Compliance & Security Framework

(Chapter -2 : DISSA Course)

Arijit Chakraborty

May 22, 2021

Cyber fraud in COVID 2nd wave – Recent Cases

- HACKERS working overtime to defraud involving **vaccines, donations, etc.**
- Cybercriminals posed as bank officials and offered loan moratorium for a “fee". There were **fake UPI (unified payment interface) handles for PM CARES Fund.**
- **120 million cybercrime victims** (February 2020 to 2021), (Norton Cyber Safety Insights Report)
- **Background**
- Once the vaccination drive started, government allowed individuals to book appointments online. It also set up a platform called **Co-WIN for registrations**.
- Cybercriminals started **releasing apps** with **Co-WIN** as part of their names.
- **Cases:** 1. cybercriminals made **fake websites** asking people to pre-book vaccines by paying upfront.
- 2. Bogus websites have been selling drugs like **remdesivir that are in short supply.**
- 3. Scammers stole data pretending to be government officials wanting to track the progress of those who are vaccinated. They ask individuals to **upload personal details and identity documents** for such tracking.
- 4. In 2020-21, **27 million Indians were victims of identity theft**

Air India – data breach : Report : May 22, 2021

- **March 2021** : Air India said that **SITA had flagged a cyber-attack** it was subjected to in the last week of February and said it led to the **leak of personal data of some of the airline's passengers.**
- Air India testament : cyber-attack compromised ata of millions of passengers from personal data registered between **August 26, 2011 and February 20, 2021.**
- **Breached data included:**

✓ passenger's name,
✓ date of birth,
✓ contact information,
✓ passport information,
✓ ticket information,
✓ frequent flyer data and
✓ credit card information.

- SITA passenger service system: breach involved data of **45 lakh passengers being leaked**.
- CVV/CVC numbers of cards **are secured** and **haven't leaked** because these were not stored by **SITA PSS data processor.**
- **No password data has leaked**, as per Air India.

Airtel CEO Alert : data breach risk

- **Airtel CEO has 'warning' for its 300-plus million subscribers:**
- Airtel CEO Gopal Vittal warned about a rise in cyber frauds amid a massive surge in online transactions during COVID 2nd wave
- Airtlel working "relentlessly" with safety features to ensure customers do not become victims
- **Fraud : modus operandi- step by step analysis**

1. *Step 1 The fraudster, **claiming to be from Airtel**, calls or sends an SMS to the customer regarding an **incomplete Know Your Customer (KYC) form.***
2. *He/she **requests customer to install the Airtel Quick Support app** from the Google Play store to allow him to help.*
3. *Since no such app exists on play store, when customer tries to install it, **he/she is redirected to TeamViewer Quick Support App.***
4. *The TeamViewer Quick Support app **allows fraudster to remotely take over the device** and accounts associated with the device.*
5. *And so, if the customer does install it, **they allow the fraudster into all their accounts connected to the device.***

Telangana: Cyber fraud goes up amid COVID-19 crisis- May 2021

- Thousands have been scammed by fraudsters with **fake oxygen cylinders, beds, ambulances and medicines**.
- Cybercrime police receiving several reports of fraudsters exploiting the situation. IS Security auditors & consultants appointed for investigation.
- *"Once the fraudster gets calls from people asking for medical services like oxygen beds availability, Covid-19 tests, vaccination etc., they collect money as advance. People are paying without verifying the genuineness of the promised help,"* ***Harinath, ACP (Cybercrime), Rachakonda.***
- **Cyberabad Police** prompted people **not to blindly trust the messages posted on social media**, emails or WhatsApp pages that promised medical assistance during the pandemic.
- *"We need to tweak privacy settings on Facebook accounts. Do not post mobile numbers openly, as fraudsters can misuse them," said Balakrishna, ACP (Cybercrime), Cyberabad.*

Cyber fraud in the name of WHO

- **Reports of cyber fraud**
- People fraudulently presenting themselves as **WHO or the COVID-19 Solidarity Response Fund, and/or sending invoices requesting payment on behalf of the Fund.**
- WHO, the UN Foundation, or the Swiss Philanthropy Foundation **will never contact individual** for credit card or banking details.
- Any other appeal for funding or donations that appears to be from WHO is a IT scam.

US SOX

Sarbanes-Oxley (SOX)

Why does it exist? The Sarbanes-Oxley Act of 2002 was passed to counteract fraud after accounting scandals at Enron, WorldCom, and Tyco impacted investor trust. These controls are mandatory for public companies.

An an IS team, how will this impact you? There are various security requirements for applications and systems that process financial data. Requirements around access management, general IT controls (ITGCs), and entity-level controls may need to be managed by the IS team.

