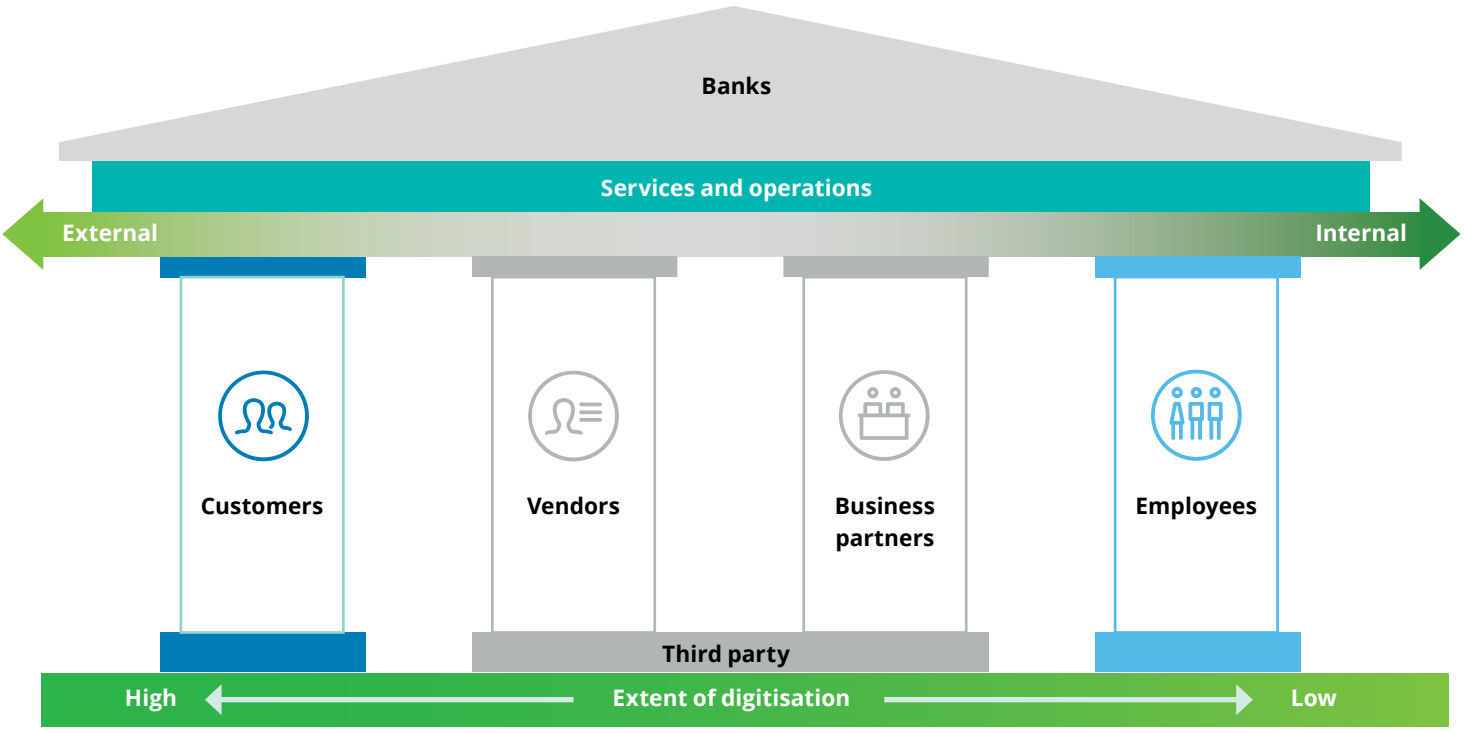




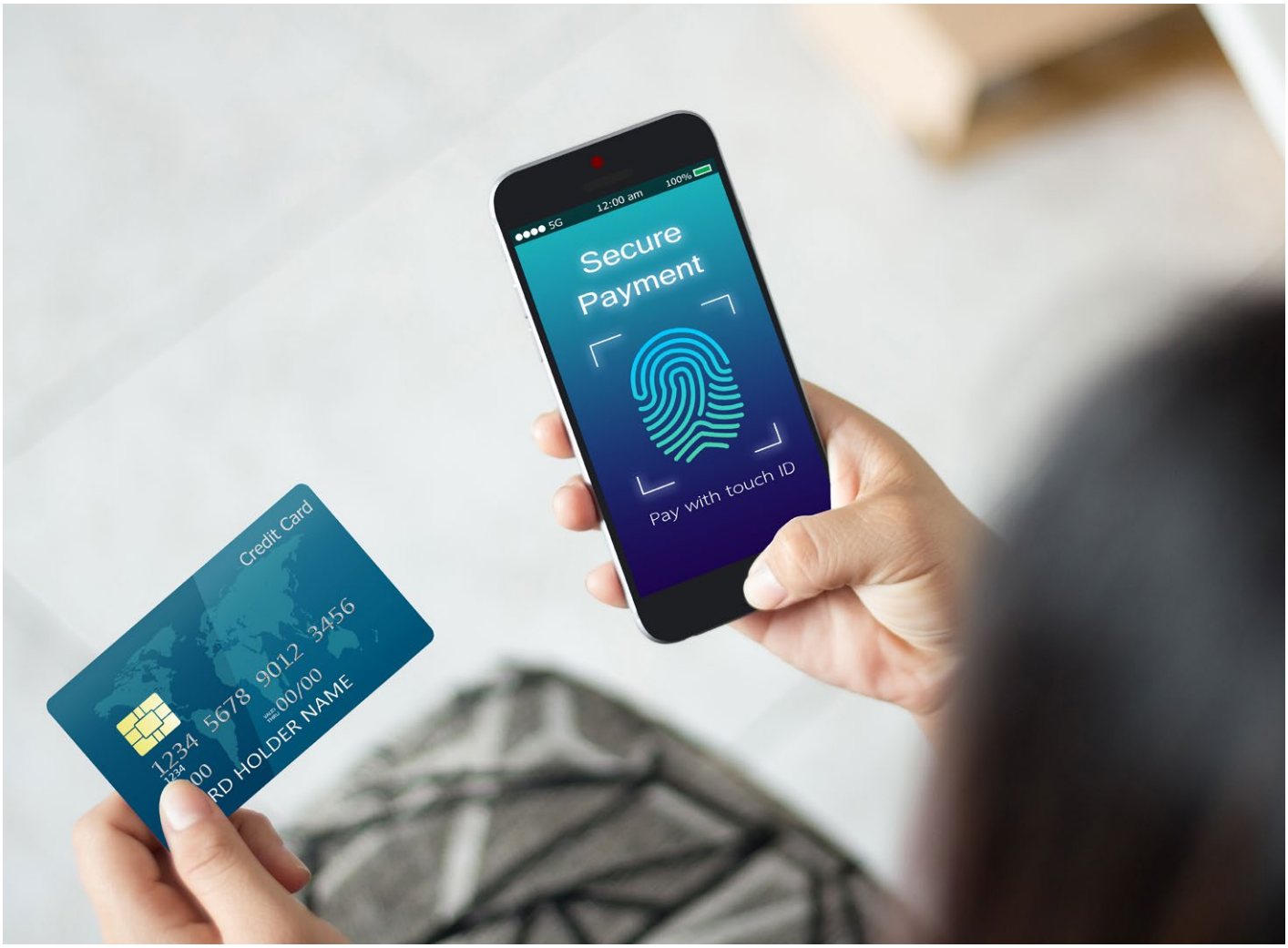
Source: Deloitte Research[vi]

Indian banks have seen a steady rise in cyber threats as they have been exploring or embracing complex technologies (such as mobile and internet banking), improving employee intranet, and more recently, adopting hybrid cloud technology. As a result, they have been selective in adopting digitisation in the past. Before the COVID-19 crisis, a majority of the Indian banks focused on strategic digitisation of their customer services and experiences − one of the four pillars of the banking ecosystem (Figure 2). The rapidly changing behaviour and preferences amongst rising urban customers, millennials, and the middle-income population (demanding faster solutions and better customised products) drove digitisation in services to customers. On the other hand, usages of digital technologies amongst the other three stakeholders—employees, business alliances, and vendors—were measured and gradual. This is partly because of the complexity of operations and the associated degree of cyber risks. In the future, this trend of selective digitisation will change because of the evolving trends in the post COVID-19 era.

Figure 2: Digitisation of the four pillars of the banking ecosystem



Source: Deloitte Research



Rapid digitisation of banks is inevitable in the post COVID-19 era

Several banks have already witnessed rapid digitisation across the four pillars in a short time after the sudden onset of the COVID-19 pandemic and the subsequent nationwide lockdown. That said, the following three factors will speed up a uniform digitisation drive in the entire banking ecosystem:

Increase operational resilience

Banking is an employee-intensive industry and maintains a high touch customer-service model (as revealed from the number of bank branches that remained open during the nationwide lockdown). Therefore, when India went into a complete lockdown after the onset of the pandemic, mobility restrictions for employees, vendors, and partners affected business operations, resources availability, and productivity.

The onset of COVID-19 and the government's response to contain the spread reveal one striking vulnerability of banks − business operations can be disrupted anytime, and most unexpectedly. Banks may have to continue to deal with disruptions in their operations due to social distancing norms, and intermittent regional and local lockdowns, going forward. They will have to build resilience in the Information Technology (IT) architecture to ensure continued access to business applications from anywhere any time to employees, vendors, and partners. Therefore, rapid digital transformation is quintessential for banks to ensure a watertight business continuity plan and uphold productivity during difficult times, while comprehending consequent information security risks against these benefits.

Improve customer outreach

In India, banks deal with a myriad of customers with different digital preferences. Their preferences vary with their knowledge of and inclination to use digital platforms, the perception of risks associated with digital processes, and the nature of information and service requirements. Therefore, banks have had to manage a hybrid of customer interaction channels.

