Booz | Allen | Hamilton

Information paper

Raising the cyber security bar in the journey to a digital India

Contents

Executive summary

The march to a digital India
The nation continues to march towards its goal of bringing 1.2 billion citizens into the fold of an all-digital economy. Based on presenceless, paperless, cashless and consent-based layers of infrastructure the country is moving quickly to establish an open platform for government, businesses and citizens to transact in an efficient, reliable and secure manner.

This ambitious project has made significant progress in recent years. Launched in 2010 the Unique Identification Authority of India (UIDAI) has achieved over 89% penetration. Approximately 1.1 billion Aadhaar identity cards, linked to biometric data, accessible over application programming interfaces (APIs) now facilitate authentication anytime, anywhere. The scheme underlies a new generation of national infrastructure services. Over 150 million paperless Know Your Customer (eKYC) transactions, 2.4 billion documents stored securely in DigiLocker, and 30 million digital and legally binding signatures, are early artefacts of this powerful India stack.

Financial services at the forefront of digital transformation
Indian regulators, financial institutions and market infrastructures are at the forefront of this digital transformation. More than 250 million bank accounts are Aadhaar linked. With initiatives such as de-monetization, electronic payments surged over 13.5% in 2017. In nine months of service the National Payments Corporation of India's (NPCI) Unified Payments Interface (UPI) saw 414 million transactions. This digital transformation is driven by new transaction schemes, growing digital transaction volumes, disruptive technology such as APIs, Cloud and Artificial Intelligence, and new fintech entrants, which continue to make financial sector participation an increasingly complex enterprise.

Increasingly sophisticated and persistent cyber threats
Unfortunately, sophisticated and persistent malicious actors threaten this transformation agenda. For the first time cyberattacks appear in the World Economic Forum's (WEF) annual global risk report as the third highest risk, behind extreme weather events and natural disasters; just two years ago, in 2016, cyber was 10th in the WEF rankings. Cases of fraud, data breaches and ransomware are on the rise globally, causing significant disruptions and damage. India is no exception.

Cyberattacks are inevitable and cybersecurity should be assumed as part of the cost of doing business in a digital economy. To effectively responding to these threats requires collaboration between all stakeholders. Financial institutions, their vendors, regulators and government agencies must co-create new tools, establish market practices for information sharing and practice incident responses together. In India, the Prime Minister's Office for Cybersecurity, CERT India, and the National Cyber Security Coordination Centre all play an important role in enabling the nation's digital defence.

Empowering SWIFT customers to respond to cyber threats

In response to persistent and sophisticated correspondent banking payments fraud, SWIFT launched the Customer Security Programme (CSP) in 2016 to raise awareness and empower its customer. The programme comprises of three pillars:

- **Secure and protect** – a set of tools and security framework to protect your operating environment
- **Prevent and detect** – services to secure relationships and transactions with your counterparties
- **Share and prepare** – timely and actionable cyber intelligence shared with the community of SWIFT users

Within the Programme, the Customer Security Control Framework (CSCF) establishes a new minimum security baseline. By the end of last year, SWIFT customers had to attest their level of compliance with the controls and submit their self-attestations to the KYC Security Attestation (KYC-SA) application. That customer security attestation data can now be made available by SWIFT customers to their counterparts through the KYC-SA. It is valuable data which should be consulted when transacting with counterparties.

