Mitigating Security Risks for Today's Travellers

We live a world that is much more vulnerable to security risks than it was even a decade ago. An organisation that specialises in providing consular services to client governments across the globe battles with the possible security risk to its personnel, property, assets, resources and reputation on a daily basis. Security threats can take the form of terrorism, natural disasters, general accidents or incidents, vandalism, cyber-attacks or data theft, to name a few. And these threats could come from anywhere at any time.

While it is not possible to eliminate security risks altogether, it is possible to mitigate them by implementing dynamic security policies and plans across the organisation.

For a consular services organisation to keep its people, assets and reputation safe from criminal, terror or other hostile acts, it is imperative to have a deeply embedded commitment to maintaining a secure working environment and to the stringent implementation of security policies/plans.

The organisation must embrace the concept of commitment-based total security, and deliver security as an integral part of the daily work practices. This means that security becomes the responsibility of all employees and is not just delivered discretely by a central security department. Each office must be responsible for the implementation of an appropriate security programme that is practical, cost-effective, in compliance with relevant laws and regulations of the country in which it is located and proportional to the risk presented at that location. A security-oriented mind-set is essential as an abiding business philosophy to mitigate risks to investment, resources and operations through a series of concerted measures and controls.

While it is incumbent on each operational centre individually to define and adopt security measures best suited to address the threats it faces, the following elements should be included in all security programmes:

- Protocols to assess potential security exposures to facilities and assets leading to the identification, selection and installation of procedures and equipment capable of deterring, detecting, delaying and otherwise mitigating potential adverse consequences arising from intentionally harmful actions.
- Predefined, effective response mechanisms that proactively identify, detect and counteract both constant and escalating security threats to personnel, facilities,

operations and reputation to minimise their potential immediate impact on personnel and business operations and longer term adverse consequences for sustainable growth and development.

- Cost-effective measures to prevent the unauthorised use, removal, theft, loss, destruction or damage to tangible and intangible company assets.
- Security management designed to enable challenges to be effectively identified and addressed and, where possible, to be turned into opportunities to further business excellence and stakeholder confidence.

Each Visa Application Centre (VAC) must adhere to benchmarked standards and compliance guidelines on security and safety in accordance with the expectation of the Diplomatic Missions it serves and ensure a secure environment for the visa applicants. Layered security comprising the following is advisable to ensure this:

- Access control for pedestrians;
- Screening of man and material before they are allowed in inside the VAC;
- Electronic access control regime to regulate entry on a need basis including for staff;
- CCTV surveillance to maintain integrity of operations and ensure best customer services; and
- Intrusion and fire detection system and periodical training of the guard force to ensure that guards are performing duties as envisaged in security Standard Operating Procedures (SOPs) for interior and exterior protection of the premises.

Employee Code of Conduct

Adherence to strict guidelines on employee code of conduct, and workplace policies on integrity and fraud are a must. Very high emphasis must be placed on employee integrity and honesty and any aberrations viewed seriously and investigated by an independent team. There must be a zero-tolerance policy on breaches of business conduct and fair reporting of incidents and events.

The institution of a whistle-blower policy and an email ID to report unethical behaviour is advisable.

On-going Security Development

Evolution of the security policy, processes and procedures is essential so that they grow to meet any change in the risk profile. This may apply to a general trend in any one location (for example, an increase in crime) or other external factors such as political change. To equip the VACs and teams to handle all threats, regular reviews of service must be conducted, including issuing of updated policies and manuals. Periodic audits and training ensure a continuous level of secure service.

On-going Reviews

All safeguards must be functional at all times. Measures to ensure this include:

- Checking of all security system hardware at the end of the day. As a standard, all security equipment should be checked and tested on a weekly basis at the end of week and documented.
- The onsite VAC manager should check all hardware related to security (that is, CCTV, access card access, IDs, etc.) to ensure that the equipment is operating and functioning properly throughout the day.
- Individual CCTV screens should be monitored; should they not be functioning properly it should be brought to the immediate attention of the VAC manager on duty.