Since the pandemic, business disruptions have caused inconvenience to multiple customer segments who earlier depended on branches for essential financial transactions or advice on complex financial products. Banks have seen a sharp decline in the use of traditional ways of communication amongst a majority of their customers. In the future, social distancing norms (to combat the COVID-19 crisis) will possibly change behaviour in the Indian society permanently. Increased demand for contactless transactions and virtual services, which are secure and convenient to use and navigate, will require banks to digitise rapidly.

Save cost

Every business strives to make its operations cost effective and banking is no exception. Banks have to provide comprehensive and essential services efficiently despite disruption, while remaining cost effective. With COVID-19, one of the biggest challenges that banks are likely to face is that of rising Non-Performing Assets (NPA). According to the RBI's latest financial stability report, macro stress tests for credit risk indicate that the gross NPA ratio of Scheduled Commercial Banks (SCBs) may increase from 8.5 percent in March 2020 to 12.5 percent by March 2021 under their baseline scenario. The ratio may escalate to 14.7 percent under a severely stressed scenario.[vii]

Rising NPAs will likely raise financial stress and credit costs. Digitisation will be key for banks to run operations efficiently, improve productivity, reduce costs, and remain competitive during and after the pandemic. As a result, there is a pressing need to allocate adequate resources towards digitisation.

Cyber-related challenges – part and parcel of digitisation

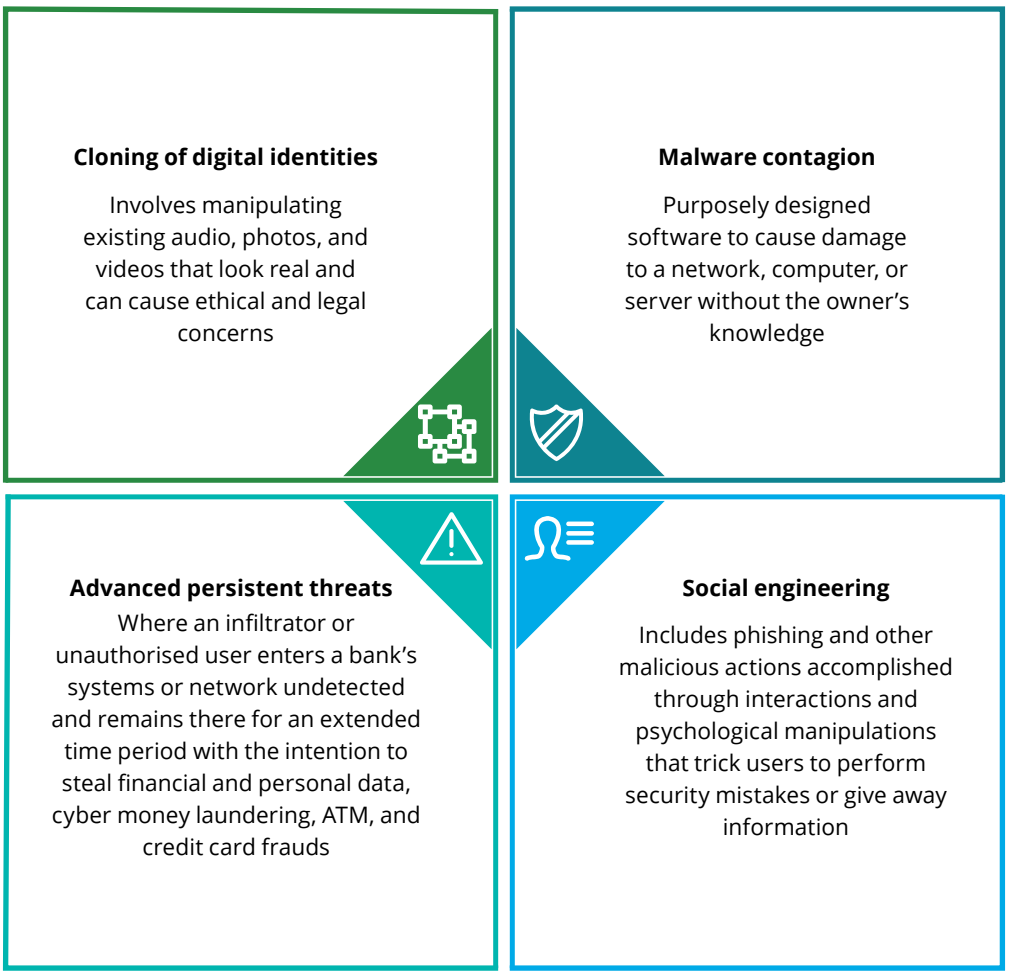
Banks' foremost agenda in board rooms has been the digitisation of voluminous confidential data and banking processes (not limited to payments). This urgency has put the spotlight on digital technologies, such as cloud, Artificial Intelligence (AI), analytics, Internet of Things (IoT), and Machine Learning (ML). With technology transformation, confidential information will be saved in remote servers and ubiquitous.