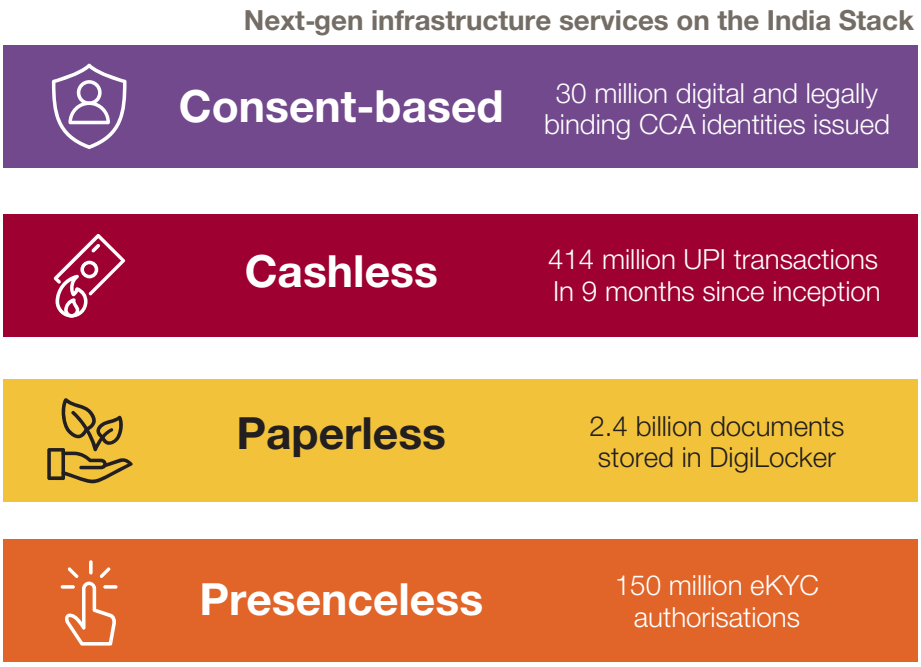
All SWIFT customers should now be busy working towards attesting their full compliance with the mandatory controls. This needs to be done by the end 2018. The new Payments Control Service (PCS), launching in the third quarter of this year, will enable real-time screening of anomalous transactions.

This cloud-based, zero-footprint solution will enable customers to define their own rulesets and screen for transaction values and volumes, business hours, suspicious accounts, currencies, countries, and other uncharacteristic behaviours.

The global payments initiative (gpi) is transforming correspondent banking. It enables faster, more efficient payments combined with transparency of transactions and fees across the payments chain. The gpi Stop & Recall service, which will again be available in the third quarter of this year, is a powerful tool in stopping fraudulent transactions before they reach fraudulent accounts.

SWIFT is committed to supporting our community in responding to this persistent threat. Contact us at csp.apac@swift.com to find out more.

An increasingly large and complex attack surface



1 Global cyber trends

Malware through popular software
According to the Booz Allen Hamilton Cyber4Sight threat intelligence team, there will be a rise in attackers hijacking updates of popular (and often free) software to spread malware and launch attacks against organizations. Booz Allen predicts that attackers will compromise a small software provider and use their software updates to attack larger companies downstream. The attackers will carry out a small attack to enable a far larger one.

Past examples of such attacks include suspected nation-state sponsored hackers compromising the updates of the free and popular software CCleaner in 2017, with the aim of carrying out cyber espionage through the system administrators of technology and telecommunications firms that used it. Similarly, in 2017 attackers compromised the update server for a popular Ukrainian tax software called M.E. Doc, sending out poisoned updates that led to the NotPetya outbreak.

An increase in nation-state-backed hacking groups
Another trend predicted for 2018 is an increase in nation states hiring mercenary hackers and wielding their expertise to disrupt key systems and organizations. Hiring of foreign cyber mercenaries is more effective than investing years in developing home-grown talent. This allows nation states to more quickly deploy cyber-attacks as a foreign policy tool to disrupt the operations of competitors and adversaries.

Past examples of such attacks include the OilRig espionage campaign and the Qatar News Agency breach, both of which allegedly involved contract foreign hackers. The Bahamut campaign's geographically varied target set suggests that the group was supported by espionage programs in multiple countries.

2 Cyber trends in India

An increase in the number of cyber attacks
According to the Indian Parliament, India was victim to a staggering 144,496 cyber-attacks in the last three years. Beyond the absolute numbers, what is most glaring is the upward trend of cyber-attacks year on year. In 2014 44,679 cyberattacks were reported. In 2015, that number rose to 49,455, and by 2016, the number crossed the 50,000 mark, with no signs of a downward turn. In addition, in a report by security firm FireEye, incident data from 2016 and 2017 found that 49% of customers in India and APAC, with at least one high priority breach, were successfully attacked again within a year.

As they are financially motivated cybercriminals pose the greatest threat to India's financial sector. Booz Allen predicts that as India's economy continues to grow and becomes more reliant on electronic payment systems, this trend will only continue upward.