Some measures and policies that can be deployed to maximise security are:

1. **Property Due Diligence**

All risks associated with VAC property are examined with respect to landlord antecedents, clear titles, encumbrances and legal risks before entering leasehold agreements.

2. **Pre-employment Screening**

Employment of the services of reputed agencies to conduct backgrounds checks of employees and contract staff including past employment, residency, education and criminal records, and so on.

3. **Physical Access Control System**

Access control is achieved through a combination of trained guards, metal detectors and electronic card-based access control systems. A comprehensive access control system should be deployed which is designed to permit only authorised persons and vehicles to enter and exit; detect and prevent the entry of objectionable material that are prohibited; detect and prevent

the unauthorised removal of assets; and provide information to facilitate assessment and response.

4. **CCTV Surveillance**

Maintenance of round-the-clock CCTV Surveillance through an integrated system of cameras and DVR for retrieval of visual evidences is essential. Complete CCTV coverage must be ensured for key strategic areas of the VAC: entrance; bank counters/cash handling areas; application submission counters; bio-metrics booths; back office; all access doors; safes containing dongles, bio-metric data storage devices; passport and cash safes, etc. Footage archiving should be done for period from minimum 15 days to maximum 30 days depending on guidance from the client mission. Footage should be monitored by the location manager for effective surveillance.

5. **Security Policies, Manuals and SOPs**

All VAC and administrative offices should be governed by corporate security policies and procedures with clear guidelines and sanctions. Focus on information protection, asset protection, life safety and loss prevention and safeguarding of the company's reputation must be enshrined in the policy manual and SOPs. Confidentiality and business conduct agreements should be signed-off by every employee before being employed.

6. **Fire Protection**

Installation of an adequate number of smoke sensors for an early detection of fire is essential. In case the VAC is located in multi-tenanted buildings, the fire detection system would be connected to the building fire control system which activates the building fire suppression system.

Adequate portable fire extinguishers should be installed in the centres for immediate response and the staff trained in handling them. Evacuation procedures should be well laid out with proper fire escape plans displayed inside with proper signage. Evacuation drills should be practiced in the centres every quarter with participation of all staff and the activities recorded.

7. **Audits and Training**

As a practice, all VACs should be subjected to periodic risk assessment audits for high and medium risk locations by an external auditor, internal audits and control checks by the company security resource and mystery audits by an external agency.

Training, such as awareness programmes to educate employees and business partners, including contractors, regarding security and the vital role each individual plays in the detection, prevention and mitigation of security events. Fire and emergency training should be conducted periodically and drills rehearsed.

8. **Secure Document Storage, Packaging and Transportation**

Transported of documents form the VAC to the client diplomatic mission must take place in dedicated, secure document boxes. The documents must be packaged into dockets and packed into tough mother bags or boxes which are water proof and fire resistant, with unique numbers which are recorded during each activity for maintaining an audit trail. Inside the VAC, all documents must be securely stored in separate passport safes with two-hour fire ratings and provided with dual lock combination.

9. **Incident Management**

All incidents such as security breaches, failure of processes, fraud cases, loss or stolen documents/assets, equipment downtime, emergencies causing operation disruptions, etc., should be reported immediately and closed with appropriate actions.

Security incidents are best reported to the concerned business unit and/or location manager within a given timelines. A report of the incident should be initiated and escalated to all the stakeholders with plans to mitigate similar issues in the future.

Apart from this, other measures that are advisable to implement include:

- Robust and secure entry control procedures; exterior doors provided with double locking arrangement.
- Physical layered security measures backed up electronic security systems – internal and external
- Policy of clean desk enforced strictly.
- Secure document transportation using robust case/box secured with padlock and tamper evident zip lock to ensure the integrity of the documents while in transit.
- Secure packaging of documents using Tamper Evident Envelopes (TEE) for all documents during transit.
- Mystery shopping and integrity checks to ensure integrity of the processes and facilities.