Higher digitisation and remote operations will lead to increased vulnerabilities and open up opportunities for cybercriminals, exposing banks to breaches or hacking.

Banks need to be mindful of the following challenges while dealing with cyber threats:

- **Sophistication of cybercrimes**
  Armed robbery is a much smaller menace now compared with cyber threats and attacks. Even though the types of cybercrime are similar to frauds banks have been experiencing for ages (Figure 3), in today's world, cyber risks have gone beyond data leakage, lack of access controls, and system downtime. They have entered the realms of cyber skulduggery that includes stealing customer debit and credit card data; siphoning off funds through reprogrammed Automated Teller Machines (ATMs); affecting the banking network's productivity; and indulging in data theft and money laundering through sophisticated software programmes and network algorithms (that vary in nature, origin, and source). Cybercriminals are capable of rapidly adapting to any virtual operating environment no matter how sophisticated the platform may be. In addition, unlike independent frauds posing microprudential risks for individual entities, cybercrimes in banks (or any financial institution) can have systemic consequences (compounded by financial and technological links between financial and non-financial institutions), leading to a multiplier effect and humongous economic losses. According to a recent IMF report, cybercrimes can also be an emerging source of a macro-critical risk.[viii]

Figure 3: The multifaceted cybercrimes



Source: Deloitte Research

- **Data management complexities**
  Banks are always the prime targets for hackers as they deal with a large amount of Personally Identifiable Information (PII) and financial data. More banks are adopting cloud and IoT for data transfers and conducting transactions to meet the rising demand for better services at reduced costs. With increased awareness amongst customers about data privacy and concerns about data governance amongst regulators, safeguarding and efficient management of data have become a priority for banks.[ix] The key issues that need to be addressed include the following:
  - **Data sharing mechanism:** It will require customers' consent and a protocol regarding who should access data. The RBI has acknowledged and envisaged an account aggregators (AA ecosystem) platform to deal with the challenge. Aggregators are responsible for transferring data without storing customer credentials and can be accessed only through consent-based authorisation.[x]
  - **Data life cycle management:** It will involve sourcing appropriate data per requirement and using technology to prevent misuse.
  - **Data ownership:** It will require rules to retain and dispose of customer information.

- **Limitations associated with legacy systems**
  Banks' IT architecture is a mesh of on-premise core legacy systems and a multitude of bespoke and ancillary applications. Although legacy systems are critical for crucial functions, they are less equipped to deal with "speed and mobile banking" requirements. To keep up with the changing paradigm, core applications are integrated with the new ones (mobile, Software as a Service [SaaS], etc.), exposing the former to security threats that are novel, frequent, and ever-evolving.

- **Securing third-party services (vendors and alliance partners)**
  A bank's cybersecurity is as strong as its weakest link. The banking ecosystem is highly integrated and banks have to rely on alliance partners (such as fintech solutions) and third-party vendors in banking operations. These vendors have to access banks' networks to conduct several of their operations; this implies that any vulnerability in their cybersecurity infrastructure could be a security risk for banks. In other words, the cybersecurity of third-party services is also banks' responsibility.

- **High exposure to compromised network and devices**
  After COVID-19, more stakeholders are trying to connect to banks' networks virtually using personal devices. An increase in the traffic volume connecting to the banks' network may lead to greater cybersecurity risks and vulnerability. Demand for remote access from employees, and use of a wide range of devices and networks by customers to access banking services may compromise banks' assets and networks. Managing threats arising from multiple access points (used by employees and customers) is a tough challenge that banks will have to address.

- **Lack of skilled cybersecurity professionals**
  Despite the steadily increasing demand and complexity of cyber risks, there is a shortage of cybersecurity workforce worldwide. According to a survey conducted globally by the Information Systems Audit and Control Association (ISACA), the majority of the respondents reported that their cybersecurity teams were understaffed and they faced resourcing and retention challenges.[xi] The New York Times reported a prediction (by Cybersecurity Ventures) that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million positions in 2014.[xii] India faces a similar challenge of a shortage of skilled professionals in this profession. The Data Security Council of India (DSCI) predicted in 2015 that India will need one million cybersecurity professionals by 2020.[xiii] In its recent report, it stated that cybersecurity services companies are likely to expand significantly in the near future; many of these companies are re-skilling about 50 percent of their cybersecurity workforce.[xiv] These reports suggest that as banks strengthen their cybersecurity infrastructure, they are likely to face a shortage of skilled professionals and challenges in skilling their own employees to deal with rising complexities in cyber risks.