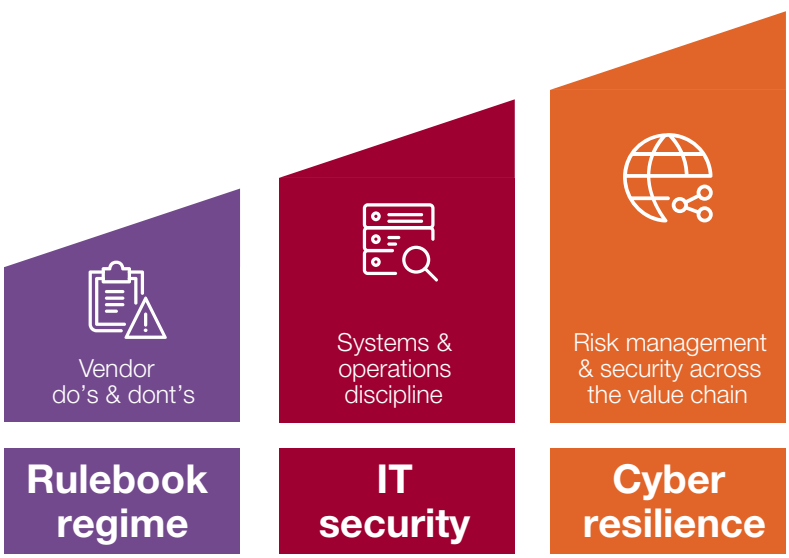
An increase in the number of data breaches
There were 18 data breaches leading to 203.7 million data records being compromised in India in the first half of 2017, according to Gemalto's Breach Level Index. Compared to the last six months of 2016, the number of lost, stolen or compromised records increased by a staggering 167 million. Companies in financial services, retail, and the government sector were the primary targets for breaches in 2017.

A study by the Ponemon Institute revealed that the average per capita cost of a data breach increased by 13%, from 3,704 INR in 2016 to 4,210 INR in 2017, causing a total organizational cost of 110.0 million INR caused by data breaches in 2017.

An increase in fraud
According to a 2017 Booz Allen threat assessment, India is projected to have an increase in mobile payment fraud. This is caused by recent demonitisation measures, leading to an increase in India's digital payments, motivating cybercriminals to target all components of the digital payment process, from individual mobile devices to online payments platforms. In addition, in the rush to adopt digital payment technologies, organizations and individuals may not adopt commensurate security controls to secure the payment chain.

The Asia Pacific Fraud Insights Report 2017 published by credit information company Experian analysed fraud trends across ten countries in Asia Pacific, noting that incorrect employment information and false income documents were two of the most frequent types of fraud committed in India.

Cyber readiness varies significantly across the financial sector



3 Recent incidents in India

WannaCry
The massive WannaCry ransomware outbreak that affected millions of computers worldwide had far-reaching effects in India. Specifically, some of the affected services included:

- Operations of state-level government service were impacted due to computers being disabled
- A government-run hospital was infected by the malware, which in turn affected its e-medicine services
- Customer care centres belonging to an energy company could not be used to serve customers, although it was reported that the critical infrastructures that supported electricity distribution were spared
- In a western state, more than 120 computers connected with GSWAN were affected (a network of 60,000 computers that connects 33 districts and 3200 government offices for secure digital communication)
- Computers of a transportation company were infected, but the attack was said to be limited to the personnel department that dealt with staff matters such as appointments, transfers, and promotions

Financial services
In early 2017, India was identified as one of several countries that had experienced the sophisticated banking malware known as TwoBee. TwoBee malware reportedly altered financial transactions sent between business accounting systems and banks, resulting in USD3.6M in losses.

In early 2018, cyber criminals hacked the systems of a major bank and transferred nearly $2 million through unauthorized remittances to accounts in countries in East Asia and the Middle-East.

Telecommunications
A state telecommunications company was severely affected by a malware attack, with the virus reportedly affecting 60,000 modems with default “admin-admin” username/password combination. The malware-infected modems reportedly prevented users from accessing Internet services for up to three days.