- Secure document storage and secure destruction – ensure a secure document management of the data for archiving and destruction after the completion of life cycle by use of shredders.
- No storage of cash overnight in the VACs; only a minimum amount stored for day to day expenses which is placed in a fire resistant safe.
- Passports stored overnight placed in fire resistant safes with a fire proof rating adequate for two hours of protection against fire.
- A specific fire escape plan per floor for each VAC and all staff are trained in the drills at regular intervals.
- Clear-cut procedures for key management; all duplicate and the original keys to be secured inside the key box located in a secure area within VAC.

Data Protection

Obtaining and implementing a certification such as the ISO 27001 Information Security Management System which mandates that all applicable statutory, regulatory and contractual requirements shall be notified using the local statutory and regulatory requirements of the host country where the VACs are located is imminently advisable. All explicit consents should be taken before collection of information and transfer of data, both alpha-numeric and bio-metric. All personal data (PII) should be used only for the purpose that it is collected for and destroyed after the end of objective of the data has been achieved. Parts of the personal data would also be masked to ensure that the identity of the subject is not revealed. The data subject rights should also be communicated and necessary information about the controller made available to the subject.

Implementation of appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down is imperative.

A managed firewall and a rule-base is configured to allow access only to the VAC and applications inside the VAC network must be installed. Audit of these firewalls should be carried out every six months. The firewall policy should include allowing access for applications,

restricted websites, etc.; allowing local machines access and allowing local and network printer access is essential.

Process Controls

Information security policies, procedures and guidelines: Information security policies, procedures and guidelines should be designed and put into practice across the organisation. These policies should be reviewed on a regular basis to ensure that they are in line with global best practices.

SOPs for documents in hard copy, soft copy and emails: SOPs should be created specifically to address the needs of VACs in terms of complying with local data protection legislation. These address personal identifiable information (PII) data residing in all possible manners: hard copies, soft copies, email and attachments, etc.

People Control

Regular alerts from the information security desk to all: The information security team should be tasked with publishing regular mails and alerts from a central information security desk to all users within the organisation. This communication ensures that users understand the information security is a due diligence that must be practiced in all aspects of their work; it should become second nature to them.

Training for VAC staff: Regular training must be imparted to the staff at VACs and the dos and don'ts of information security reiterated. Incident reporting must be encouraged and mechanism to do so shared with the VAC staff. Employees must be encouraged to ask questions and awareness built.

Access to Systems

- The database should be encrypted to prevent unauthorised users from gaining access to the data and protect the confidentiality of data while it is handled by the organisation. The data must be purged from the database after the visa application cycle is completed or as per the guideline provided by the client Embassy.
- To facilitate transmission over a secure network, all offices must be protected from external threats through firewalls, maintained and controlled by the central IT team.

- All policies with respect to incoming and outgoing traffic (at the VAC/office level) should be defined and controlled at the VAC/office firewall level. Simultaneously, similar policies must be defined on the firewalls at the data centre level.
- Firewall rules should be configured in such a way that only VACs that require access to the respective applications can do so.
- IP restrictions should be enabled on the applications such that the application is accessible only from the visa application centre and not from anywhere else.
- To access computers in the VACs, each user should be assigned a unique user ID that needs to be mandatorily authenticated via an active directory infrastructure before a user can access the system.

Protecting Against Accidental Data Destruction or Loss

Appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing should be stringently laid down.

Backup of the Data

Data security and protection must be implemented through a rigorous data backup cycle which consists of daily, weekly and monthly backups in an encrypted format taken on media installed on a SAN. These backups can be retained for a period of six days, and regular mock tests conducted to ensure media integrity. Data on the primary site should also be replicated onto the DR site at periodic intervals.

For a consular services organisation, to operate effectively in today's world, it is imperative to consider security paramount to its operation and services. This white paper touches on some measures that can be put in place to deal with any threat at any level, whether it is physical or logical.

BLS International Services Limited is one of the largest providers of Government to Citizen (G-to-C) services, based out of India. Deploying state-of-the-art technology, proficient personnel and benchmarked processes, the organisation enables client governments to significantly enhance the delivery of their citizen services. The fact that, in a little over a decade, BLS has exponentially scaled up its operations to serve eight client governments across 47 nations speaks volumes for the superior quality and effectiveness of its solutions.