- **Governance and regulatory compliances**
  The volume of regulations has increased dramatically over the past few years. In early 2020, the Indian government, under the aegis of National Security Council Secretariat through a well-represented task force, initiated formulating the National Cyber Security Strategy 2020 (NCSS 2020) for the next five years (2020-25) to ensure a 'safe, secure, trusted, resilient, and vibrant cyberspace'.[xv] Banks are required to fulfil the regulatory obligations related to cybersecurity.[xvi] With cyber risks expected to rise, regulatory compliances are only likely to increase, making it more difficult for banks to manage and adhere to these. For instance, the RBI has issued more than 10 advisories/alerts on various cyber threats and best practices to supervised entities since March 2020. It issued some of them in coordination with the Indian Computer Emergency Response Team (CERT-In).[xvii]

Tackling the cybersecurity challenge will be key

To stay relevant and competitive, banks will have to meet stakeholder expectations while preventing threats and adhering to regulatory requirements, by improving their cyber defence efforts. As banks increasingly focus on moving resources on digital platforms, they should expect higher and more sophisticated attacks. These attacks will shift from in-house devices to those hosted on digital platforms accessed by different stakeholders and directly target end-users' computing environments.

Banks will have to proactively tackle cyber risks from various aspects of security − data, application, identity, infrastructure, and cloud − as well as administer end-user education, and regulatory compliances (Figure 4). They have to constantly address security gaps, plan a security roadmap, assess and benchmark best practices, and make strategic investment decisions in cybersecurity core domains in line with business needs and risk appetite.

Figure 4. Dimensions of cybersecurity banks have to be aware of

Application security
Tools and methods to protect applications after deployment by monitoring, resolving, and enhancing apps' security with antivirus programmes, firewalls, and encryption

Infrastructure security
Solutions to protect the corporate infrastructure, such as network communications, data centres, IT platforms, and connected devices

Information/data security
Tools to protect confidential, private, and sensitive information or data from misuse, unauthorised access, disclosure, damage, modification, and disruption

Cloud security
Tools include security procedures and technology to secure cloud computing environments against both external and internal cyberattacks

Identity and access management security
An architecture or security policies enforced to define and manage the roles and access privileges of individual network users, and protect critical and sensitive data

Regulatory focus
Complying with the RBI guidelines on the cybersecurity framework that focuses on three areas:
- Cybersecurity and resilience
- Cybersecurity Operations Centre (C-SOC)
- Cybersecurity Incident Reporting (CSIR)

End-user education
Involves educating employees and third-party services on the importance of protecting sensitive information and security measures to avoid cyberattack

Source: Deloitte Research

Seven-step recommendations to address cyber threats

The existential threats to banks from cyber criminals cannot be over emphasised. Therefore, banks must build a robust security threat monitoring mechanism by implementing “state-of-the-art” solutions. They can mitigate cyber risks by adopting a few approaches shown in Figure 5. These recommendations are not exhaustive but essential to ensure robust security and compliance. Details of the recommendations are mentioned in a separate sidebar at the end of the report.

Figure 5. Recommendations to deal with cyber threats

Seven-step recommendations for banks

01

Prioritising cybersecurity assessment
- A continuous threat assessment using a risk-based approach
- Cybersecurity maturity assessment
- Bridging the gaps
- Integrating cyber risk assessment with fraud risk and financial crime reporting

02

Securing remote access control
- Enabling server-based computing and digital workspaces
- Deploying zero clients and thin clients
- Reviewing remote connectivity solutions and security governance
- Deploying an advanced and robust authentication and authorisation
- Deciding on the scope of services that need secured access

03

Tightening access to third-party services
- Prioritising access to and availability of services for alliance partners and vendors
- Restricting or controlling their access to core infrastructure
- Exploring the possibility of modifying contractual agreements to monitor third-party access to banking infrastructure

04

Contracting or outsourcing cybersecurity capabilities
- Dealing with shortages of cybersecurity professionals using leading-edge services of third-party security providers
- Considering outsourcing a myriad of cybersecurity functions, such as security operations and insider threat detection (including threat hunting and threat intelligence)

05

Adopting advanced technology solutions and tools
- Creating many lines of defence at different levels in the security ecosystem
- Adopting defence options for threat intelligence and response capabilities, such as:
  - Zero-trust architecture
  - Advanced endpoint security systems
  - Augment cybersecurity with AI
  - DevSecOps

06

Raising awareness through training
- Introducing formal training programmes on cyber threats and cybersecurity practices for employees
- Involving different methods to educate employees
- Developing cybersecurity culture at every level and viewing it as a continuous process

07

Bolstering security through threat identification and response competencies
- Integrating a modern and evolving security infrastructure while digitisation
- Embedding security, confidentiality, and policy checks into their DevOps decisions and actions

Source: Deloitte Research

Summary

Cyber challenges for tomorrow

Banks will likely adopt technologies such as mobile, cloud, remote access, and IoT, not out of choice but out of the need to sustain business during the pandemic and thrive thereafter. Such transformative digitisation will also result in an increased attack surface. For bank executives, the focus will be on achieving business goals even as they recalibrate strategies to address the ever-evolving cyber risks.