Data breaches
In late 2016, a compromise of a payment service network allowed cybercriminals to compromise credit card information that was processed by approximately 90 ATMs. Direct losses were estimated to total USD195,000, not including the cost of replacing compromised cards.

In early 2017, an online search and discovery service for restaurants had its company’s database breached, which led to the personal details of 17 million users being stolen. The leaked information included user IDs, names, email addresses and hashed passwords, which were reportedly listed for sale on the Dark Web.

Hacking of government websites
According to statistics tracked by the Indian Computer Emergency Response Team (CERT-IN), more than 22,000 Indian websites including 114 government portals, were hacked between April 2017 and January 2018. Of the hacked websites, a total of 493 were used for malware propagation.

4 Correspondent banking risks

Safe, reliable, secure and efficient financial transactions are hallmarks of a well-functioning financial system. According to the Financial Stability Board 72% of jurisdictions released plans to issue new regulations on cybersecurity for the financial sector. The Committee on Payments and Market Infrastructures (CPMI) has issued a discussion note on reducing risk of wholesale payments fraud to end endpoint security, proposing a strategy to identify and understand the range of risks, establish security requirements, promote adherence and information sharing, provide tools, speed response times, and to learn from past incidents.

In response to the cyber-threat facing the banking community SWIFT established the Customer Security Programme (CSP) in 2016. This broad programme is designed to raise awareness of cyber risks and empower our customers in their response. The CSP establishes a security baseline, and provides tools and information, providing the wherewithal the community of SWIFT users, regulators and industry associations need collaborate to raise the bar on security.

5 Customer Security Programme

CSP Objectives
The CSP is articulated around three mutually reinforcing areas. Customers first need to secure and protect their local environment (You), prevent and detect fraud in their commercial relationships (Your counterparts) and continuously share information and prepare against future cyber threats in collaboration with others (Your community).

Combating fraud is a challenge for the whole industry – there are no quick fixes. The threat landscape adapts and evolves by the day, and both SWIFT and its customers have to remain vigilant and proactive over the long term. While customers are responsible for protecting their own environments, SWIFT's Customer Security Programme (CSP) has been established to support customers in the fight against cyber-attacks.

This programme addresses three key aspects of your business and your relationships, enabling you to take action with the support of SWIFT's programme.

1. You
Securing your own local environment is the most important action you can take. Securing the physical set-up of your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber-related fraud.

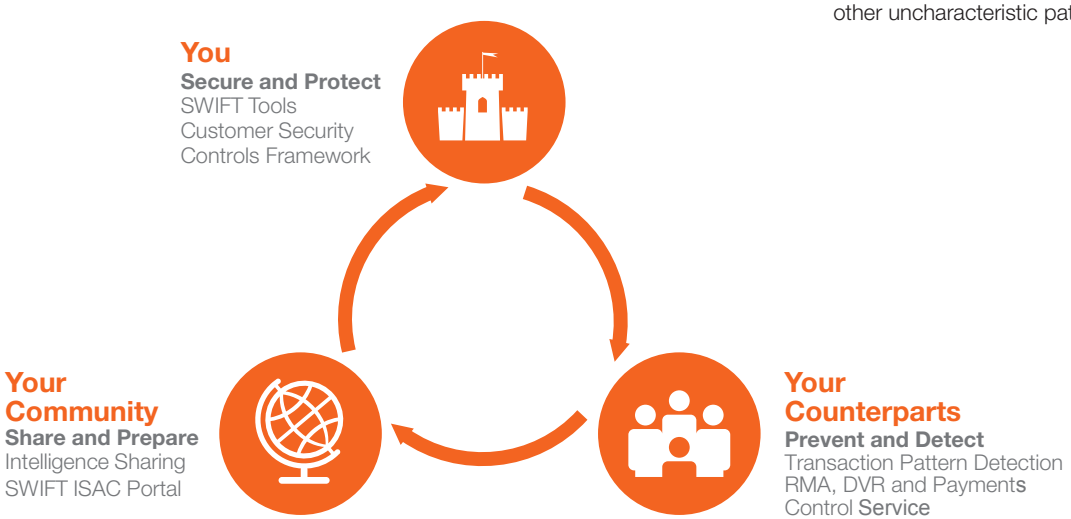
What you can do
Take all preventive measures to secure your local environment; sign up to SWIFT's Information Sharing and Analysis Centre (ISAC); stay up to date with SWIFT's latest security updates; get ready to comply with mandatory controls in the Customer Security Control Framework (CSCF) by December 2018.