What types of organizations leverage this framework? Public companies, or companies eyeing a potential initial public offering (IPO).

SOX 404 Attestation

- SOX Section 404 requires organizations to have an external audit performed to assess & report on effectiveness of internal controls.
- PCAOB AS5 introduced a 3-level framework describing entity-level controls at varying levels of precision (direct, monitoring, and indirect.)
- Similar to IFC u/s 143 (3)(i) of Companies Act 2013
- TOC, TOD, Walkthrough, RCM
- Increasing focus on ITGC & AppSec in risk assessment

Control structure – SOX Compliance

1. Transaction-specific (transaction-level) – Authorization or review (or preventive system controls) related to specific, individual transactions;
2. Transaction summary (transaction-level) – Review of reports listing individual transactions;
3. Period-end reporting (account-level) – Journal entry review, account reconciliations
4. Management review controls (direct entity level)
5. Monitoring controls (monitoring entity level) - Self-assessment and internal audit reviews to verify controls are designed and implemented effectively;
6. Indirect (indirect entity level) - Controls that are not linked to specific transactions, such as the control environment (e.g., tone set by management , IS Policy review).
7. IT assessment approach
8. Focused ITGC testing to support - fully automated controls have not been changed without authorization and that control reporting generated is both accurate and complete.
9. Key ITGC focus areas

- ❑ change management procedures applied to specific financial system implementations during the period;
- ❑ periodic monitoring of application security,
- ❑ separation of duties.

PCI DSS

PCI DSS

Why does it exist? The Payment Card Industry Data Security Standard (PCI DSS) exists to protect the security of cardholder data. These controls are mandatory for organizations that process credit card data. The standards are made up of multiple levels, and the extent to which organization interacts with credit card data will determine what level of PCI compliance of organization needs to achieve. For example, banks, merchants, and service providers will be held to higher standards given the nature of the business.

As an IS team, how will this impact you? Aside from enforcing certain procedures and controls based on PCI DSS level, organization may have to complete self-assessment questionnaires, quarterly network scans, and on-site independent security audits.

What types of organizations leverage this framework? Merchants, payment card-issuing banks, processors, developers, and other vendors.

PCI COMPLIANCE

- Payment card industry (PCI) compliance
- mandated by credit card companies to help ensure security of credit card transactions in the payments industry.
- Payment card industry compliance refers : *technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.*
- PCI standards for compliance are developed and managed by the PCI Security Standards Council

ICT Infra & Policy - Case : Konkan Railway Corporation Ltd

- Konkan Railway Business Operations fully dependent on Information and Communication Technology (ICT), since its inception, which helps it remain lean, efficient and using less paper.
- IT applications (apps)
- 1. Java Based Railway Applications Package(JRAP):
- customised ERP developed and maintained by IT Dept.in KRCL is a 24x7 'pillar' of KR business.
- 2. Fully integrated 'Railway Applications Package', 1st & still unparalleled custom-ERP system for Railway Operations.
- 3. Online Annual Performance Appraisal for all employees of Konkan Railway - part of this ERP.
- IR Applications:
- 4. KRCL implemented IR applications like IREPS - Indian Railway E-Procurement, & Control Office Application (COA) for train operations integrated with National Train Enquiry System(NTES) and the Unreserved Ticketing System(UTS).
- 5. E-Office: App implemented as replacement to traditional File system, paperless office , towards digital transformation and speedy clearances.
- 6. Gyansagar: e-Learning Portal implemented to enhance and support classroom teaching and offer on-line courses, evaluation, and assessments to Konkan Rail Academy.

- 7. Online Employees Self Service Portal (ESSP)
- employees SSP designed to provide access to all KRCL employees their official information regarding Personal and Service profile, Pass, Leave and Attendance details, Pay & Allowances, Claims, etc. and list of tasks to be performed by navigating user-friendly menu links on this single platform.
- As means of Corporate Communication, ESSP also provide important Highlights/Achievements, Upcoming Events, News, Broad Cast Messages and other Trending information pertaining to KRCL.
- 8. RRD Portal: Digital initiative for Retired Employees, for availing of Post complimentary Retirement Pass facility , Medical Reimbursement facilities
- 9. NIC email system implemented as part of Corporate mailing facility for all employees as the main means of communication for KRCL.
- 10. Disha or the KRCL intranet, provides information : organizational activities, circulars, procedures, policies, as a part of the official communication for employees.
- 11. Through Website - www.konkanrailway.com: information :

✓ current train position on KRCL.
✓ Information on passenger facilities and amenities,
✓ Feedback form for complaints and suggestions.
✓ Tender enquiry,
✓ status of contractors/vendors bills.
✓ Latest news/press releases,
✓ updates related to Recruitment notifications.

Thank You