Banks will have to prioritise and invest in cyber defence to create an agile and resilient infrastructure of the future. Such an infrastructure will address the current cybersecurity risks and prepare itself for cyber challenges of the future. However, for that to happen, the initiative has to come from bank executives and board members who set goals and allocate budget. Accelerating cyber capabilities to match the speed of digital transformation will require executive attention, prioritisation, budget, resources, and governance. Only the leadership can drive such a change. Banks' leaders will decide the degree of agility, pace of change in infrastructure, and collaborative efforts required towards building cybersecurity of the future.

The second part of this series will examine how the banking industry is responding to the changing operating environment today and adapting to cyber challenges of tomorrow. Assuming a few possible economic and banking scenarios, the report will provide perspectives on the current awareness amongst bank executives regarding the changing dynamics of digitisation and resulting cyber threats. It will also focus on their medium-to-long-term strategies and investment in these two areas. The analysis will be based on interviews of several experts within the banking industry and on the subject.

Sidebar: Details of the recommended steps

The seven-step recommendations for banks are as follows:

01. Prioritising cybersecurity assessment

Cyber threats are dynamic and rapidly evolving, which means banks may not be equipped to prevent every threat at a time. To manage cybersecurity risks and protect critical assets, banks will have to prioritise their efforts and invest in key cyber areas that matter. One of the ways could be to segregate cybersecurity from IT solutions, and identify areas where vulnerabilities and risks are the highest by breaking the value chain. Banks will have to classify risks through inherent risk assessment (including reporting), evaluate the maturity levels of cyber resilience, and then focus on bridging the gaps if any.[xviii] That will involve the following:

- **A continuous threat assessment using a risk-based approach** requires banks to continuously examine the volume of cyber threats and attacks they face. Thereafter, they need to create a risk profile to determine the cyber risk exposure (such as low, medium, and high). These risk profiles could be associated with technologies, delivery channels, products and services, infrastructure, organisational character, and operating environment. Using AI, banks have to ensure that inherent risk levels are at the minimum required maturity levels.
- **Cybersecurity maturity assessment** is needed to ensure that the actual maturity levels of cyber resilience have reached the minimum required levels, according to the National Institute of Standards and Technology (NIST) framework. This process is critical in managing and strengthening the cybersecurity position, and covers a comprehensive review of the entire operating environment.
- **Bridging the gaps** will be essential (based on priorities) to elevate the actual level of resilience to the expected levels. This requires identifying and developing a roadmap to improve maturity to the expected levels.
- **Integrating cyber risk assessment with fraud risk and financial crime reporting** will be essential as cyber risks are manifesting into the fraud and financial crime domain. It is the interacting and evolving nature of risks that necessitates a continuous monitoring to enable a desired response. Therefore, an important first step is to understand the changing nature of frauds and money laundering tactics. Fraud risks are no longer unrelated loss instances caused by malicious intentions of employees, customers, and others; money laundering is not limited to the transactions with faked identities. The ability to hack into a bank's network has provided an avenue for defrauding, which has a systemic impact and multiplier effect. Monitoring and reporting these evolving trends through an integrated lens is necessary.

02. Securing remote access control

Working remotely using remote access management solutions requires higher bandwidth controls. This would need reviewing remote connectivity solutions and security governance; deploying advanced and robust authentication and authorisation; and deciding on the scope of services that require secured access. Similarly, server-based computing and digital workspaces, such as virtual desktop interface, enable employees working remotely to access data through a secure, encrypted connection (leaving no trace of activities on user devices after logging off). Banks may choose to deploy zero clients and thin clients based on applications and peripherals that users/employees may want to use with devices.

03. Tightening access to third-party service providers

Mobility restrictions and supply chain disruptions could compromise the security of the alliance partners and vendors that work with banks. By accessing the banking network and assets remotely, such services may also compromise banks' cybersecurity. Banks may have to prioritise access to and availability of services the other parties offer. This can be done by restricting or controlling their access to core infrastructure. It will likely require modifications to contractual agreements to monitor their access to banking infrastructure.

04. Contracting or outsourcing cybersecurity capabilities

To deal with talent shortages and keep up with the increasing demand for cybersecurity, banks could consider using new channels (such as third-party security providers with enhanced capabilities). Contractors or outsourced capabilities may be more efficient and can often deliver leading-edge services. Banks may consider outsourcing a myriad of cybersecurity functions, such as security operations and insider threat detection (including threat hunting and intelligence).