2. Your counterparts
Companies do not operate in a vacuum and all financial institutions are part of a broader ecosystem. Even with strong security measures in place, attackers are very sophisticated and you need to assume that the worst may happen. That's why it is also vital to manage security risk in your interactions and relationships with your counterparties:

1. **Control who you are transacting with** using the Relationship Management Application (RMA). This allows you to control who you can send to and receive transactions from. A more granular RMA Plus is available to further control the type of transactions between counterparties.

2. **Validate your payment activity** with Daily Validation Reports (DVR) or FINInform. Use the 'golden copy' of data from the SWIFT network to reconcile quickly identify fraudulent transactions.

3. **Minimise the risk of your sent payments by putting appropriate fraud prevention mechanisms** in place using the Payments Control Service (PCS). Screen for unusual payment values, currencies and recipients, payments outside of business hours, and other uncharacteristic patterns.



3. Your community
The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can easily be replicated elsewhere in the world. If the worst happens, or you suspect something is wrong, it is vital that you share all relevant information and tell us there is a problem – which is part of your obligation to SWIFT as a user.

In cases of suspected customer fraud, it is important to act fast and take decisions in real time.

What you can do
Inform SWIFT if you suspect that you have been compromised; sign up to the SWIFT ISAC and act upon the intelligence provided; comply with the CSCF mandatory controls and submit your self-attestation by December 2018; and install all mandatory updates from SWIFT within the prescribed timeframes.

Summary
By focusing action on supporting your efforts, your counterparty relationships, and your community, SWIFT's CSP is already making a strong impact on preventing, detecting and responding to fraud and reinforcing the security of global banking. By December 2017, 89% of all BICs completed their attestation to the CSCF and confirmed their current level of compliance. This represents 99% of all FIN traffic over SWIFT.

The fraud threat is adaptive, so the tools and controls introduced under the CSP will continue evolving, and we are committed to working over the long term to achieve the objectives of the programme.

This is the first part of a journey which involves SWIFT and its community of customers, regulators, overseers and third parties to collectively work together to fight against cyberattacks.

For further information visit:

www.swift.com/csp

6 Customer Security Control Framework

To create a security baseline for the global financial community, SWIFT has introduced a set of core security controls that all users must meet to secure their local SWIFT related infrastructure. Detailed security controls (16 mandatory and 11 advisory) have been published, and documentation is available in the CSP section of the User Handbook on swift.com. All controls have been defined by SWIFT and industry experts and are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The control definitions are in line with existing information security industry standards, and are product-agnostic.

All customers must comply with the Customer Security Control Framework v1.0 by end 2018.

What practical steps should your organisation take to comply with the mandatory security controls?
Please read and take time to understand the SWIFT Customer Security Controls Framework documentation and the Customer Security Controls Policy that outlines the related attestation process.

SWIFT is organising Customer Security Work Sessions across India to provide further guidance. You will be invited to your nearest session.

You can also follow SWIFTSmart training modules related to the Customer Security Controls Framework. SWIFT strongly encourages you to start a project to assess your current level of compliance with the mandatory controls that apply to your organisation.

Identify any gaps and create an action plan to close them as fast as possible to mitigate security vulnerabilities.

You can also call upon third parties to help you to implement the customer security controls. SWIFT has published a directory of cyber security service providers on our website to help you to identify possible project partners.

Visit https://www.swift.com/myswift/customer-security-programme-csp

What is the purpose of the customer security attestation process?
Through the attestation process, SWIFT is increasing the overall level of transparency on cyber security among users of the SWIFT network.

SWIFT customers of all shapes and sizes, and from all geographies, have to evaluate their current cyber defences against the best practices and attest their compliance against the controls. Furthermore, the attestation structure we have put in place enables (and encourages) customers to share their attestation information with their counterparts. In doing this, SWIFT's aim is to increase the level of cyber security transparency and awareness between users. The detailed controls were published in mid-2017 and customers had until 31 December to attest their compliance against them. Although a challenging deadline, the community's response to complying with this first stage was extremely positive; by the deadline 89% of customers representing 99% of SWIFT traffic had attested.