05. Adopting advanced technology solutions and tools

Banks have to create many lines of defence at different levels in the security ecosystem. Some options that banks are rapidly adopting are mentioned below:

- **Zero-trust architecture:** It is being widely adopted in many organisation for protecting sensitive data and responding to modern cyber threats in a "perimeter-less" world. The architecture's design is such that it secures perimeters and addresses any threat that is detected within a network.[xix] The architecture's rationale is that every perimeter (device, user, network, or application) cannot be trusted. It, therefore, monitors every data, user, and location of access for threats. Users cannot access data and resources unless they are authenticated and their access is authorised.
- **Advanced endpoint security systems:** These are associated with providing security from cyber threats to endpoints or entry points of end-user devices. These devices include desktops, laptops, and mobile devices that connect to the banking network or clouds. A few options that banks may choose are mentioned below:
  - Endpoint verification, which allows creating an inventory of devices that access a bank's data. It monitors and reports the security posture (using ML algorithms). Banks can set up endpoint verification to corporate devices and bank employees can install it on their devices.
  - Provide cloud-based devices that run on a cloud-based operating system that has cloud storage, to employees or third-party service providers. Such a cloud-based operating system is device agnostic, and constantly syncs apps, preferences, and information fed by employees or third-party service providers.
- **Augment cybersecurity with AI:** It can help deal with challenges related to talent shortage and skill gaps as demand for cybersecurity increases. Banks may consider adding cognitive technologies that can help automate routine tasks, and increase alertness and sensitivity to anomalies. This will help allow cyber professionals to focus more on tasks requiring human prowess. Technologies such as AI, automation, text and speech processing, robotics, and ML can address mundane, repetitive low-priority cybersecurity issues (that take employees' time and affect their efficiencies).[xx] It also informs intelligent decisions (through analytics) facilitating a forward-looking, prognostic approach to security challenges.[xxi]
- **DevSecOps** (development, security, and operations) will enable security integration into the application development life cycle.[xxii] It can increase awareness of the risks that could affect solutions being developed, and design tools to test and analyse software vulnerabilities. In addition, AI-driven threat assessments, security automation, and scaled cyber solutions are a few of the top-ranked defence concepts that banks may want to prioritise as future investment for threat intelligence and response capabilities.

06. Raising awareness through training

Formal training programmes on cybersecurity practices should be introduced for employees to recognise phishing and social engineering attacks. These programmes will help them to be better aware of cyber threats. Training should involve different methods to educate employees and not just focus on a few elements of cyber awareness. The cybersecurity culture should be developed at every level and regarded as a continuous process.

07. Bolstering security through threat identification and response competencies

Certain digitisation implementations may get fast-tracked during the pandemic. This will require banks to rethink how security is integrated across the modern and rapidly evolving infrastructure. In addition to investing in security tools and solutions (as discussed above), banks have to be forward-thinking to enhance their approach to cyber risks and threat intelligence.[xxiii] One of the solutions for banks could be to embed security, confidentiality, and policy checks into their DevOps decisions and actions.

References

[i] Ashwin Manikandan, “Moody’s warns banks of increased cyber risks” The Economic Times, July 08, 2020, https://economictimes.indiatimes.com/industry/banking/finance/banking/moodys-warns-banks-of-increased-cyber-risks/articleshow/76856381.cms?from=mdr#:~:text=Mumbai%3A%20Global%20rating%20agency%20Moody's,most%20physical%20processes%20into%20digital

[ii] Tom Kellermann, and Ryan Murphy, “Modern banks heists 3.0”, VMware Carbon Black, May 2020, https://cdn.www.carbonblack.com/wp-content/uploads/VMWCB-Report-Modern-Bank-Heists-2020.pdf

[iii] Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50122

[iv] PTI, “Financial frauds rising due to dependence on digital payment platforms: NSA Ajit Doval”, Money Control, September 19, 2020, https://www.moneycontrol.com/news/india/financial-frauds-witnessing-a-spike-due-to-dependence-on-digital-payment-platforms-ajit-doval-5859641.html

[v] Press Trust of India, “Rise in cyber attacks from China, Over 40,000 Cases In 5 Days: Official“ NDTV, June 23, 2020, https://www.ndtv.com/india-news/rise-in-cyber-attacks-from-china-over-40-000-cases-in-5-days-official-2251111

[vi] The information has been compiled from the listed news agencies and sites;
The New York Times, "MasterCard Says 40 Million Files Put at Risk", https://www.nytimes.com/2005/06/18/business/mastercard-says-40-million-files-put-at-risk.html; CRN, "Citibank Breach Allegedly Connected To Russian ATM Fraud Scheme", https://www.crn.com/news/security/222003033/citibank-breach-allegedly-connected-to-russian-atm-fraud-scheme.htm; Wired, "Bank Worker Pleads Guilty to Hacking 100 ATMs", https://www.wired.com/2010/04/malware-targeted-100-atms/; Reuters, "Citi says 360,000 customers hacked in May cyber attack", https://in.reuters.com/article/us-citigroup/citi-says-360000-customers-hacked-in-may-cyber-attack-idUSTRE75F0RU20110616; The Washington Post, "Flame FAQ: All you need to know about the virus", https://www.washingtonpost.com/blogs/blogpost/post/flame-faq-all-you-need-to-know-about-the-virus/2012/06/20/gJQAAlrTqV_blog.html; The Financial Express, "Hitachi Payment Services: Mid-2016 breach in India due to sophisticated malware", https://www.financialexpress.com/india-news/hitachi-payment-services-mid-2016-breach-in-india-due-to-sophisticated-malware/544051/; The Hindu, "Hacked: How $171 mn stolen from Union Bank was recovered", https://www.thehindu.com/news/national/hacked-how-171-mn-stolen-from-union-bank-was-recovered/article18063938.ece; Reuters, India's Cosmos Bank loses $13.5 mln in cyber attack, https://www.reuters.com/article/cyber-heist-india-idUSL4N1V551G; The Times of India, "Another Maharashtra cooperative bank’s server hacked, Rs 68 lakh siphoned off", https://timesofindia.indiatimes.com/city/mumbai/another-co-op-banks-server-hacked-rs-68l-siphoned-off/articleshow/69242381.cms; DNA India, "40,000 cyber-attacks attempted by Chinese hackers on Indian banking, IT sector in five days", https://www.dnaindia.com/india/report-40000-cyber-attacks-attempted-by-chinese-hackers-on-indian-banking-it-sector-in-five-days-2829381#:~:text=A%20top%20police%20official%20in,in%20the%20last%20five%20days; IMF working paper, "Cyber Risk Surveillance: A Case Study of Singapore", https://www.imf.org/en/Publications/WP/Issues/2020/02/10/Cyber-Risk-Surveillance-A-Case-Study-of-Singapore-48947