SWIFT Customer Security Controls Framework - Objectives and Principles

Secure Your Environment	1 Restrict Internet access
	2 Segregate critical systems from general IT environment
	3 Reduce attack surface and vulnerabilities
	4 Physically secure the environment
Know and Limit Access	5 Prevent compromise of credentials
	6 Manage identities and segregate privileges
Detect and Respond	7 Detect anomalous activity to system or transaction records
	8 Plan for incident response and information sharing

How do you get started?
SWIFT has created a KYC Security Attestation (KYC-SA) application to submit your attestation.

A representative from your organisation should be assigned to manage the process of contributing your data. That assigned user has access to further training to ensure your data is submitted correctly. Each organisation also needs to assign an approver of the data – which should be a CISO or equivalent level in your company.

What happens when your attestation data has reached the KYC-SA?
The data remains yours and it will be stored securely. Your business counterparts will be able to send you a request to view your attestation data. This creates an opportunity for your organisation to be transparent about your attestation status, which may increase the trust and confidence of your counterparts in doing business with you.

You have full discretion and may choose to grant access or reject access to such requests.

What about viewing the compliance status of my own counterparts?
You are also free to submit requests to view the attestation data of your counterparts. This information can help you to determine if you are comfortable doing business from a cyber risk management perspective, and to identify any additional measures you might want to put in place to enhance the security of that business relationship.

You should be preparing to use this information in your organisation's daily risk management processes.

Follow-up actions by SWIFT
To support the effectiveness of the Customer Security Controls Framework, SWIFT reserves the right to report to supervisors or others, as applicable, the names of users that fail to complete their self-attestation or fail to comply with all mandatory security controls by the relevant deadlines. Reporting to supervisors will start in 2018, and continue on an annual basis.

- From January 2018, SWIFT reserves the right to report users that have failed to submit a self-attestation
- From January 2019 onwards, SWIFT extends that right to also report users who have failed to self-attest compliance with all mandatory security controls (or who connect through a non-compliant service provider).
- For users that are not supervised, identical circumstances and data may be reported by SWIFT to their messaging counterparties.

The Customer Security Controls Framework and Attestation Process

For additional information and support on the Customer Security Controls Framework and Attestation Process, please refer to the CSP materials available via the User Handbook, SWIFTSmart training portfolio, mySWIFT, Knowledge Based Tips, videos, webinar recordings, and FAQs.

7 Strengthening fraud detection, response and recovery

The evolving character of cyber threats has changed the fraud landscape considerably. Institutions are re-evaluating their back-office systems and controls, and readiness to detect, respond and recover from incidents of fraud.

This requires a thorough review of existing systems, level of automation and integration, operator access and operations practices. In India banks and financial institutions are encouraged to:

1. **Ensure secure integration and straight-through-processing** of financial transactions to channel infrastructure. All transactions should typically originate from back-office systems that keep accurate ledgers of financial assets and liabilities. Any manual creation or authorisation of transactions must be restricted to limited staff, monitored and audited.

2. **Use structured message formats only for financial transactions.** Free form messages should be limited to broadcast and queries to counterparties. Structured message types facilitate automated screening and auditing.

3. **Use global market practices messages, such as MT 192 or 199, for payment cancellations.** To ensure timely response to fraudulent transactions, globally standardised cancellation requests should be used to stop transactions and process recovery of funds.

4. **Use gpi to track payments and stop and recall transactions.** Banks should subscribe to the GPI to have trace payments across the chain of correspondent banks and quickly stop processing of fraudulent transactions.

5. **Define and practice incident response plans.** Unlike operational incident response plans, the triggers and actions arising from security incidents are different. Timely communication and collaboration with customers, vendors, regulators, security agencies and authorities is key. SWIFT support is your first line of response.

6. **Instil a culture of cyber awareness across the organisation.** The majority of breaches occur through human social engineering. Front line should be periodically reminded and tested in their cyber awareness and readiness.

Cyber security is the responsibility of the entire institution, and should be a recurring Executive and Board agenda item. Such a detailed review will strengthen the operations capability, enabling effective fraud detection, response and recovery.

8 Are you prepared to respond?

Have you secured your infrastructure?

Review the configuration of your channel against SWIFT best practices

- SWIFT infrastructure security review
- Operational excellence review
- Architecture analysis

Comply with security controls

- Back office data flow security
- Two factor authentication
- Other security integration services

Have you implemented necessary controls?

Ensure independent reconciliation with golden-source data

- Daily validation reports
- Business intelligence reports
- Real-time flow monitoring

Implement transaction controls

- Payments control service
- gpi stop & recall

Ensure strong relationship management

- Regular RMA analysis and clean-up

Do you have the capacity to respond?

Ensure your staff are aware and trained to detect and respond to cyber threats

- Security bootcamps
- Tailored training
- SWIFT Administration and Operation certifications
- SWIFTSmart

Ensure your staff have access to latest cyber intelligence

- SWIFT Info Sharing & Analysis Centre
- SWIFT security guidelines

Have you secured your ongoing operations?

Implement independent monitoring and operations support

- Alliance Managed Operations
- Local support
- Premium custom support

9 References

- "What is the India Stack?", IndiaStack.org, April 2018
- "Vision & Mission", Unique Identification Authority of India – Government of India, uidai.gov.in, April 2018
- "About DigiLocker", DigiLocker – Your documents anytime, anywhere, digilocker.gov.in, April 2018
- "eSign Online Electronic Signature Services", Controller of Certifying Authorities, cca.gov.in, April 2018
- "Data Releases", Reserve Bank of India, rbi.org.in, April 2018
- "Reducing the risk of wholesale payments fraud related to endpoint security, Discussion note", CPMI, September 2017
- "Cyber4Sight® Special Report: Foresights 2018", Booz Allen Hamilton, December 2017
- "Cyber4Sight® Threat Assessment: India", Booz Allen Hamilton, February 2017
- "Indian Parliament, Reference Note (No.35/RN/Ref./July/2017)", Indian Parliament, July 2017
- "India's Cybersecurity Landscape: The Roles of the Private Sector and Public–Private Partnership", Nir Kshetri, June 2015
- "How India Is Moving Towards A Digital-First Economy", Harvard Business Review, November 2017
- "India's City Union Bank CEO says suffered cyber hack via SWIFT system", Reuters, February 2018
- "Breach Level Index 2017", Gemalto, April 2018
- "India's Transition To Digital Has Caused a Spike in Cyber Attacks, But They Can Be Fought", Forbes, September 2017
- "FireEye M-Trends Report 2018", FireEye, April 2018
- "Data Breaches on the Rise in India: Gemalto", CIO&Leader, September 2017
- "Breach Level Index 2017", Gemalto, April 2018
- "2017 Cost of Data Breach Study", Ponemon Institute (sponsored by IBM), June 2017

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. Within the Programme, SWIFT has established an information sharing initiative and created a dedicated Customer Security Intelligence team, bringing together a strong group of IT and cyber experts.

The team undertakes forensic investigations on security incidents within customer premises related to SWIFT products and services; the related intelligence is published in a readily readable and searchable format in the 'SWIFT Information Sharing and Analysis Centre' (SWIFT ISAC) a global portal which is available to the SWIFT community. By feeding back this intelligence in anonymised form to the wider community, SWIFT aims to help prevent future frauds in customer environments.

SWIFT Avenue Adele 1,
B-1310 La Hulpe, Belgium
Web: swift.com
LinkedIn: linkedin.com/company/swift
Twitter: twitter.com/swiftcommunity

About Booz Allen Hamilton

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world.

We solve the most difficult management and technology problems through a combination of consulting, analytics, digital solutions, engineering, and cyber expertise. With global headquarters in McLean, Virginia, our firm employs more than 23,300 people and had revenue of $5.80 billion for the 12 months ended March 31, 2017.

Web: www.boozallen.com
LinkedIn: linkedin.com/company/booz-allen-hamilton
Twitter: twitter.com/BoozAllen

Copyright

Disclaimer