[vii] Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50122

[viii] Joseph Goh, Heedon Kang, Zhi Xing Koh, Jin Way Lim, Cheng Wei Ng, Galen Sher, and Chris Yao, “Cyber Risk Surveillance: A Case Study of Singapore”, IMF working paper, Monetary and Capital Markets Department, February 2020, https://www.imf.org/en/Publications/WP/Issues/2020/02/10/Cyber-Risk-Surveillance-A-Case-Study-of-Singapore-48947

[ix] Deborah Golden and Irfan Saif, “The future of cyber survey 2019”, Deloitte, 2019, https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html

[x] Reserve Bank of India, “Master Direction: Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016”, Master Directions, September 02, 2016 and updated on November 22, 2019, https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

[xi] ISACA, “State of cybersecurity 2020: Part 2: Threat Landscape and Security Practices”, ISACA, 2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc201

[xii] Paulette Perhach, “The mad dash to find a cybersecurity force”, The New York Times, November 7, 2018, https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html; and

[xiii] Data Security Center of India, “Cyber security: 1 million cyber security professionals needed by 2020”, Press Release, DSCI News Center, August 2015, https://www.dsci.in/content/cyber-security-1-million-cyber-security-professionals-needed-2020-0#:~:text=Cyber%20security%3A%201%20million%20cyber%20security%20professionals%20needed%20by%202020,-Published%3A%20Aug%2C%202015&text=Along%20with%20the%20Data%20Security,creating%20a%20master%20training%20programme

[xiv] Data Security Center of India, “India Cybersecurity Services Landscape - A Global Hub in the Making”, May 21, 2020, https://www.dsci.in/content/India-Cybersecurity-Services-Landscape

[xv] National Informatics Centre, Ministry of Electronics & IT (MeitY), National Cyber Security Strategy 2020 (NCSS 2020), https://ncss2020.nic.in/

[xvi] Bank Quest, “Cyber security in banks”, The Journal of Indian Institute of Banking & Finance, January-March 2018, http://www.iibf.org.in/documents/BankQuest/Bank-Quest-Jan-Mar-2018-Final-200418.pdf

[xvii] Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50122

[xviii] "Cyber resilience assessment framework", Hong Kong Monetary Authority, May 2016, https://docplayer.net/85773113-Cyber-resilience-assessment-framework-consultation-draft.html

[xix] Alper Kerman, Oliver Borchert, Scott Rose, Eileen Division, and Allen Tan "Zero Trust Architecture", NIST-NCCOE, 2020, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

[xx] Deborah Golden, "AI-augmented cybersecurity", Deloitte, June 08, 2017, https://www2.deloitte.com/us/en/insights/industry/public-sector/addressing-cybersecurity-talent-shortage.html

[xxi] Note: A few of such security solutions are security information and event management (SIEM) and security orchestration, automation and response (SOAR).

[xxii] Deborah Golden and Irfan Saif, "The future of cyber survey 2019", Deloitte, 2019, https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html

[xxiii] Deborah Golden, Jason Frame, Kelly Miller Smith, "COVID-19: Cyber Preparedness & Response", Deloitte, https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/COVID-19%20Cyber%20Preparedness%20and%20Response.pdf; Note: A few of such security solutions are security information and event management (SIEM) and security orchestration, automation and response (SOAR);

Connect with us

Sanjoy Datta
Partner and Leader, Financial Services
sanjoydatta@deloitte.com

Aruna Pannala
Partner, Financial Services
apannala@deloitte.com

Munjal Kamdar
Partner, Financial Services
mkamdar@deloitte.com

Dr. Rumki Majumdar
Associate Director and Economist
rumajumdar@deloitte.com

Acknowledgments

Ranjan Kotian
Roshan Kule
Pramod Potharaju

Deloitte.